# AVIATION SECURITY MANAGEMENT

## The Context of Aviation Security Management
## Volume 1, 2 and 3

Andrew R. Thomas

Greenwood
PUBLISHING GROUP

# Aviation Security Management

# Aviation Security Management

## Volume 1

## The Context of Aviation Security Management

Edited by
Andrew R. Thomas

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

**Library of Congress Cataloging-in-Publication Data**

Aviation security management / edited by Andrew R. Thomas.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978–0–313–34652–1 ((set) : alk. paper)
ISBN-13: 978–0–313–34654–5 ((vol. 1) : alk. paper)
ISBN-13: 978–0–313–34656–9 ((vol. 2) : alk. paper)
ISBN-13: 978–0–313–34658–3 ((vol. 3) : alk. paper)
1. Airlines—Security measures. I. Thomas, Andrew R.
HE9776.A95 2008
363.28'76068—dc22 2008018728
British Library Cataloguing in Publication Data is available.



Library of Congress Catalog Card Number: 2008018728

ISBN-13: 978–0–313–34652–1 (set)
978–0–313–34654–5 (vol. 1)
978–0–313–34656–9 (vol. 2)
978–0–313–34658–3 (vol. 3)

First published in 2008

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the United States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48–1984).

10 9 8 7 6 5 4 3 2 1

# Contents

# Preface

Because of September 11, 2001, there is an almost universal recognition that aviation security is a deadly serious business. Yet, still, today around the world, the practice of aviation security is rooted in a hodgepodge of governmental rules, industry traditions, and local idiosyncrasies. In fact, seven years after the largest single attack involving the air transport industry, there remains no viable framework in place to lift aviation security practice out of the mishmash that currently exists. The purpose of this three-volume set is to begin to change that. It is my sincere hope that this work, written from a truly global point of view, will be the first of many on this most important topic.

The fact that over half of the contributors to this set come from outside of the United States is no coincidence. Although roughly 40 percent of all air transport today takes place within the United States, the long-term trend is for dramatic increases in global system usage, driven by high-growth emerging markets like China, India, Russia, and Brazil. It is widely estimated that the total volume of passengers and cargo moved via the international air transport system will nearly triple in the next 25 years. Although America will remain the single largest player, the surge will come from emerging markets.

This evolving reality mandates that aviation security management be viewed not merely on a country-by-country basis but as a global endeavor, where best practices—regardless of where they originate—are integrated into a new paradigm that is truly global in scope and scale. With that in mind, *Aviation Security Management* is intended to serve as a foundation for researchers, practitioners, and educators around the world who are looking to develop new knowledge and pass it along to the next generation of aviation security managers.

Dishearteningly, however, there is only a handful of academic programs—currently less than a dozen—where someone can actually study transportation security management. The number of schools where an aviation security management curriculum is available is even smaller. Such a lack of educational opportunities means that unless something is done quickly, the tens of thousands of new aviation security mangers who will join the profession in the coming years will not have had the opportunity to learn the best in transportation security management research and practice.

To professionalize the field of transportation security management in general, and aviation security management in particular, several requirements need to be met. First and foremost, there must be a body of knowledge and a repertoire of behaviors and skills needed in the practice of the profession, knowledge, behavior, and skills that are not normally possessed by the nonprofessional. To date, very little of that body of knowledge and repertoire exists in a clear and cogent format. While many researchers and practitioners across multiple disciplines have been engaged in their own worthwhile pursuits, there remains a deficiency in the availability of clearinghouses for that knowledge. Bluntly asked, where does one go to learn about the emerging ideas, thoughts, technologies, and best practices in transportation and aviation security management?

Clearly there is neither the need nor the desire to provide those who seek to harm transportation networks with information they can use against us. As researchers, practitioners, and educators, we must be ever vigilant, striving to balance the need for open knowledge with the necessary parameters of sensitive information. I am certain we can do both—that is, provide cutting-edge knowledge to a growing body of well-intentioned researchers and practitioners while maintaining the integrity needed to ultimately make transportation more secure.

Which brings us back to those clearinghouses. This set of volumes and the recently founded *Journal of Transportation Security* are intended to be some of the first building blocks of a much more extensive foundation, which will ultimately serve to prepare for the arrival of a true profession: transportation security management.

This first volume takes a penetrating look at the context in which global aviation security management has been carried out in the past and will likely be carried out in the coming decades.

In chapter 1, long-time aviation security practitioner Gary Elphinstone briefly traces aviation security practice from its inception up to the late 1960s. John Harrison then takes the reader through the evolution of aviation security management and education from 1968 to the present.

R. Ray Gehani and G. Tom Gehani provide readers with a broader understanding of the role air transport plays in the global supply chain. Barry E. Prentice then takes this to the next level when he explores both the tangible and the intangible benefits of aviation security measures.

Although technology often seems to dominate many conversations about the effectiveness of aviation security, Mohammed Karimbocus from Mauritius reminds us that it is the human element that has always dominated the responses to threats and attacks.

The role of the International Civil Aviation Organization (ICAO) in global aviation security management and practice seemingly gets less attention than it deserves. Moses A. Alemán—who worked with ICAO for many years—details the international aviation security program established by ICAO.

Historian Stephen E. Atkins revisits the tragic events of September 11, 2001, and answers the critical question as to how the hijackers on September 11 approached American aviation security and were able to evade it. Then, James J. F. Forest of the Combating Terrorism Center at the U.S. Military Academy fully explores the modern terrorist threats to aviation security in the post–September 11 era.

Next, Mary F. Schiavo, one of the foremost aviation attorneys in the world and former inspector general of the U.S. Department of Transportation, investigates how aviation security and the legal environment interface with each other. Schiavo then presents the most comprehensive chronology of attacks against civil aviation around the world yet published.

The appendix contains a U.S. Government Accountability Office (GAO) report that explores the how the September 11 attacks impacted the financial condition of the air transport industry and how industry responses affected competition.

*Andrew R. Thomas, University of Akron*
*Editor*

*This page intentionally left blank*

# CHAPTER 1

# The Early History of Aviation Security Practice

*Gary Elphinstone*

Violence or the threat of violence against aviation traces itself back almost to the origins of commercial flight. The first known major case of commercial aviation violence occurred in the skies over Chesterton, Indiana, on October 10, 1933. A United Airlines transcontinental flight bound for Oakland left Newark at 4:30 P.M. and stopped in Cleveland to change pilots. At 6:57 P.M., the Boeing 247, with four passengers and three flight crew members aboard, left Cleveland for Chicago and passed over Toledo some 43 minutes later. At 8:45 P.M., the pilot, Richard Tarrant of Oak Park, Illinois, radioed from over North Liberty, Indiana, that all was well and he was flying at an altitude of 1,500 feet.

A little after 9:00 P.M., several residents of this small northwest Indiana town reported hearing and seeing an explosion in the sky. John Tillotson, who lived near to where the plane went down, said he was sitting by a window when the plane exploded and he saw it clearly. He believed that he heard screams and a woman's voice shouting, "Help! Help! Oh my God."[1] According to other witnesses who also observed the first explosion, the plane blew up a second time upon hitting the ground. All on board perished, including the first flight attendant to be killed while on duty, Alice Scribner, 26, of Chicago.

It was believed the plane was flying west on scheduled time and in apparently fine condition. Given the nature of the wreckage, the size of the crash's debris field, and the testimony of dozens of witnesses, judgments on the reasons of the crash immediately focused on a bomb. Eventually the U.S. Department of Commerce aeronautics branch concluded the aircraft was destroyed by an explosive device placed in the cargo hold, a possibly a container of nitroglycerin attached to a timing device. Although no suspects were ever

charged in the bombing, it was most likely a criminal attack rather than a politically motivated one.[2]

Aviation provides a tremendous number of opportunities to individuals or groups seeking to achieve their violent ends. First criminals and later terrorists realized that aviation gave them access to a wide variety of options when it came to getting what they wanted. Criminals have traditionally looked upon aviation as an environment ripe with offerings. Billions of tons of cargo, hundreds of millions of passengers, and the ability to move easily and, more recently, affordably for long distances has lured criminals to use aviation as one of the most viable means to enrich themselves. For terrorists, aviation has long served as a target-rich environment offering a place on the world stage to trumpet their political, social, or religious beliefs. Moreover, we have seen that air travel provides disruptive passengers with a venue to exhibit a wide variety of aberrant, abnormal, or abusive behaviors.

The results of the actions of those who commit criminal activities against aviation range from the petty (as in the case of the theft of a pocketbook or wallet from a passenger inside an airport terminal) to the marginal (as when a drunken passenger threatens a gate agent) to the catastrophic (as on September 11, 2001). Consequently, it is the highest goal of aviation security to lessen the amount of violence perpetrated against the aviation system. Hence, aviation security can be defined as a combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference.

## UNDERSTANDING TODAY BY LOOKING BACK

To best understand the current state of aviation security, it is necessary to look back and see where we have come from. Table 1.1 provides an overview of how aviation security has evolved:

**Table 1.1**
**Evolution of Aviation Security Practice**

| *Year* | *Defining event* | *International/national action* |
|---|---|---|
| | | Paris Convention 1910 |
| 1933 | First recorded bombing of commercial aircraft | |
| 1944 | | Chicago Convention |
| 1945 | | IATA founded |
| 1947 | | ICAO founded |
| 1945–62 | Spate of hijackings by persons fleeing communism | |

**Table 1.1**
**Evolution of Aviation Security Practice (*continued*)**

| *Year* | *Defining event* | *International/national action* |
|---|---|---|
| 1963 | | Tokyo Convention |
| 1968 | First terrorist hijack of commercial airline—El Al, July 22 to September 1 Spate of hijackings to Cuba (19) | IFALPA action on hostages |
| 1969 | Continuation of hijackings to Cuba | Committee on Unlawful Interference established |
| 1970 | Hijacking of TWA, Swissair, Pan Am, and BOAC aircraft and destruction at Dawson Field, Jordan | Formation of IATA Security Advisory Committee Hague Convention |
| 1971 | | Montreal Convention Issue of first edition of *ICAO Security Manual* |
| 1970s | | Introduction of passenger screening, sky marshals, and other security measures for international flights |
| 1972 | JRA assault at Lod Airport, Israel, 23 killed, 70 wounded Cathay Pacific aircraft destroyed in flight, 81 killed | |
| 1974 | Start of terrorist bombings of airline offices TWA aircraft destroyed in flight, 88 killed | |
| 1975 | | Annex 17 to Convention first issued |
| 1977 | Lufthansa aircraft hijacked, incident terminated by armed assault by German GSG 9 | |
| 1978 | | Bonn Declaration |
| 1979 | | AACC (ACI) and IATA establish the Joint Aviation Security and Facilitation Working Group |
| 1980–82 | High point in terrorist attacks against civil aviation. (105 attacks in three years) | |
| 1983 | Gulf Air aircraft destroyed in flight, 112 killed | |

(*continued*)

**Table 1.1**
**Evolution of Aviation Security Practice (*continued*)**

| *Year* | *Defining event* | *International/national action* |
|---|---|---|
| 1985 | Air India Flight 182 aircraft destroyed in flight, 329 killed TWA Flight 847 hijacked, Lebanon Simultaneous terrorist attacks at Rome and Vienna airports | Ad hoc group of experts on aviation security met in August to rewrite Annex 17. (Issued in May 1986) Baggage reconciliation introduced on international flights. |
| 1986 | | FAC was established and assumed responsibility for implementation of airport security measures |
| 1987 | Korean Airlines Flight 858 destroyed in flight, 115 killed | 100% screening of domestic flights introduced in Australia. First meeting of ICAO Aviation Security Panel (replaced Committee on Unlawful Interference) |
| 1988 | Kuwait Airways Flight 422 hijacked—16 days duration Pan Am Flight 103 destroyed over Lockerbie, Scotland—269 people killed | Montreal Protocol |
| 1989 | UTA Flight 772 destroyed in flight—171 people killed Avianca Airlines aircraft destroyed in flight over Colombia | Increased R&D effort to detect explosives and harden aircraft and containers |
| 1990 | | Presidents Commission on Aviation Security & Terrorism. |
| 1991 | Singapore Airlines 737 hijacked | Baggage reconciliation introduced Convention on the Marking of Plastic Explosives |
| 1993 | Truck bombing of World Trade Center Complex in NYC | |
| 1993 | | Fifth edition of Annex 17 effective (43 standards) |
| 1994 | IRA Mortar attack on Heathrow Airport, UK Air France hijacked by Algerian extremists—French commandos terminated incident in Marseille | |

**Table 1.1**
**Evolution of Aviation Security Practice (*continued*)**

| *Year* | *Defining event* | *International/national action* |
|---|---|---|
| 1995 | Operation Bojinka foiled—Al Qaeda plot to attack multiple U.S. aircraft and fly one into CIA headquarters | |
| 1996 | Ethiopian Airlines B767 hijacked and crashed into sea when aircraft ran out of fuel—123 people killed Explosion aboard TWA Flight 800—All passengers and crew killed | Fifth edition of ICAO Security Manual issued Gore Commission established by U.S. president |
| 1997 | | Sixth edition of Annex 17 effective (47 standards) |
| 1999 | | Checked baggage screening to be introduced at international airports |
| 2001 | September 11 attacks | |

As illustrated, the evolution of aviation security has been marked by two streams that are intertwined one with another: defining events and international and national action. The chapters and appendices in this set of volumes will detail many of the defining events and the actions taken by international and national actors. I'd like to highlight just some of the roots of aviation security leading up to the critical year of 1970.

## Paris 1910: The First International Aviation Conference

With the advent of a machine that could cross national borders, sovereign interests were aroused and decisions were taken by governments in these early days in order to establish a legal framework. The genesis of this awakening to the significance of the airplane occurred in France in 1908, which is where the legal structure of civil aviation begins. The French government was increasingly concerned by the number of flights penetrating French sovereign airspace. They called for a conference of representatives of 21 European nations to discuss the future regulation of air transport. Eighteen nations accepted the invitation and the conference was held during May and June of 1910.

The conference focused on the legal status of airspace and the authority of nations to regulate the movement of aircraft over land and water. The outcome was that of the 45 articles placed before the committee, 43 articles and 2 annexes (supplements) were accepted. The Paris Convention also authorized the creation of the Paris-based International Commission for Air Navigation (ICAN). ICAN played an essential role as a focal point for international aviation and soon extended its sphere of influence beyond the boundaries of Europe. ICAN operated until World War II and was to become the forerunner of ICAO (the International Civil Aviation Organization).

## The Chicago Convention of 1944

During and after World War II, aircraft design and capabilities were changing rapidly, and at the same time a vast network of passenger and freight movement was being established. However, there were many problems, both political and technical, to which solutions had to be found in order to benefit and support the postwar environment.

This development of the airplane into a major form of transport brought with it huge problems. For instance, there was the question of commercial rights: what arrangements would be made for airlines of one country to fly into the territories of another? The need for safety and regularity required the building of airports. How would they be constituted? What language would be the common one for the industry? How about the establishment of weather reporting systems and operational standards? These and countless other questions were far beyond the capabilities of individual governments to solve.

As they planned for peace after World War II, many countries came to believe that additional measures of control needed to be installed in the interests of safety. Confidential discussions were held in the United States on the future role of civil aviation.

The positions of the three major powers at a conference in 1943 were difficult to reconcile; The United States stood alone as the global aviation leader, while Russia and Great Britain were far behind. The United States was undamaged by the war, had extensive experience in logistical air transport operations, and possessed a massive aircraft fleet. It was manufacturing nearly all the world's aircraft and had a huge fleet of DC-3s at its disposal. There was considerable potential to dominate postwar civil aviation.

In September of 1944, Vice President Henry Wallace, on behalf of President Roosevelt, invited 55 nations to a conference in Chicago to discuss the future of postwar civil aviation. For more than five weeks, the delegates considered the many challenges of international civil aviation, and ultimately accepted what is known as the Chicago Convention on International Civil Aviation. The Chicago Convention provided the beginning of standardization in aviation throughout the world in such areas as communications for long air routes, airport infrastructures, air navigation, and air traffic control. In addition, another charter was adopted: it was to become the idea of aviation

security and was titled "The Prevention of Unlawful Interference to Civil Aviation."

### The Birth of Aviation Security

In the early 1960s, due to a spate of hijackings of aircrafts by citizens seeking to flee Communist oppression, the ICAO Council's legal committee was directed to develop international conventions to deal with unlawful interference with civil aviation, which resulted in the birth of aviation security at the Tokyo Convention. The outcome was agreement on theapplication of the charter adopted at the Chicago Convention to offenses committed by a person who is on board an aircraft. Clearly, this was only one step toward the broader goal of establishing aviation security practices. Still, it was a start.

In September 1970, two related events triggered the call for an international, coordinated aviation security program. After hijacking two flights—involving a British Airways and a TWA aircraft—members of the Popular Front for the Liberation of Palestine ordered the planes flown to an abandoned World War II airport. The hijackers released the passengers and then blew up both planes. The same group had carried out a similar attack on a Pan Am 747 in Cairo a few days earlier. International aviation would never be the same again.

## TODAY

Aviation is one of the world's most important businesses. The growth of the industry over the past decades has made it one of the engines for the expansion of the global economy. The aviation industry has driven a substantial part of the economic and social integration that has brought much of the world closer. By moving billions of passengers and billions of tons of cargo each year, the industry has changed the way of life of most human beings on this planet. Distance is now often measured in hours rather than weeks or months. New York to Hong Kong takes 13 hours by air—35 days by sea. Manufactured goods produced in Chicago can be transported to distributors in Ouagadougou, Burkina Faso, within 48 hours. The United Parcel Service (UPS) and Federal Express (FedEx) can send an envelope from Cleveland to Tashkent in 72 hours. The aviation industry has changed forever the way many human beings look at the world around them.

An emphasis on airline security continues to be fundamental to a healthy global civil aviation system. The growth in air travel of passengers and freight is dependent upon

- an adequate and efficient infrastructure with which to support airport operations without a harmful impact on the environment;
- speedy and efficient handling of passengers' baggage and freight at departure, transit/transfer, and arrival points; and
- a safe and secure environment.

It is the responsibility of anyone associated with the aviation industry to contribute to the safety and security of its operations, not just dedicated aviation security professionals.

## NOTES

1. Andrew R. Thomas, *Aviation Insecurity: The New Challenges of Air Travel* (Amherst, NY: Prometheus, 2003), 167.
2. Ibid.

# CHAPTER 2

# Aviation Security Practice and Education: 1968 Onward

*John Harrison*

Terrorism involving aviation has been going on for many years. The most dramatic terrorist attacks in history were those conducted by al Qaeda on September 11, 2001. Civil aviation is intimately involved in the metamorphosis of groups with specific and identifiable objectives—demands for liberation from occupation or a separate homeland—to transnational groups with almost no known objectives. One can trace the development of terrorism as a phenomenon as well as its tactical development by studying its interaction with international civil aviation. Even as terrorism moves through an organizational evolution, from highly structured organizations to self-generated and operationalized cells, such as those that planned an attack against Fort Dix in New Jersey, plotted against John F. Kennedy Airport (JFK), and attempted to bring liquid explosives aboard a plane in the United Kingdom, the focus of terrorists remains on aviation.

The aviation sector has, for years, been involved in cross-border criminality, which also includes terrorism. Transnational criminal organizations use the aviation system to transport contraband and, increasingly, people across the globe. Cocaine smugglers have used the FedEx air delivery system to transport their products across the United States, and narcotics smugglers from Guyana have used U.S. Mail pouches to smuggle millions of dollars worth of cocaine into the United States through JFK. Organized gangs of human smugglers routinely attempt to use the aviation system to move people into North America and Europe. Kenyans desperate to flee their country have been found stowed away in the wheel wells of British Airways flights, arriving frozen to death at Heathrow.

This chapter will attempt to provide an evaluation of the operational environment that the civil aviation industry faces due to crime and terrorism.

The chapter will examine the traditional responses to crime and terrorism and will attempt to raise a significant and often overlooked area in security, that is, education. The argument is that security education is reactive and lacks a comprehensive approach that is targeted at addressing the current and evolving threat and risk environment. Done well, however, it is capable of creating a professional cadre of motivated line staff and management members.

## THREAT VERSUS RISK

One of the ironies facing the aviation sector is that while the industry is advanced in evaluating economic risks in its decision making and in taking the necessary steps to manage those risks, it is still focused on responding to security threats and appears to have great difficulty in developing and articulating its response. In most of the world, the service providers, particularly the carriers, are no longer responsible for security. Nevertheless, the industry bears the direct and indirect costs both of the implementation of security measures and of the failures that occur if, despite such measures, criminals and terrorists still manage to carry out their activities.

The suggestion here is that there needs to be a better system of evaluating and responding to risk. The first element in this approach is to understand what threat means. Threat is an exploitable vulnerability. When one examines the range of potential targets that modern aviation offers to a perspective terrorist, the threat appears enormous and unmanageable. The theft and counterfeiting of travel documents, the attacks on land and air targets, and the theft of equipment, just to name a few of the problems, indicate that there are weaknesses and potential gaps that terrorists can exploit. And as the Irish Republican Army (IRA) famously stated to British authorities, "We have to be lucky once; you have to be lucky all the time." So how does a society protect everything it values? What is needed here is to shift from simply responding to the threat and move to examining the situation from a risk perspective.

There are many ways of examining risk, but the two critical elements are the probability of a given vulnerability being exploited and the consequences of that exploitation. The simple process of evaluating these two elements helps to order the environment and allows limited resources to be deployed optimally. One can further refine the evaluation model by applying the threat structure to terrorist groups. Evaluating the threat posed by any given group rests on knowledge in three areas: the intentions of a given group, its ability to act on these intentions, and the operational environment involved. This additional step is critical to assessing the threat and risk environment; without it, the security community will remain focused on the potential threat and never grasp the actual threat and its accompanying risk. While the primary focus of security-related information has been on the users of the aviation system, more attention needs to be given to those working within the system. The terrorist

plot against JFK International Airport and the April 2004 arrest at JFK of 25 cargo and baggage handlers working for a Guyana-based cocaine smuggling ring[1] show that the threat comes from within as well as outside. One critical element of security is the ability to conduct rapid and ongoing security checks on staff working in all areas of aviation. This is a necessary first step in protecting carriers' national interests, but it has historically been blocked by labor interests. It would seem that a reasonable compromise can be reached that protects both the employees and the users of the aviation system.

Critically, this is one area where the aviation industry is leading the government. Aviation has long understood the aforementioned model, and most of the security courses offered to the industry both before and after September 11, 2001, include threat and risk evaluation components.

## THREATS TO VARIOUS SEGMENTS OF THE AVIATION INDUSTRY

The above discussion raises a question: what are the threats to aviation? Given the size and complexity of the system, there is no simple answer. The two broad categories of aviation are the landside and airside categories, both of which will be addressed in this section. From the terrorist perspective, the landside segment offers a large and relatively untapped operational environment. Only four notable attacks have taken place against landside aviation: the Japanese Red Army attack on Lod Airport in 1972, the Abu Nidal attack on the Rome and Vienna airports in 1985, the Tamil Tigers' attack on Colombo Airport in 2001, and the Glasgow attack in July 2007. One can argue that the more traditional terrorist organizations, such as those mentioned above, have wanted to limit casualties and retain a moral legitimacy, and harming large numbers of innocent passengers would undermine both objectives. New terrorist groups have none of these limitations, so it remains unclear as to why more landside attacks have not yet occurred. Criminal activity is more common on the landside. This includes smuggling, theft, and other activities directly related to aviation, but also ancillary activities such as identity theft from travel documents or crime in airport-based hotels. This issue becomes more pressing as the industry moves to wireless travel, as envisioned by some Japanese airports.

Access control is a critical issue for security. This includes access not only to secure areas but to the perimeter fencing as well. There are many countries where basic security is lacking or in poor repair, allowing unauthorized persons to gain easy access to aircraft as stowaways. While there is currently no evidence to suggest that terrorists are exploiting this weakness, the possibility of such exploitation exists. The current high-tech solutions offered by biometrics and other forms of technology are encouraging.

But the best way to protect aviation also involves the weakest and least developed area, that is, people. The need for trained and motivated staff members who are encouraged and supported in their efforts to protect civil aviation is the most vital component. All of the profiling and scanning

equipment will not stop a determined attacker if the security personnel are inattentive or corrupt. This is exactly what occurred in the suicide bombings targeting Russian aviation in August 2004. While the threat is potentially high, the risk posed by terrorist attacks on the landside remains, with minor exceptions, quite low. The criminal threat is higher, but the risk is low because criminal interference with landside aviation is marginal.

The aviation industry, landside and airside, encompasses four components. The first is commercial civil passenger aviation, including international civil aviation, which is the primary focus of this chapter. The threat in this category remains high, as its impact on the entire civil aviation industry is high. The second component is military and other government-related aviation. Aircraft within this component are also targets of terrorists. For example, al Qaeda tried to shoot down a U.S. military cargo aircraft in Saudi Arabia in 1995.[2] But actions against such official aircraft do not usually generate the publicity that assaults on passenger aviation do, so while the threat in combat zones is high, it remains low outside of these zones. The third component is cargo aircraft. The threat to cargo aviation is economically important but this area has never been explicitly targeted. The 2003 attempt to shoot down a DHL aircraft in Baghdad was the choice of a target of opportunity, as few passenger aircraft serve Iraq.[3] Although al Qaeda has allegedly been interested in hijacking a cargo aircraft, to date there has been no publicly disclosed evidence of such an attempt. As such, threats involving cargo security present a low level of threat and a low risk.

The fourth component is general aviation, which includes private, corporate, charter, and agricultural aviation, and all other types of aviation not mentioned above. This is a component that terrorists have largely ignored. Al Qaeda has been interested in crop dusters as a means of dispersing chemical or biological weapons and it may have plotted to attack the U.S. Embassy in Paris[4] by using a suicide helicopter attack and to attack North Atlantic Treaty Organization (NATO) shipping in the Straits of Gibraltar, but these are exceptions to the rule. Additionally, given the limited damage caused by these aircraft, such as the private aircraft that crashed accidentally into an apartment building in New York City, the threat and risk remain low.

The criminal exploitation of aviation is common across all four categories. The threat posed to the system is twofold: first, the use of aviation to transport contraband and humans illegally from one country to another, and second, the theft of goods, as well as parts, in transit. Both are a growing issue of concern for the industry, but as the commercial threat to the industry is much less severe than the political threats posed by terrorists, the focus of this chapter will be on the latter.

It is critical to note that any security measure must balance not just individual rights and convenience but also criminal and terrorist activity. Attempts to respond to the terrorist threat alone, to the exclusion of counter-criminal efforts, are often self-defeating. Any facility that is well maintained and policed will help to dissuade terrorists from using it as a point of attack. Terrorists and

criminals share much of their methodology; thus, having a well-trained, alert, and active staff and police presence is the best deterrent.

Just as there are two broad categories in the operational environment (that is, landside and airside), there are two general categories of training: these are compliance and general management. The first category is designed to meet ICAO or other national requirements for security staff. It most commonly involves the line staff responsible for security, such as screeners, but ongoing educational requirements are common for both line and management staff. General management training is defined as involving courses that while useful are not specific to the security or aviation industry. These are courses that are delivered across industries, including courses involving motivational skill or goal development. There is no argument that these skills are critical to managers, but they are not sufficient to provide increased security skills.

Most current training on countermeasures is inadequate in its efforts to assist security staff in detecting suspicious behavior irrespective of the motivation for such behavior. The critical weakness in the current configuration is that the focus remains on security staff and cabin crews. Carriers such as Singapore Air attempt to broaden the exposure through programs such as its annual Safety and Security Week. This program brings together aircrews, airport staff, security personnel, and nonsecurity headquarters staff to be briefed on all aspects of safety and security.[5] This model is a good starting point for assisting staff in their training, but a wider, sustained effort is needed.

## THE THREE PHASES OF THE POLITICAL THREAT

The terrorist threat to international civil aviation has gone through three phases during the past 80 years. The first, 1948 to 1968, was characterized by flight from persecution or prosecution. The second, 1968 to 1994, was political. The third began in 1994 and is ongoing—it involves the use of aircraft as weapons or battlegrounds. Each has been marked by a singular, defining event but has involved aspects of the other stages. Each stage has also elicited a response that in many cases has profoundly changed civil aviation.

The first phase, the flight from persecution or prosecution (1948 to early 1968), involved people attempting to leave their home countries who hijacked aircraft for fast and convenient escapes. The first such hijacking occurred on April 6, 1948, when the three crew members (including the pilot) and 21 of the 26 passengers hijacked a Ceskoslovenske Aerolinie (CSA) internal flight from Prague to Bratislava and landed in the U.S. Occupation Zone in Munich. All of the hijackers were seeking political asylum.[6] This type of escape was appealing to the hijackers because many of them were former military pilots. Also, the defectors were greeted as heroes who had made a dramatic dash for freedom. Even when a Soviet pilot was killed resisting the taking over of a flight, few in the West viewed this as a criminal act. From 1948 through the late 1950s, asylum was a fairly common goal (20 out of 37 hijackings).[7] The persecution or prosecution phase waned from the late 1950s as jet aircraft use

became more widespread and the focus shifted from Eastern Europe to the United States. In the industry's view, there was no need for enhanced security as jets were far too difficult to control without experience. Thus, there was a general perception that hijackings would gradually decline.

The Cuban Revolution, led by Fidel Castro, ousted the pro-U.S. dictatorship of Fulgencio Batista in January 1959, and Castro began to consolidate his hold on power. A hijacker "highway" between the United States and the island of Cuba soon appeared. Cubans who had been associated with the Batista regime or disliked the drift toward Communism devised ways to get to the United States, just 90 miles away. From 1960 to 1969, 49 out of a worldwide total of 91 hijackings or attempted hijackings involved escapes from Cuba to the United States.[8] Beginning in 1961, some of the traffic went in the opposite direction—people wishing to make a quick exit from U.S. jurisdiction (criminals, the mentally unbalanced, and some self-described revolutionaries) escaped to Cuba. Almost all ended up serving time in Cuban jails, although a few "revolutionaries" managed to escape that fate.

There may have been political motives for escaping from Eastern Europe or Cuba, but aircraft were not viewed as the means of delivering a political message. There were no efforts to use the aircraft as anything other than getaway vehicles; individuals fleeing Communist countries were showing their desire to flee from a repressive system, but they were not seizing aircraft to call attention to the broader political questions. Those fleeing to Cuba were attempting to escape justice, or in the case of homesick Cubans, to return home; they had no broader political agenda. People still use aircraft as a means of escape: several hijackings attempted in China during early 2003 were initiated by people trying to reach Taiwan.

Nevertheless, due to hijackings, security became a concern for civil aviation for the first time. The now common passenger screening machines, passenger profiling, and armed police at airports were all introduced as a result of this phase. Industry training followed later. The international community began rapidly passing conventions requiring specific security procedures. States, and the industry, began training for compliance rather than risk, an understandable approach given the rapidly developing situation.

Phase two, beginning in 1968, wedded politics and interference with international civil aviation.[9] The Popular Front for the Liberation of Palestine (PFLP) hijacked Israeli state airline El Al Flight 426, bound for Tel Aviv from Rome, on July 23. The three hijackers diverted the Boeing 707 and its 38 passengers and 10 crew members to Algiers. For some of the victims, the ordeal lasted five weeks, the longest hijacking on record. Many terrorism experts date the age of modern terrorism from this incident. The PFLP also introduced mass hijackings as a tactic when, from September 6 to 12, 1970, the PFLP and its allies hijacked four aircraft, a total of 577 passengers, and 39 crew members. Only two of the four aircraft arrived at the PFLP-occupied Dawson Field in Jordan (a former British military field, which gave its name to the hijacking incident). The hijackers demanded that the Swiss, German, United Kingdom,

and Israeli governments release the Arabs they were holding. The hijacking ended with the destruction of three aircraft (two in Jordan and one that landed in Egypt), but no passengers were lost. During this incident, the PFLP had attempted to hijack an El Al plane departing from Amsterdam but was foiled by an in-flight security officer. The flight landed safely in London.[10]

Hijackings were the most popular tactic for many individuals. Between 1967 amd 2004 there were nearly 1,000 airline hijackings. It is estimated that approximately 85 percent were carried out for political purposes. The remainder were conducted by terrorists.[11] The international civil aviation regime began to respond to the menace, deploying the so-called X-ray machines, for example. That measure was only partially effective, as it foiled an average of only about 19 percent of the terrorist hijackings at the time.[12] But it did cause the terrorists to switch to other tactics.

Terrorists switched from hijackings to sabotage bombing, partially as a result of increased security. Terrorists during this phase were looking for the drama of armed propaganda, while limiting the risk of casualties. But sabotage bombings presented a greater risk for the terrorists because of the large numbers of casualties created by such attacks.[13] Nevertheless, such tactics are still frequently used to convey a message, usually retaliatory. The bombing of Pan Am Flight 103 was one such example; it was targeted in response to U.S. raids on the Libyan military and terrorist infrastructure. It was not intended to "instruct" the public; no official claim of responsibility was made. The United States did not require a claim of responsibility to know where responsibility lay. This attack also illustrates the risks inherent in such operations. Because the aircraft exploded over land, rather than over the ocean as planned, it provided gruesome images that enraged the public. Any intended message was drowned out by the grief and cries for retaliation. The image of the nose section of the Boeing 747 resting in a Scottish field became the symbol of international terrorism until September 11, 2001.

It is critical to remember that casualty figures are not vital to the terrorists; in fact, the fewer the better. The propaganda value of an attack is more important than the lives lost.

The evolving threat caused the security industry to evolve as well. The security tactics deployed for the first phase threat were adapted, and thus passenger profiling, screening, and eventually baggage reconciliation became standard practice rather than being targeted to specific flights. The provision of security became a permanent fixture, requiring a more formal training and career path for staff. Compliance training continued to be the norm, but the security industry began to adopt the approach of the bourgeoning management training industry. Management training was imported directly into security training. Some of the lessons learned from this type of training are no doubt valuable, but as most of the instruction was conducted by people who were not security specialists, it was of questionable security value.

The third phase, which began in 1994 and is ongoing, is characterized by the use of aircraft not as means of delivering a message but as instruments with

which to inflict massive casualities. Terrorism experts had begun to detect a trend in the late 1980s toward an extremist interpretation of religion by terrorist groups. Islamist groups' interpretations are most widely studied and viewed as dangerous, but extremist violence also emerged in the Sikh, Christian, Jewish, and Hindu religions, as well as in so-called new religions known as cults. While much of the cult violence was directed inward,[14] with the notable exception of Aum Shinrikyo,[15] traditional religions directed violence outward. This externally focused violence sought to justify extreme violence against non-coreligionists through the demonization of "the other" and to rationalize wanton destruction by identifying violence as a sacred duty.

International civil aviation concerns about religiously motivated terrorism have characterized phase three. On December 24, 1994, Air France Flight 8969 bound for Paris from Algiers was hijacked by the Algerian terrorist organization, the Armed Islamic Group (GIA). Four hijackers boarded the aircraft disguised as Air Algerie security staff.[16] Authorities delayed the departure but were intimidated into giving the go-ahead when two of the 227 persons on board met their deaths at the hands of the hijackers. The French government decided not to allow the aircraft to approach Paris because its consulate in Oran, Algeria, had received an intelligence warning that the hijackers intended to blow up the aircraft over the French capital.[17] The flight crew convinced the hijackers that refueling in Marseille was a must. After the aircraft touched down, hours of fruitless negotiations ensued, whereupon the terrorists demanded fuel or they would destroy the aircraft. French Special Forces (GIGN) stormed the aircraft and, after a 25-minute fire fight, rescued the 161 remaining passengers (some had been released during the negotiations) and three members of the flight crew.[18] The melee ended with the death of the hijackers; nine GIGN commandos were injured, some seriously. The terrorists had not revealed their exact target, but it was Paris, and the aircraft was their weapon. This change in tactics ushered in a new era for international civil aviation. No longer was civil aviation a political stage for terrorists; it was their weapon and battleground.

The GIA, a radical Islamic terrorist organization, had been attempting to establish an Islamic state in Algeria. Its brutal tactics contributed to more than 100,000 deaths during the civil war fought there throughout the 1990s. France was a particular target because of its support for the military government that denied the radicals an election victory in 1991. The suicide hijacking was the GIA's revenge. Using civil aviation as an instrument of revenge is not new; using it to target an entire city is.

Al Qaeda is in a class by itself in conceiving, and in some cases executing, terrorist spectaculars. The first was Ramzi Yousef's attack on New York's World Trade Center in February 1993. Yousef and his coconspirators had planned to topple one tower into the other, potentially causing 250,000 casualties. The 1993 incident killed six and wounded thousands. The failure of the ground-based attack led the cell to consider an aviation attack.

The most audacious plan, Operation Bojinka, was designed by Khalid Sheik Mohamed, Yousef's uncle, who was to be the mastermind of the September 11,

2001, operations. Yousef and five coconspirators planned to place bombs on 11 or 12 U.S. transpacific carriers during a 48-hour period, in a series of events that would have killed as many as 5,000 people.[19] The explosive was to have been liquid nitrogen concealed in contact solution bottles that, in the opinion of most experts, not even the most highly skilled and motivated security screener would have been able to detect. It was to have been part of a larger operation that included an aviation suicide attack against the Central Intelligence Agency headquarters. It remains unclear whether the operation was to have involved a general aviation aircraft, such as the one that was flown into the White House in February 1993 by a man (not a terrorist) committing suicide, or an attack similar to those that were to occur on September 11.[20] The plot was never brought to fruition due to a fire mishap in the apartment where Yousef was staying in Manila, and he was subsequently captured.

Al Qaeda demonstrated its creativity on September 11 when its operatives turned four jumbo jets into a quartet of poor-man's cruise missiles. These events, and the case of Richard Reid and the missile attack in Mombasa, Kenya, were designed to inflict enormous casualties, any political message aside. The perpetrators' willingness—even eagerness—to die makes phase three of the threat the most dangerous and certainly the most difficult to defend against.

While terrorists transitioned from phase two to phase three, the security industry did not. The intelligence and security services missed the significance of the emergence of religious terrorism and its impact on international civil aviation. Aviation was no longer simply a stage for violent political theater; aircraft were now being used as weapons. This would appear to require a total reexamination of existing security assumptions and their related training and implementation. Sadly, no one was aware of the requirement. The existing training infrastructure had grown stale. This is in part due to the reliance either on retired security professionals who had aging anecdotes but little teaching ability or on academics who may have been able to teach but were unable to translate the material into useful information for security professionals at any management level. At the time when management and academia needed to be working together, they failed to develop the most basic working relationship.

One consequence was the aviation industry's continuing reliance on the government or for-profit security consultants for both critical information and training. While most of the commercial providers were disseminating valid information, some provided exaggerated or misleading information to provide a basis for either their own product or that of a strategic partner. Many of the providers reveled in the cult of knowledge, telling the industry that only professionals with access to classified information could provide the necessary current intelligence and training materials. What the aviation industry needed to know was that 90 to 95 percent of all information on terrorism is available through open sources. The industry does not need to invest in its own research and analysis; it can utilize the existing academic infrastructure. An additional

benefit is that in many cases academics can provide training materials and in some cases trainers for at least some aspects of the course. There has been some positive movement in this direction, but memories are long, and the past relationship in training has not been forgotten by any party.

## THE INTERNATIONAL RESPONSE

The civil aviation system was one of the earliest international systems. The rapid spread of this industry in the last few decades is a tribute to the growth in both business and leisure spending. This growth has stretched the international civil aviation system to its limits in many areas, security training being one. The proliferation of training providers has stretched the quality, without decreasing the price of the services available. Even in the developed world, where money and resources are plentiful, training costs are an issue. This situation is even more acute in the emerging aviation markets of Asia and Africa. Resource limitations and inadequate technical capacity present an easy opportunity for terrorists to enter the system to pursue their nefarious ends. Many nations have attempted to address this concern by working with the developing markets to address the frontline security weaknesses. Funding is available for fencing, X-ray machines, and staff to reduce these weaknesses. The critical weakness remains the lack of qualified middle and senior managers able to provide managerial, let alone critical, leadership and strategic direction.

One effort to address this is an innovative training course provided by the Singapore Air Transport Services (SATS). A joint effort between the Singapore government and SATS, the program brings promotable middle and senior managers to Singapore for two weeks of intensive security training. The program is premised on the fact that "many nations helped Singapore to develop. Singapore remembers this and wants to return the assistance."[21] The critical component of this program is the recognition that there must be a balance between technical and human solutions to security and that the balance requires a different approach to management. Much of the developing world cannot afford or support the widespread use of technology. With the availability of plentiful low-cost labor there is a viable alternative. This does, however, place an additional burden on management.

Technology has many well-understood advantages and limitations. In a management context, it is supposed to improve efficiency while reducing staff numbers. This, among other issues, reduces the need to recruit, train, motivate, and retain large staffs. The equipment needs to be maintained, a difficult issue no doubt, but the challenge of managing a staff with limited management experience is reduced. The SATS program is important for its capacity-building efforts, as well as for instilling the need for a flexible, layered approach to security.

Despite the laudable efforts mentioned above, there is still a severe gap in training for security staff at all levels. In the past, the threat and risk environment

developed at a slower rate, permitting training to evolve. This meant that practical work experience counted more heavily than formal training. The industry did not take advantage of this slower evolution, but it had the potential to blend experience with proactive training in order to remain ahead of the threats. The far more rapid developments and evolution in the current phase of terrorism have negated this potential advantage and placed a premium on strategic thinking rather than tactical implementation—exactly what the current training will not achieve.

## RECOMMENDATIONS AND CONCLUSIONS

The problems described above need to be addressed at three levels: strategic, operational, and tactical. Each has a corresponding training component that will be addressed below. For the training level, the critical component is to develop a comprehensive program that provides the skills necessary for compliance training, management training, and more comprehensive professional training.

The strategic level involves a battle of ideas. In general terms, we are not even engaged in this issue in any serious or sustained manner. While the international aviation system cannot, or should not, be involved in this directly, it can and must understand what the change in terrorism has meant and how it will impact its operations.

**Recommendations:**

- A sustained research effort by the industry to understand the trends in transnational threats and how they will impact its operations
- Industry investment in nontechnical research in order to support technical security efforts

The social science research mentioned above is essential to assist both an understanding of terrorism and also the operational approach needed to counter the threat and mitigate the risk posed by terrorists. The enormous lead time and expenditure required to develop and deploy technology often means that it becomes redundant due to a shift in terrorist tactics. By engaging with the existing threat research infrastructure, we can avoid this continuing problem.

This is most appropriate for senior managers. They need to be able to think about the trends across their industry, a skill they have developed quite well in the business sense. However, they need to apply this skill in wider areas of society that will impact the industry, and this is something they currently do not do as well, if at all. They need to understand the strengths and limitations of the policy community and the strengths and weaknesses of their industry, and how they can cooperate to achieve similar goals. Training courses have to be designed to get senior management to think strategically, manage knowledge, and gain an understanding of where to go for analysis.

The second level of analysis of terrorism is the operational level. This refers not only to the operations of the organized groups, such as al Qaeda, Hamas, Islamic Jihad (IJ), and others, but also to the response to these groups. The response community is doing exceptionally well in this area. Organized groups are finding their operational environment heavily restricted. There has been similar success with regard to the aviation environment. The commitment to a multilayered approach to such steps as an increase in access control, the introduction of air marshals, and the provision of locked cockpit doors is positive. But the international community needs to take a more active role in the critical area of standards and information sharing.

**Recommendations:**

- ICAO needs to establish basic standards for such items as cargo screening, document security, and other in-flight issues.
- ICAO needs to have enforcement power, which can and should include economic incentives for meeting required standards and recommended practices.
- ICAO and the International Air Transport Association (IATA) should establish a joint intelligence and security center (JISC).

The international community is attempting to address the first issue, but there are powerful domestic forces that hinder these efforts. There are, for example, technology requirements for screening systems that are designed not to enhance security but to protect domestic manufacturers from competition. This is understandable but not acceptable. ICAO member states can currently opt out of security requirements by simply informing the ICAO that they are doing so, but they are not required to disclose which or how many requirements they are not following, how long they intend to be out of compliance, and if they have any intention to regain their former status. This ability is understandable, as states do not want to publicly disclose their vulnerabilities. Even restricting the information to member states is of limited value, given some of the connections member states have to terrorist groups. The difficulty is that carriers and passengers are not aware of the risk they face and are thus not able to make informed business and travel decisions.

One way to provide enforcement is to work with the insurance industry to provide adjustable rates for carriers and airports that are at various levels of compliance. Those in full compliance could get a reduction in insurance premiums, as long as they spend the savings on security. One can look at funding security through mechanisms such as infrastructure bonds as well.

The best way to defeat an asymmetric opponent is through information sharing. The international aviation community can provide an example through merging the efforts of ICAO and IATA in creating a joint security and intelligence center. This can leverage the laudable security efforts of both organizations with a central repository for the collection of information relating to terrorist and criminal interference with civil aviation. This will offer

the industry the opportunity to have both a tactical and strategic analysis capability addressing industry-specific needs. The individuals involved at this level are in middle management, and they need to have the skills to be not only security managers but potential leaders. Thus, they need to know not only the elements of their job but also the elements of broader security issues. Courses should include analysis, introduction to intelligence, threat and risk calculation, terrorist operations, and perhaps a "red teaming" module. These are all skills designed to help them to see various aspects of their job, understand the strengths and limitations of intelligence, and understand how to think about the field, but even more importantly, understand how the opposition is thinking.

The final level of analysis is the tactical level. This means dealing with the increasing threat presented by self-organized, self-radicalized, and self-operationalized cells, illustrated by the recent plots against Fort Dix and JFK. The general record against this threat is mixed. There are far more of these cells than of the larger groups, so the threat is greater, but the risk they pose is substantially less, as they are more limited in their access to funding and training and so their skills are reduced. They are more likely to conduct London– or Madrid–style operations rather than September 11–style operations. They still pose a potential threat to aviation, as it is relatively simple to hijack an aircraft, though rather more complicated to introduce an explosive device. As this trend is still emerging, the industry can use the breathing space to address existing weaknesses and develop a coherent, proactive strategy to deal with current and emerging threats.

**Recommendations:**

- Develop and implement a more coherent tactical response.
- Provide regular and realistic training.
- Assist stakeholders in developing economically viable responses across the system.

The two critical elements in the first recommendation are staff and training. The industry must be involved again in its own security. This may require the recruitment and training of the proper staff. It also requires that all staff members in the industry recognize their role in security and understand that they are empowered to act on their concerns. Staff must understand the operational environment and what can easily be turned into a defensive tool in the event of an incident. For example, if there is an attempt to hijack an aircraft, the cabin crew must recognize that they have a nonlethal weapon readily available to disrupt an attacker—coffee, ideally hot. Martial arts and other self-defense courses are useful, but unless the staff members attend regular sessions in the gym, the odds that a martial arts approach would work are limited. Using coffee or a food cart is much more effective in the disruption of an operation.

The examples above show why training is important. The understanding of how an event will take place and how to respond is not intuitive, but it can

be learned. It is believed that the first five to seven seconds in a hostage or other type of attack are the most critical. How an individual responds within that time frame may determine the outcome for both the individual and all involved.

Any security program must be economically viable. This seems to be common sense, but frequently it is not seen as such. As can be illustrated by the debate over protection against Man Portable Air Defense Systems (MANPADS), the economic cost can seem prohibitive when looked at from a threat and risk assessment perspective at least on the surface.

Just as important as the economic viability is the fact that any security policy must include input from the individuals who are going to have to implement it. They are the ones who will have to be able to understand the operational environment and the best and most efficient way to implement a new policy, as well as deal with the daily consequences of each new initiative.

This involves the line-supervisor or junior manager level. Training for them is very compliance oriented. They need to learn how to perform spot surveillance and to learn basic compliance and other rudimentary management skills. Much of this is already being accomplished in training, but unless it serves as a basic building block for a continuing career path, the training is divorced from the essential objective—creating a professional security staff.

Critically, the training industry needs to move away from its reliance on government. Undoubtedly, the above recommendations all rest on the ability of the stakeholders to gain access to high-quality information and intelligence. While cooperation between the government and industry is improving, there is still room for progress. One way to work around chokepoints within the system is to access information directly. About 95 to 99 percent of all information in the counterterrorism field is available through open sources. This includes both analysis and raw information, which can help create realistic training as well as the framework that the industry needs to evaluate its risk. The aviation industry does not need to invest in its own analytical capabilities; private sector firms and academic centers can provide information and analysis.

The threat and risk facing international civil aviation are constantly evolving. It is now common for groups to have an evolutionary life cycle of around six months, making response very difficult. The most effective security strategy is to develop a comprehensive, layered security structure. The critical components in maintaining a robust and flexible response are staff, training, intelligence, and, most critically, the will.

Terrorism and crime are human activities and thus can be reduced and perhaps prevented by human activity. Thus the move toward greater reliance on technology in all aspects of aviation and security may have a negative impact on security. Humans, with all of their limitations, are some of the best early warning detectors currently available. While the focus is on identifying the best personality type to work in security, it is essential to make sure that all staff members understand that they are empowered and expected to act in a potential security-related situation. This is not confined to security and other

ground staff. Ticket agents, sky caps, and everyone else in the industry need to be invested in the notion that security is an all points effort. The only way to protect civil aviation is to calibrate the response to the threat and risk posed by a given threat and allow humans to remain engaged in attempting to reduce the threat.

## NOTES

1. Deborah Feyerick and Phil Hirschkorn, Baggage, Cargo Handlers Arrested in Drug Probe: Smuggling Ring Accused of Importing 400 Kilos of Cocaine," CNN New York Bureau, November 26, 2003, http://www.cnn.com/2003/law/11/25/baggage.handlers/index.

2. Information from Dr. Rohan Gunaratna, during a question and answer session after the author's presentation at the Changing Face of Terrorism Conference, Singapore, 2003.

3. Robert Wall and David Hughes, "Missile Attack on DHL Jet Keeps Self-Defence Issue Bubbling," *Aviation Week and Space Technology*, November 30, 2003.

4. Malcolm Brabant, "French Police Probe Helicopter Attack," BBC Online, September 26, 2001, http://www.news.bbc.co.uk/2/hi/europe/1565588.stm.

5. The author has had the opportunity to address this program on several occasions.

6. David Gero, *Flights of Terror: Aerial Hijack and Sabotage since 1930* (London: Haynes Publishing, 1997), 10.

7. Ibid., 10–17, for motivations, and see Jin-Tai Choi, *Aviation Terrorism: Historical Survey, Perspectives and Responses* (New York: St. Martin's Press, 1994), 6, for the total numbers for the period.

8. Gero, *Flights of Terror*, 17–31, and Choi, *Aviation Terrorism*, 6. A total of 80 of the 91 hijackings or attempted hijackings had Cuba as a destination.

9. There were politically motivated instances before 1968. The hijacking of a Pan Am flight during the 1931 coup in Peru is the first example, although others argue that the hijacking of a Cuban internal flight by Raul Castro in 1959 was the first political hijacking.

10. See Choi, *Aviation Terrorism*, chapter 3, 14.

11. Ariel Merari, "Attacks on Civil Aviation: Trends and Lessons," in *Aviation Terrorism and Security*, ed. Paul Wilkinson and Brian Jenkins (London: Routledge, 1999), 13. The statistics from 1997–2004 are augmented by adding those from the FAA and Aviation Safety Network. The numbers are estimates, as neither definitions of hijackings nor reporting of them are standard.

12. Ibid., 20 and note 11, above.

13. For an excellent debate on the subject of when and why to claim credit for attacks, see "Terrorism and Claiming Credit: The Debate," *Terrorism and Political Violence* 9, no. 1 (Spring 1997): 1–19.

14. See Choi, *Aviation Terrorism*, chapter 1, 31, note 76.

15. The 1995 sarin gas attack on the Tokyo subway by members of the Aum Shinrikyo cult seemed to confirm all the trends identified by terrorism experts. A religious group used a weapon of mass destruction (WMD), in this case a gas, against a civilian target in order to inflict massive casualties. While most commentators point to this attack as the first example of the trend, I think the GIA attack covered in this section is actually the first.

16. Peter Harclerode and Mike Dewar, *Secret Soldiers: Special Forces in the War Against Terror* (London: Cassell, 2002), 507.

17. Ibid., 510.

18. Ibid., 509–15.

19. Simon Reeve, *The New Jackals* (Boston: University Press of New England, 1999), 90–91. *Bojinka* is Croatian for explosion, an apt name for this plan. Not only did the plotters intend to attack 11–12 American airliners, but they also planned attempt to assassinate Pope John Paul II and President Clinton on each man's visit to the Philippines. They planned to use aircraft to attack the site of the Pope's open-air mass, and to drop bombs on President Clinton's motorcade. There was also a preliminary plan for the September 11 attacks.

20. Rohan Gunaratna, *Inside Al-Qaeda* (New York: Columbia University Press, 2002), 6.

21. Introductory video for SATS training course.

# CHAPTER 3

# Air Transportation in Evolving Supply Chain Strategies

*R. Ray Gehani and G. Tom Gehani*

In the past 10 years, transportation by air has seen the fastest growth of all modes of transportation in the United States. Transportation costs account for a significant share of the cost of the goods sold in most enterprises and have a large impact on customer service and competitiveness of enterprises. During the age of regulated transportation in the United States (until the early 1980s), low-cost leadership logistics was the dominant driver for supply chain strategy. With deregulation reforms, the logistics service providers were forced to integrate multiple modes of transportation and migrate to more value-added bundling in their differentiated supply chain strategy. In this chapter, we review the significant role that air transportation plays in global supply chains and examine how air transportation emerged with the fastest growth of all modes of transportation, by volume and by revenue.

The role of air transportation in the supply chain has evolved significantly in the past three decades. The terrorist attacks on September 11, 2001, brought about additional strategic shifts in supply chain management and logistics practices. Prior to the deregulation of the U.S. transportation sector in the early 1980s, transportation service was a commodity. Competition in this service sector was driven by low-cost leadership strategies. There was little differentiation in price or performance across different transportation service providers. Transport deregulation gave birth to new differentiation strategies based on service functionality, modal diversity, flexibility, speed, capacity, scalability, and other factors.

A major new form of differentiated supply chain strategy has been that the air transportation service providers not only provide product movement but also facilitate product and parts storage. Goods in different forms, such as raw

materials, parts and components, work-in-progress subassemblies, and finished goods, need to be transported and stored at different stages in a supply chain, value-adding chain, and demand chain.

The efficiency and effectiveness of alternate transportation, logistics, and supply chain strategies have a significant impact on the overall productivity and the competitive performance of a global enterprise. In-transit inventory captive in the transportation system is usually inaccessible and must be minimized. The application of recent innovations in information technology, such as radio frequency identification devices (RFID) and the geographic positioning system (GPS), enhances the supply chain managers' access to in-transit inventory. The global supply chain managers must make decisions regarding temporarily storing certain inventory in a warehouse versus hiring a transportation service provider to move it. In global supply networks, managers may have to divert a shipment in midstream from its intended destination to a new, more pressing destination.

## TRANSPORTATION AND SUPPLY CHAIN STRATEGY

In this chapter, we discuss why the transportation logistics strategy for airfreight service providers must evolve and differentiate as a result of the U.S. deregulation reforms. With lower barriers to entry for new transport service providers and increasing threats of substitute modes of transportation, air service transportation providers must migrate to differentiate their service strategies rather than continue to rely heavily on their traditional low-cost leadership strategies, which were more effective under highly regulated and predictable markets.

Purchased supplies must be transported safely and swiftly from the places where they are generated (manufactured or mined) to the marketplaces where they are in demand. To ensure excellent customer service, adequate production in conjunction with optimum levels of inventories must be planned and provided. A global business demands that fluctuating and varying supplies match with uncertain demand. Transportation by different channels plays a key facilitating role in an effective deployment of inventories and sourcing of parts, components, and finished goods from worldwide suppliers.[1]

Supply chain logistics involves the management of inventory at rest and in motion. Either goods are flowing or they are in storage. The Council of Logistics Management defines logistics as that part of the supply chain that "plans, implements, and controls the efficient, effective flow and storage of goods, services, and related information, from the point of origin to the point of consumption, for the purpose of conforming to customers' requirements."[2]

Transportation service adds value by moving raw materials, intermediate goods, and finished products at the time and place these are needed. Transportation service providers offer a bundle of services for a price that depends on the quantity of goods moved, the distance moved, and the urgency with which these goods are moved over the desired distances.

### Transportation and Logistics Costs

Logistics costs are usually divided into transportation costs, inventory carrying costs, and administrative costs. Transportation accounts for the majority of the logistics costs.

In the current deregulated transportation markets, managing a supply chain logistics strategy involves balancing (a) the costs of appropriate levels of inventories, (b) the costs of manufacturing, and (c) the costs of transportation. Economies of volume scale and economies of transportation distances must be taken into consideration. Often, transporting 10,000 pounds costs just as much as transporting 2,000 pounds. Consolidation saves the cost of making several shipment orders, but it may increase the inventory holding cost. To avoid maintaining cost-incurring high levels of holding inventories, the cycle fill times must be reduced in conjunction with competitive logistics and transportation services. All these trade-offs favor the air transportation mode over other transportation modes for large volumes transported over long distances.

## ECONOMIC SIGNIFICANCE

The cost of supply chain logistics plays a significant role in the U.S. economy. The *State of Logistics Report*, presented annually by the Council of Supply Chain Management Professionals, monitors the transportation costs, total inventory-carrying costs, and total logistics costs. The logistics costs in the United States increased from $898 billion in 1998 to $910 billion in 2002, and to $1,180 billion in 2005.[3] This represents about 6 to 10 percent of the U.S. Gross Domestic Product (GDP; see Table 3.1). This share used to be much higher, at 16.2 percent, in 1981. This fall in the relative share of the cost of supply chain logistics in the U.S. GDP is due to (1) the deregulation of the transportation sector, (2) advances in technology, (3) the use of e-commerce, and (4) the streamlining of supply chains. In 2005 compared to 2004, however, there was an annual 15 percent increase of US$156 billion. This was due to (1) higher fuel costs, (2) supply chain off-shoring and outsourcing, (3) higher costs of security, and (4) shortages of rail capacity and truck drivers.

Of these, the transportation costs, including road, rail, sea, and air transportation costs, account for approximately 55–60 percent of the total logistics costs. The inventory cost is about half of that, or about 30–35 percent, and the rest is administrative cost.[4]

### Transportation Costs and Product Prices

Depending on the type of product, the transportation costs may account for as high as 40 percent of the price of a product. Bulky and low value products tend to have a higher ratio of transportation costs to their prices. In very high-value and low-weight items (such as bulk electronic parts and components), the transportation costs may be as low as 1 percent.

**Table 3.1**
**The U.S. Freight Bill by Transportation Mode (in billion US$)**

| | *Air Cost $B* | *Road Cost $B* | *Rail Cost $B* | *Water Cost $B* | *Pipe Cost $B* | *Other Costs $B* | *Total Transp. GNP Cost $B* | *U.S. GNP* | *Total/ %* |
|---|---|---|---|---|---|---|---|---|---|
| 1960 | 0.4 | 32.3 | 9.0 | 3.4 | 0.9 | 1.7 | 47.8 | 500 | 9.0 |
| 1970 | 1.2 | 62.5 | 11.9 | 5.3 | 1.4 | 1.8 | 83.9 | 1,046 | 8.0 |
| 1980 | 4.0 | 155.3 | 27.9 | 15.3 | 7.6 | 3.5 | 213.7 | 2,831 | 7.6 |
| 1990 | 13.7 | 270.1 | 30.0 | 20.1 | 8.3 | 7.7 | 350.8 | 5,832 | 6.0 |
| 2000 | 27.0 | 481.0 | 36.0 | 26.0 | 9.0 | 11.0 | 590.0 | 9,960 | 5.9 |

*Source:* Adapted from Robert Delaney, "Twelfth Annual State of Logistics Report," presented to the National Press Club, Washington, DC, June 4, 2001.

Often, a small effort in optimizing the transportation logistics strategy can result in significant cost savings and performance improvements. Cost minimization, however, is not the only criterion for choosing transportation channels and services. For example, supplies are procured and transported to meet certain production schedules and market demands. Transporting with low cost and long lead times may exhaust inventories, resulting in expensive plant shutdowns and finished goods stock-outs.

Similarly, reliability may vary significantly from one transport mode or company to another. A cheaper transporter may have a higher damage level, a higher level of lost shipments, and lower service reliability. Selecting such a transporter may add significant costs and other headaches.

The just-in-time lean supply chain management and global outsourcing demand that transporters should not only be reliable but that they should be faster with lower cycle times and more flexible. With smaller lot sizes and frequent set up changes, deliveries must be damage free in transit and without any delay. Deeper supply chains, with global sourcing, add pressure and complexity to timely transportation management.

All these disruptive external environmental and internal organizational factors favor a migration from a low-cost leadership strategy to the use of a service differentiation strategy for logistics transportation. In the next section we will discuss how deregulation reforms have motivated this shift in transportation strategy.

## DEREGULATION OF TRANSPORTATION LOGISTICS

Transportation played key strategic roles in the rise and fall of the great ancient civilizations of Egypt, India, Greece, and Rome. The River Ganges in India, like the River Nile in Egypt, provided the transportation needed to move agricultural produce along the plains of northern India and transformed the nomadic Aryan hunters into domestic agricultural farmers. The restricted

land transportation across high mountains of the Hindu Kush insulated the prosperous Indian subcontinent from westerners until the sea routes to India were opened by sea explorers like Vasco de Gama in the fifteenth century.

Due to the significance of the transportation sector to the economy of the United States, for over a century, the U.S. transportation sector was strictly regulated by government with closely controlled rates and delineation of allowable routes or geographical areas. These regulations were imposed at the federal, state, and local levels. In the 1970s, the U.S. government started gradually deregulating the transportation sector.[5] Whereas the economic regulations have been relaxed, the transportation sector must adhere to increasing safety and environmental regulations. These relate to working conditions, the transportation of hazardous and dangerous goods, and vehicle emissions.

Since the September 11 terrorist attacks on the World Trade Center and the Pentagon in 2001, the governments have imposed higher security standards at airports and seaports. The transportation regulatory policies are being continually assessed, on a day-to-day basis, as new assaults unfold. These have a significant impact on supply chain logistics and transportation operations management.

The U.S. government is deeply vested in the smooth functioning of the transportation network running its economic, food, and defense supplies—both nationally and internationally. Historically, national and state governments closely regulated the transportation carriers in terms of their geographic and business scope, by specifying the prices they could charge for their services. In the case of the U.S. Postal Service, the government directly provides the transportation service to its citizens instead of relying on private service providers driven by short-term profit.

For more than a century, the U.S. government regulators, guided by a policy of making transportation stable, economical, and accessible to all, invested heavily in building the transportation infrastructure, such as the Baltimore and Long Beach seaports, the Erie and Ohio canals, the interstate highway system, and airports.

Early transportation in the United States was dominated by the canal and railroad system. Individual states monopolized the legal rights within their borders, and there were no consistent interstate controls by the federal government. The U.S. Congress passed the 1870 Act to Regulate Commerce and created the Interstate Commerce Commission (ICC). At the dawn of the twentieth century, transportation carriers exploited their freedom by resorting to excessive profiteering, collusive price fixing, and anticompetitive practices. In 1903, the Elkins Act was passed, followed by the 1906 Hepburn Act, to establish federal regulatory control over pricing, particularly the maximum rate. The Hepburn Act had implicit jurisdiction over oil pipeline carriers. From early on, the Standard Oil Company developed pipeline transportation as a key mode competing with rail transportation. The 1910 Mann-Elkins Act enabled ICC to (a) examine and veto the proposed rates, and (b) remove discriminatory rates by service providers.

The 1920 Transportation Act expanded the power of ICC to include a reasonable minimum rate as well as the maximum rates. The 1887 Act was renamed the Interstate Commerce Act.

The post–World War I experience gave birth to the 1935 Emergency Transportation Act, which set standards for reasonable rates. In addition, as road transportation acquired a significant share of the total transportation market, the 1935 Motor-Carrier Act also expanded ICC regulation of the increasing numbers of for-hire motor carriers.

Water transport in the United States was loosely regulated by the 1940 Transportation Act under ICC for domestic water. Water transport in foreign trade and commerce with the noncontiguous states of Alaska and Hawaii was regulated by the Federal Maritime Commission (FMC).

The 1948 Reed-Bulwinkle Act allowed the transportation service providers to collaborate and jointly set prices, exempting them from the antitrust restrictions of the Clayton, Sherman, and Robinson-Patman acts.

To regulate the emerging airlines and air transportation sector, the 1938 Civil Aeronautics Act established a separate Civil Aeronautics Authority (CAA) to promote the sector's growth and ensure its safety. In 1940, the CAA was reorganized first as the Civil Aeronautics Board (CAB) and later as the Federal Aeronautics Administration (FAA). In addition, for the emerging aerospace sector, in 1951 the National Advisory Committee on Aeronautics was renamed the National Aeronautics and Space Administration (NASA).

Between 1970 and 1973, the U.S. rail industry started deteriorating. The National Railroad Passenger Cooperation (AMTRAK) was established by the 1970 Rail Passenger Service Act. To provide economic aid to seven major northeastern railroads facing bankruptcy, the Regional Rail Reorganization Act was passed in 1973. Under this act, on April 1, 1976, the Consolidated Rail Corporation (CONRAIL) started operating parts of these seven rail services. In 1976, the Railroad Revitalization and Regulatory Reform Act (4-R) and the Rail Transportation Improvement Act provided additional resources to AMTRAK and CONRAIL, and started deregulating the transportation sector.

## Deregulatory Reforms

In 1966, the Department of Transportation (DOT) was established to oversee the deregulation reforms in the U.S. transportation sector. The deregulation reforms were first introduced in air transportation: air carriers were encouraged to compete over prices, and the restrictions on setting up new air carriers were relaxed under CAB. The entry of and pricing by domestic cargo airlines, shippers' associations, and freight forwarders were deregulated by 1977. New rivals were allowed to enter the transportation sector provided they were willing, able, and fit to provide the promised services, rather than because of necessity or public convenience. The 1978 Airline Deregulation Act was passed on October 24, and CAB was shut down on November 30, 1984.

The road and rail transportation sectors were deregulated under the 1980 Motor Carrier Act (MCA) and the Staggers Rail Act (SRA).

The 1980 Motor Carrier Act (MCA) abolished the restrictions on the types of road carriers and the range of transportation services provided, in order to improve productivity and stimulate competition among road transportation service providers. ICC continued to oversee predatory pricing. This dramatically transformed the road transportation sector.

The 1980 Staggers Rail Act (SRA) deregulated the U.S. rail transportation sector, allowing vital freedom to the carriers to price competitively in their different market segments. The rail service providers were also free to merge or discontinue poor-performing rail segments. The 1994 Negotiated Rate Act helped further expand the rate freedom.

The 1994 Trucking Industry Reform Act (TIRA) deleted the mandate for the road carriers to file their rates with ICC. The 1995 ICC Termination Act abolished ICC, effective January 1, 1996, and appointed a small Surface Transportation Board (STB) to continue deregulation across all transportation modes and carriers.

### Interstate Inconsistency

Whereas there is a need for state-by-state consistency, often there was a conflict of jurisdiction in the United States between the federal and state agencies over transportation issues. In 1993, ICC ruled that if goods were shipped from out of state then the in-state shipments from warehouse to markets were also deemed interstate shipments. To avoid the additional cost burden of state regulation, the 1996 Federal Aviation Administration Authorization and Reauthorization Act was passed to facilitate a smoother flow of goods. The 1998 Ocean Shipping Reform Act deregulated the need to file tariffs with FMC.

## ADOPTING DIGITAL TECHNOLOGY INNOVATIONS

The innovations in digital technology and widespread use of the Internet gave birth to the 2000 Electronic Signatures in Global and National Commerce Act, which was designed to give digital signatures in electronic documents the same legal authority as signatures in legal paper documents. In 2004, the U.S. Department of Defense mandated that its 45,000 suppliers use RFID tags for all its supplies to the military.

The September 11 terrorist attacks in 2001 forced the United States to revamp its supply chain system and make it terrorism proof. Andrew Thomas in his 2003 book, *Aviation Insecurity*, has described how susceptible the U.S. aviation sector is to further acts of terrorism.[6] The 2001 USA Patriot Act was passed on October 26, to make sweeping increases in inspections and screenings at airports, seaports, and border crossings by road. This gave birth to the Customs-Trade Partnership against Terrorism (C-TPAT), a collaborative preventive program between government agencies and businesses.

Rampant globalization gave birth to new protective laws. The 2000 Byrd Amendment, also called the Continued Dumping and Subsidy Act, imposed fines on foreign firms suspected of underpricing and dumping their goods in the U.S. market and redistributed these fines to the complaining U.S. firms. This has resulted in a number of international lawsuits alleging U.S. violations of the guidelines set by the World Trade Organization, and has resulted in retaliatory duties on many U.S. goods by importing foreign countries.

Global competitiveness has also demanded a revision of the Jones Act, under Section 27 of the Maritime Act of 1920, mandating that goods shipped from one U.S. port to another U.S. port must be shipped by U.S.-built ships operated by U.S. crews and operating under a U.S. flag.

The aforementioned deregulatory reforms have had a significant impact on the U.S. transportation markets. Many transportation service providers are forced to differentiate their transportation logistics strategies to accommodate their new, dynamic, and fast-changing markets. To survive and to grow in these new markets, transportation service providers can no longer supply commodity-like services with a low-cost leadership strategy. They must increasingly examine and adopt innovative ways to differentiate their transportation logistics strategy.

The U.S. deregulation reforms have lowered the barriers for potential new entrants into the transportation services market and increased the intensity of the rivalry between existing transportation service providers. With higher threats of alternate substitute modes of transportation, the buyers of transportation services have gained greater bargaining power. With increasing pressure on overall potential profitability due to deregulation, U.S. transportation service providers are forced to differentiate their transportation logistics strategy by using multiple modes of transportation. In addition to using multiple transportation modes, they adopt innovations such as GPS, RFID, and other technologies ato improve visibility, reliability, and transparency throughout the multimodal transportation markets.

## FIVE COMPETING MODES OF TRANSPORTATION

There are five basic modes of transportation. These are water, rail, pipeline, road, and air—in the order in which these modes were introduced. Supply chain managers must carefully understand the key attributes of these different transportation modes, so that they can effectively mix and match the cost advantages and disadvantages of these modes to meet their customers' demands most appropriately. Given below is a more detailed description of the air mode of transportation. Then other modes of transportation are discussed in relation to air transportation.

### Air Transportation

Air transportation is the newest and the fastest-growing mode of transporting goods over long distances. Airfreight has the primary advantage of

**Table 3.2**
**10-year Growth in Gomestic Freight Shipments by Mode, Volume, and Revenue**

| | | *Air* | *Road* | *Rail* | *Rail intermodal* | *Water* | *Pipe* |
|---|---|---|---|---|---|---|---|
| 1996 | Freight vol. mil. tons | 11 | 6,549 | 1,682 | 135 | 1,044 | 1,443 |
| 1996 | Mode vol. share % | 0.1% | 60.3% | 15.5% | 1.2% | 9.6% | 13.3% |
| 1996 | Freight revenue $billion 13.3 | 346.0 | 29.6 | 5.6 | 7.4 | 18.3 | |
| 1996 | Mode revenue share % | 3.2% | 82.3% | 7.0% | 1.3% | 1.8% | 4.4% |
| 2006 | Freight vol. mil. tons | 24 | 8,242 | 1,979 | 211 | 1,137 | 1,600 |
| 2006 | Mode vol. share % | 0.2% | 62.9% | 15.0% | 1.6% | 8.6% | 12.1% |
| 2006 | Freight revenue $billion 29.4 | 446.0 | 35.1 | 8.7 | 8.1 | 20.2 | |
| 2006 | Mode revenue share % | 5.4% | 81.5% | 6.4% | 1.6% | 1.5% | 3.7% |
| 96–06 | Freight vol. change % | 118.2 | 25.9 | 17.7 | 56.3 | 8.9 | 10.9 |
| 96–06 | Mode revenue change % | 121.1 | 29.0 | 18.6 | 55.4 | 9.5 | 10.4 |

*Source:* Adapted from information in the ATA Foundation Third Annual United States Freight Forecast to 2006. *Trucking Activity Report*, American Trucking Association, Economics and Statistics Department, Alexandria, Virginia, 2007.

providing faster speed than other modes. Goods can be transported coast-to-coast by air in hours when it takes days by other modes.

Table 3.2 illustrates the 10-year growth, from 1996 to 2006, in U.S. freight transportation by different modes.[7] During this period, airfreight volume increased by 118.2 percent, and freight revenue increased by 121.1 percent. The corresponding increases for road transportation were only 25.9 percent and 29.0 percent respectively. The growth for rail was only around 18 percent in this 10-year period.

Airfreight is usually costlier than other modes of transportation, and it must be coordinated with trucks to provide the needed door-to-door service. The speedier and costlier air transportation is differentiated by integrating with field warehousing. Air transportation is limited by aircraft and airport availability, load size, and weight lift capacity.

For many years, air freight was transported aboard passenger aircrafts. Dedicated airfreight service was introduced by the launching of airfreight service providers such as Federal Express, DHL, Airborne Express, and the United Parcel Service. They initially transported high-priority documents.

Whereas there are approximately 400,000 miles of air routes, airfreight in the United States accounts for much less than 1 percent of intercity ton-miles. The airports and airways are developed and maintained by government and state authorities. The fixed costs include purchasing aircraft, cargo containers, and specialized handling equipment. These costs are relatively low compared to the fixed costs for the rail, water, and pipeline modes of transportation. Variable costs for air transportation are usually high due to rising fuel costs, user fees, and in-flight as well as ground-handling labor.

The products most suited to the air mode are usually of high priority, high value, time sensitive, and perishable. Examples include high-fashion apparel, cut flowers, fresh fish, and repair parts. Scheduled and chartered airfreight services are often used for some of these. Beyond certain distances, the air mode is particularly best suited for emergency deliveries. Medical supplies requiring narrowly monitored temperatures and other health care services may evolve as a lucrative segment of the market for air transportation.

## Road Transportation

The use of road transportation by automobiles has risen rapidly since World War II. Auto carriers, such as trucks, account for almost 80 percent of the transportation costs of U.S. enterprises today.

This mode provides door-to-door service, from short to long distances, and for products varying in size and weight. Trucks can transport large volumes at lower rates. Due to its flexibility in terms of door-to-door delivery and its ability to use a variety of roads, this mode is extensively used by just-in-time producers and suppliers. The United States has close to a million road miles.

In comparison to rail, road terminals require small fixed-cost investments. The facilities are often built and maintained by state governments. User and toll fees vary by usage. The variable costs for this mode, including the cost of drivers, fuel, and material handling labor, are high. High maintenance costs, the shortage of certified and reliable drivers, and safety in material handling are some of the challenges for this transportation mode.

Auto carriers prefer transporting high-value products over 500 miles, and usually prefer transporting products weighing less than 15,000 pounds for intercity shipments.[8]

Auto carriers are classified into (1) small-parcel ground carriers, (2) less-than-truck-load (LTL) carriers with less than 15,000 pounds, and (3) truck-load (TL) carriers with loads of over 15,000 pounds without intermediate stops. LTL carriers require consolidation. Some leading LTL carriers are TNT Freightways, Yellow Freight, Roadway, and Consolidated Freightways. LTL loads are usually carried over shorter distances than LT loads, and LTL loads cost more per unit weight. There are some specialty carriers such as Waste Management.

### Rail Transportation

Prior to World War II, transportation by rail dominated supply chain logistics in the United States. Today, compared to auto carriers, rail transportation is slower, more inflexible, and results in higher shares of losses and damage. The rail mode, however, has an advantage in transporting large tonnage over long distances.

Some intermodal transport service providers use a piggyback system, using truck trailers on flatcars (TOFC) and containers on flatcars (COFC). This helps them take advantage of long-distance transportation by rail and the door-to-door service of the auto mode. It also reduces damage and handling delays at terminals.

### Water Transportation

Water is the oldest mode of transportation. In the ancient times, manually powered sailing ships were used for international trade. In the early 1800s, sails were replaced by steam power, which itself was replaced by diesel motors in the 1920s. By the dawn of the twenty-first century, the United States had approximately 26,000 miles of inland waterways, not counting coastal and Great Lakes shipping.[9]

Most international transportation of goods uses deep-sea transport. The water mode is also pronounced on inland lakes and rivers. The biggest advantage of water transportation is that it allows the shipment of very large quantities.

Whereas water transport is inexpensive for large tonnages of commodities such as grain, coal, and others over long distances, the water mode of transportation is inflexible. It requires adequate handling equipment and access to convenient nearby waterways . Water transporters must team up with auto carriers for door-to-door transportation services using truck trailers or containers.

### Pipeline Transportation

Pipelines are primarily used in select cases for transporting gases or liquids. Pipelines account for the transportation of close to 60 percent of crude oil and natural gases. In the United States, approximately 180,000 miles were maintained by the end of the twentieth century.[10] Whereas pipelines demand high initial fixed investments for construction and right-of-way expenses, their variable costs are much lower. Pipelines operate round the clock and seven days a week. They are limited by relatively high maintenance costs and type of commodity (in gas, liquid, or slurry forms). No empty containers need to be returned.

## SELECTING THE AIR TRANSPORTATION MODE

Often, a buyer specifies the transportation mode by which the purchased goods are to be transported. The transportation service provider with multiple modes of transportation can offer alternative modes as well as a mixed-modal

**Table 3.3**
**Relative Ranking of Different Modes by Operational Attributes**

| | *Air* | *Road* | *Rail* | *Water* | *Pipe* |
|---|---|---|---|---|---|
| Speed | 1 | 3 | 2 | 4 | 5 |
| Reliability/dependability | 5 | 3 | 2 | 4 | 1 |
| Availability | 3 | 2 | 1 | 4 | 5 |
| Capability | 4 | 2 | 3 | 1 | 5 |
| Frequency | 3 | 4 | 2 | 5 | 1 |
| Total | 16 | 14 | 10 | 18 | 17 |

*Note:* Lower rank is better.

transportation service. When the Freight on Board (FOB) origin terms are used, the buyer has the legal right to specify the transportation mode. Good past performance leads to future repeat business.

Suppliers, producers, and buyers expect their air transport service provider to deliver goods fast, on time, in good condition, and at a competitive price. If a buyer has limited prior experience, and the transporter is well established, it may be a better strategy to let the transportation service provider choose the appropriate mode. In either case, the advantages and disadvantages of each transportation mode must be carefully weighed to arrive at the best mode mix, considering the needs of the enterprises involved.

Suppliers always expect their transportation service providers to keep them abreast of any significant events, such as shortages of planes or containers or excessive delays along the scheduled supply route. After selecting the mode of transportation, say, air, the supply manager must decide which transportation service provider to contract.[11]

Table 3.3 illustrates the relative ranking of the different transportation modes (such as air, road, rail, water, and pipeline) by their different operational attributes. Whereas air transportation is fastest, transportation by rail is ranked best for availability, and water is ranked highest for dependability and capability. Pipeline transportation, with its constant availability, is ranked highest by frequency. When the rankings for all the operational attributes are added together, air transportation falls in the middle: it has a better ranking than water and pipe transportation, but a worse ranking than rail and road.

## SUPPLY CHAIN PERFORMANCE SCORECARD FOR AIR TRANSPORT

We have developed a composite Supply Chain Performance Scorecard (SCPS) to assess: (a) the efficiency of the air transportation mode in comparison with other modes of transportation, and (b) to compare the performance of one transportation service provider with the performance of another.

This composite SCPS has four attributes, described and discussed below. Each transportation mode has its advantages and disadvantages. A transportation service provider, as well as its customers, must balance these advantages and disadvantages for each transportation mode and produce a portfolio with the most balanced performance attributes.

### Speed and Time Efficiency

Time is of strategic competitive significance for deep and complex global supply chains. Most suppliers provide estimates for normal delivery times using different modes. Customers also rely on their own actual past experiences to estimate delivery times. Speed refers to the time taken to transport and handle goods. Airfreight is the fastest mode. Road transportation can transport large volumes with greater flexibility. In the case of a distant location requiring two-way transportation, air transportation emerges as the most profitable mode.[12]

In addition to delivering at a fast speed, air transportation shippers, just like water shipping carriers, must be concerned with ensuring the complete security of goods at an affordable cost.

### Cost per Performance

Different transportation modes and service providers are evaluated by their respective costs for similar service performances. Most enterprises in regulated markets compete with rivals mainly with regard to their costs. Costs, however, are not limited to the prices at which the supplies are procured. Sometimes, the cost of acquiring supplies or putting these to use may be as significant as the price of the goods.

Third party logistics (3PL) providers are increasingly popular. They are differentiating themselves from their rivals by offering additional value-adding services such as inventory management, warehousing, and minor assembly operations. Further, the 3PL service providers may offer information systems that enhance the customer service levels of their clients.

Sometimes, clients select the transportation mode, the route, and the carriers for safe and on-time transportation of their goods within a specified total transportation cost.

### Reliability and Flexibility

Reliability or dependability refers to the degree of variance of a service from expected or promised delivery times. Two logistics service providers transporting goods between two identical locations may differ significantly in their attentiveness to their customers.

Air cargo carriers must retrieve and deliver goods as advised while minimizing damage, thefts, and accidents. A related aspect is transparency of the

global supply chain. Air cargo carriers must be robust, failure tolerant, and able to rapidly recover from disruption or failures. Failures and disruption in parts of a global supply chain should not cascade into a collapse of the entire chain. In addition, a global supply chain must be resilient in recovering quickly from disruptions or failures in normal supply chain operations. Resilience is determined by the design of the individual processes and the architecture of the overall global supply chain.

### Scalability and Responsiveness

This is the ability of a transport service provider to handle and meet the variability in transportation services demanded, such as larger load sizes or longer distances. It includes the availability of transportation services between specified distances, and the frequency with which these services are available.

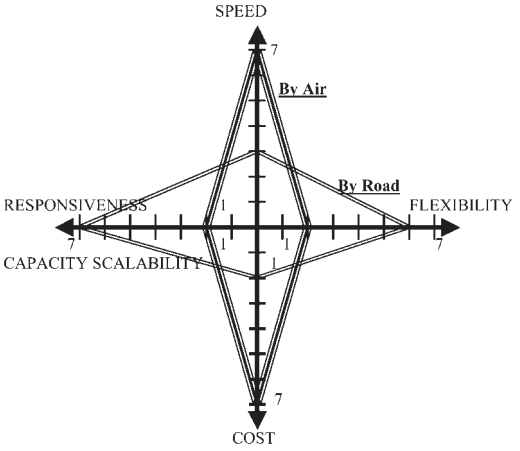
### Comparing Performance Portfolios

Clients must carefully assess all the four performance attributes (using simple or weighted mean criteria) for each of the five shipping modes and the different air transportation providers. Figure 3.1 shows a typical radar graph comparing the performance portfolio for air transportation with that for road transportation.

Some additional special criteria may determine the choice of a transportation mode or service provider.

The size of the goods to be transported or the types of containers required may limit the transportation modes or the transportation service providers.

**Figure 3.1**
**Comparison of Air and Road Transportation Modes**



There is a wide array of choices for transporting small packets. Aircraft transportation is not convenient or cost effective for bulk solvents and slurries. Goods flowing through global supply chains must be legal to transport and must be legitimately presented to the government authorities.

The transportation of fragile or sensitive goods (such as electronic components, biomedical supplies, and other items), may involve damage and claims on the logistics service providers. Clients must, therefore, select a safe transportation mode and select transportation service providers with sound financial health.

For some critical service requirements, such as those relating to extremely time sensitive goods, a privately owned or leased aircraft, as provided by the Federal Express Custom Critical Services, may be the most appropriate or the only strategic choice for a client. Depending on the frequency of such critical service requirements and capacity utilization criteria, outsourcing to a carrier may seem more advantageous and viable than owning a private aircraft fleet.

## AIR TRANSPORTATION AND EVOLVING SUPPLY CHAIN STRATEGIES

For most U.S. enterprises, transportation expenditures account for a significant share of their cost of goods sold (COGS). Transportation service also has a strong impact on customer service. With the rampant deregulation in the different transportation sectors, reviewed earlier, rapid serial innovations in information and telecommunication technologies, and intensified rivalry in globalized markets, air transportation and logistics must be carefully related to the overall strategic competitiveness of an enterprise.

Wherever permissible, air freight to be transported should be consolidated across different units of an enterprise, to increase the overall bargaining power with the service providers and to increase the economies of scale and scope for the enterprise. Long-term relational contracts with key trustworthy transporters help assure manufacturers and customers a steady stream of needed materials and information.

Leading enterprises such as Toyota, Wal-Mart, Dell, Amazon.com, and others have repeatedly demonstrated that a transportation and logistics strategy, carefully cross-functionally coordinated with other key functions such as production, warehousing, marketing, and accounting, can generate a sustainable and hard-to-beat competitive advantage and growth for long periods of time.

This study concludes that rising client expectations from transportation service providers and the overall balance of the portfolio of the Supply Chain Performance Scorecard for air transportation relative to other transportation modes have boosted the fast growth of air transportation in the United States during the past 10 years. Future growth and the role of air transportation in the evolving supply chain strategies of U.S. enterprises will, however, depend significantly on the rate at which aviation fuel prices and other variable costs increase in the next few years.

## NOTES

1. David Simchi-Levi, Philip Kaminsky, and Edith Simchi-Levi, *Designing and Managing the Supply Chain: Concepts, Strategies and Case Studies* (Boston: McGraw-Hill, 2008), 7–8.
2. Council of Logistics Management, *Definition of Logistics*, http://www.clm1.org.
3. R. V. Delaney and R. Wilson, *14th Annual State of Logistics Report* (Washington, DC: Council of Supply Chain Management Professionals, 2004).
4. Simchi-Levi, Kaminsky, and Simchi-Levi, *Designing and Managing the Supply Chain*, 7–8.
5. Donald J. Bowersox, David J. Closs, and M. Bixby Cooper, *Supply Chain Logistics Management* (Boston: McGraw-Hill/Irwin, 2002), 170–76.
6. Andrew R. Thomas, *Aviation Insecurity: The New Challenges of Air Travel* (Amherst, NY: Prometheus Books, 2003).
7. Bowersox, Closs and Cooper, *Supply Chain Logistics*.
8. Ibid., 343.
9. ENO Transportation Foundation. *Transportation in America* (Washington, DC: ENO Transportation Foundation, 1999).
10. Ibid., 44.
11. Michiel R. Leenders, P. Fraser Johnson, Anna E. Flynn, and Harold E. Fearon, *Purchasing and Supply Management*, 13th ed. (Boston: McGraw-Hill, 2006), 178.
12. Ibid.

# CHAPTER 4

# Tangible and Intangible Benefits of Transportation Security Measures

*Barry E. Prentice*

Transportation networks are the conduits through which economic activity takes place. This ranges from the simple task of day-to-day attendance at a job to international trade flowing through seaports. A shutdown of transportation facilities can have a significant effect on the economy. For a group wishing to make a significant statement, transportation provides a highly visible platform that is guaranteed to be widely reported. Aircraft disasters receive extensive media coverage whether or not terrorists are involved.

Virtually everyone uses transportation daily in one form or another. If making a statement and creating fear are objectives, then the transportation network is an ideal target. Moreover, public involvement in and ownership of transportation is pervasive. Infrastructure is mainly publicly owned or quasi publicly owned. Attacks on transit systems, port facilities, and airports allow the terrorists to claim they are striking at "the government."

Transportation networks are recognized as "soft" targets, and security has been increased worldwide. I categorize specific security programs into four broad groupings:

- improved inspection
- advanced notification
- law enforcement
- transportation security funding

Inspection programs include the screening of air passengers and freight. Baggage and cargo are passed through X-ray detection systems, and enhanced documentation is required for goods and persons. Related inspection measures

include advanced notification systems. U.S. Customs and Border Protection requires information on the contents of vehicles, trailers, and containers prior to arrival at ports of entry. Current regulations require 24 hours notice for ocean container entry and a minimum one-hour pre-arrival notification for trucks.

Law enforcement runs the range of activities from air marshals on commercial flights to more and better trained officers at all ports of entry. In the United States, grants are made to nonfederal organizations for the improvement of transportation security. Examples include the Transit Grant Security Program and support for the Highway Watch Program of the American Trucking Association. In Canada, the government announced the $80 million Transit-Secure program in 2006 in order to provide a government contribution to the costs of increasing security in the rapid transportation systems of the six largest urban centers.

Efforts to increase public security have direct costs to governments and the private sector. Federal, state, civic, and foreign governments bear the cost of hardening targets within a country. The senior levels of governments also bear the cost of ensuring the ability to trade. The U.S. Transportation Security Administration indicates that the costs of its air security increased from $1 billion in 2001 to $5.7 billion in 2003.[1] In Australia, aviation security measures costing $273 million were undertaken in 2002 and 2003.[2] (This cost was partially borne by the aviation industry and partly by the Australian government.)

For the private sector, security costs typically fall into the categories of increased administration costs, security equipment costs (for fences, cameras, lock passes, etc.), and the cost of waiting time. The U.S. Congressional Research Service indicated that security spending by the transit sector (rail and passenger bus) was $2 billion from 2001 to 2005.[3] The effect of U.S. border security measures on the Canadian trucking industry includes an estimated cost of between C$179 and C$406 million.[4]

The cost and effectiveness of transportation security programs is an ongoing debate. There has been substantially less analysis of the benefits arising from transportation security than analysis of the funding and private sector costs. The broad assumption is that the benefits of security are the protection of the public at large and the avoidance of negative economic consequences. This chapter focuses on the benefits of security measures and finds that the benefits are much more pervasive than is generally appreciated.

## TANGIBLE AND INTANGIBLE BENEFITS OF TRANSPORTATION SECURITY

In this analysis, I describe security measures using four categories:

- sovereignty protection
- terrorism prevention
- interdiction of illegal activities
- personal security

I classify the benefits of the security measures in each category according to the answers to two general questions: are the benefits the intended effect or a side effect of the activity, and can the benefits be quantified at market prices? This creates four groups. The intended outcomes are the direct benefits, while the positive spillovers of security measures are the inadvertent or indirect benefits. If these direct or indirect benefits can be measured using market prices, they are classified as tangible benefits. If market prices do not exist, then the benefits are considered to be intangible.

Sovereignty protection provides security related to foreign business and goods, financial transactions, communications, and travelers. Table 4.1 shows the benefits to the United States of sovereignty protection.

Compliance with Canadian border regulations facilitates trade, which results in higher levels of growth for business and ultimately a higher standard of living in the country. The reduction of smuggling and similar illegal economic activity provides benefits to both the government and the private sector. Illegally imported goods have the effect of undermining producers within the local economy. For example, the importation of counterfeit goods may undermine domestic production of high-end consumer goods. As domestic producers prosper, so do the government and the public at large through larger tax revenues.

Transportation is a conduit for the introduction of undesirable pests and diseases. Inspections at borders aim to prevent such occurrences that could undermine domestic production or domestic markets.

Sovereignty protection measures have two indirect tangible benefits. The requirement for electronic filing at the Canada/U.S. border allows disparate members of the supply chain to use similar information. This eliminates inconsistencies and increases productivity. Walton and Maruschek note that "electronic data interchange (EDI) is a technology that can help reduce the cost of supplier co-ordination by improving the ability of the purchasing manager to manage suppliers and by enhancing buyer-supplier relationships."[5]

**Table 4.1**
**Benefits of Sovereignty Protection**

| | *Direct benefits* | *Indirect benefits* |
|---|---|---|
| Tangible benefits | Compliance with Canadian regulations | Interoperability of the supply chain |
| | Reduction of smuggling and illegal activity | Expansion of trade |
| | Control of foreign disease and pests | |
| Intangible benefits | Enhanced sovereignty | Culture of obedience to law |
| | Fair immigration practice | |
| | Protection of flora and fauna | |

Security improvements can promote increased efficiency of cross-border traffic. The efficiency impact is large. A study related to the Asia Pacific Economic Cooperation (APEC) countries suggests that improving efficiency at ports where the below average APEC members are brought up to average would increase trade flows in the region by 9.7 percent, while simply improving the customs environment results in a 1.8 percent gain.[6]

Transportation security enhances sovereignty. The imposition of Canadian security regulations on ships operating in the Northwest Passage strengthens Canada's claim to the waterway and the northern landmass.

Improved sovereignty protection promotes the fair application of immigration policy. Illegal entry mocks the efforts of new immigrants who follow the regulations and the extensive waiting times required to gain lawful immigration.

Better security reduces the likelihood that foreign vessels will knowingly pollute Canadian waters. The social benefit of preserving Canadian flora and fauna does not have a market valuation, short of a tourist benefit, but there is a psychic benefit for citizens who are aware that the environment is not being harmed.

The creation of a culture of law obedience is an intangible indirect benefit of sovereignty protection. Canadian society has not become conditioned to black market activity. Once the public views certain regulations and laws as nuisances or irrelevant, an attitude of disrespect for the law can spread to other aspects of the culture.

Threats of espionage and aggression became more diffused with the end of the Cold War. Rather than military secrets, commercial espionage became the larger target. Rather than preparing for massive military strikes, preparing for the threat of aggression shifted to the identification of terrorist cells and the protection of strategic civilian targets. Table 4.2 summarizes the benefits related to terrorism protection.

Investors require larger risk premiums if terrorist acts threaten their investments. Palac-McMiken suggests that at the macro level, improved security can result in increased investment and higher levels of GDP.[7]

The tourism industry is another direct beneficiary of antiterrorism security. If country risk increases, tourism decreases. An example is the decline in tourism to Toronto with the sudden acute respiratory syndrome (SARS) outbreak in 2003.

**Table 4.2**
**Benefits Related to Terrorism Prevention**

| | *Direct benefits* | *Indirect benefits* |
|---|---|---|
| Tangible benefits | Reduced risk premiums<br>Maintenance of tourism<br>Higher property values | Development of security technology<br>Lower supply chain costs |
| Intangible benefits | Open border for U.S. trade<br>Better interjurisdictional coordination | Travelers feel safer |

Security measures increase property values for several reasons:

- Personal safety of the owners and employees ensures that people come to work and can be productive.
- Safer facilities attract more, better-trained employees.
- Loss of income through disruptions caused by terrorism is reduced.
- Consumer loyalty is encouraged by reliability of supply, which is a highly desirable attribute of customer service.

Technology that improves security creates tangible indirect benefits. For example, RFIDs that increase throughput speed as a method to limit opportunities for terrorists to infiltrate cargo movements provide the opportunity to lower supply chain costs. As noted by the World Bank, "new security protocols being deployed at ports, customs offices, and border posts around the world have the potential to streamline trade transactions as well as promote safety and security."[8]

Terrorism prevention also has a variety of intangible benefits. A critical benefit for Canada is maintaining trade with the United States. Trade with the United States is responsible for 52 percent of the Canadian GDP.[9] Over $1.8 billion in trade crosses the Canada-U.S. border every day. Although rising oil exports have recently affected the modal shares of transport, in 2001, 70 percent of this trade was moved by truck. In that year, more than 13 million trucks and 68.3 million personal vehicles crossed the Canada-U.S. border. The United States accounted for over 80 percent of all export earnings in Canada and provided two-thirds of Canadian imports.[10]

Improved terrorism prevention results in improved interjurisdictional coordination. Reducing the opportunities for terrorist acts improves efficiency and effectiveness. For example, search and rescue efforts can be mobilized faster and draw upon available resources that are closest to the need for help. Similarly, information sharing can help track criminal activity as well as that of suspected terrorists.

The indirect intangible benefit of terrorism prevention is that travelers feel safer. Security is essential for business and tourist travel. Business travel and trade will increase if business people feel safe at their destinations and so are willing to travel to take advantage of potential business opportunities. Tourists are unlikely to travel to destinations that they feel are unsafe.

Governments enforce laws and regulations to ensure transportation safety, prevent property damage, and block criminal activities. Illegal activities range from hours of service violations to the distribution of counterfeit aircraft parts and the movement of stolen goods. Table 4.3 provides the benefits related to the interdiction of illegal activities.

Improved inspection, enhanced security of facilities, and better monitoring of participants, such as truck drivers, all serve to decrease the frequency and severity of insured losses. The direct tangible benefit is the decrease in insurance premiums charged.

**Table 4.3**
**Benefits Related to the Interdiction of Illegal Activities**

| | *Direct benefits* | *Indirect benefits* |
|---|---|---|
| Tangible benefits | Reduced risk premiums<br>Lower staff costs<br>Crime does not pay so well | Lower supply chain costs |
| Intangible benefits | Better interjurisdictional coordination | Reduced managerial stress<br>Travelers feel safer<br>Culture of obedience to law |

Where conditions are perceived to be insecure and unsafe, workers seek higher wages. A current example is the high wages paid to the civilian contractors that are working in Iraq and the oil industry of South America. These extreme cases illustrate the link between security and labor costs. Weak security programs also drive up recruitment and training costs. High turnover rates require a continuous effort to sustain employment levels, and they weaken morale. Firm lose the benefits of experience and the loyalty of long-term employees, or what is sometimes called the "corporate memory." In short, weak security results in higher production costs.

With better security, less opportunity exists to sell stolen merchandise in the local market, export stolen property to other countries, or engage in money laundering. Interdiction of money laundering has focused attention on financial institutions that transfer funds internationally. As financial controls increase, criminals have turned to trade as a means of transferring illegally gotten funds out of an affected jurisdiction. One method is to overpay for imports or to undercharge for exports. The partner company sells the goods at the correct value and obtains "clean" money for the criminals. New data mining technology can identify imports and exports with invoice values that are inconsistent with market prices. This is leading to better interjurisdictional coordination.

The tangible indirect benefit of better interdiction activities is lower supply chain costs due to reduced theft losses and fraud. FIA International Research in, a report to the International Cargo Security Council, indicated that cargo theft worldwide was $50 billion in 2001 with $25 billion in the United States. Even a 10 percent reduction in theft due to improved security through interdiction would result in a $5 billion per year benefit.[11]

Better interdiction of criminal activity reduces stress for managers who are responsible for supply chain functions. If shipments are interrupted by theft or damage, extra management time must be spent expediting emergency supplies to maintain customer service. Higher staff turnover also increases managerial stress in the recruitment and training of new employees. Uncertainty in general forces management to maintain a higher level of preparedness than would be needed in a more secure environment.

**Table 4.4**
**Benefits Related to Personal Security**

| | *Direct benefits* | *Indirect benefits* |
|---|---|---|
| Tangible benefits | Reduced risk premiums<br>Fewer Employment losses, medical expenses, etc.<br>Computer security | Higher asset values |
| Intangible benefits | Improved crime prevention<br>Reduced stress and intergroup tension | Transference of fear to real risks |

Transportation security also provides benefits to individuals, as presented in Table 4.4.

As with the commercial supply chain, improved security reduces insurance costs for individuals. If homeowners or small business operators install alarm systems in their vehicles, their insurance premiums decrease. With improved security, insurance may be provided to individuals and businesses that were previously not insurable. Better security reduces the potential for harm to individuals and lowers medical costs and lost productivity during recovery periods.

Computer security is also affected by transportation security. As transportation systems become more dependent on computer-based technologies, and requirements for hardening these systems against attack increase, individuals subsequently benefit as the security technologies spill over.

Better security at the individual level has the indirect benefit of increasing asset values. In a secure environment, individuals and individual businesses are more confident about investing in property improvements and exhibit greater care over their surroundings. Problems like vehicle vandalism, arson, and theft can destabilize a neighborhood and cause some residents to relocate if petty crime becomes chronic.

Taylor and colleagues prepared a comprehensive analysis of the security of transit and rail systems. The analysis reports that "According to Federal Transit Administration data, an average of 279 people have been killed on or by public transit each year over the past decade. In addition, an annual average of 18,748 people have been injured on or by public transit over the same period.[12] Crimes ostensibly unrelated to transit use—such as being robbed or killed while waiting at a bus stop—would push these figures far higher." Protection from harassment and assault of this magnitude is a direct intangible transportation security benefit. Taylor and colleagues suggest that fear of crime is a deterrent to the use of public transit. Consequently, increased security measures could have a positive effect on ridership.

Another tangible benefit of improved transportation security is reduced stress and intergroup tension. People who feel secure about themselves, their

families, employees, customers, and suppliers feel less stress than people who are worried about their personal security and the security of others. The weaker the security provided, the greater the stress for all individuals in society.

An indirect intangible benefit relates to the differences in how individuals cope with risk. A low tolerance for risk can lead to extreme efforts to avoid perceived danger that are disproportionate to the probability of an incident. An example is hoarding by individuals as a result of a highly publicized risk event in another part of the country (or world). While individuals should be prepared for potential adverse events, a more stable and secure environment results in a lower transference of fear.

## SUMMARY AND CONCLUSIONS

The widespread perception of transportation security measures is that costs are significant and measurable, while the benefits of enhancing public security are general and indeterminate. This analysis suggests that transportation security measures provide a wide range of benefits to society, businesses, and individuals.

Based on positivist and normative concepts of risk, this analysis constructs an economic model in which social benefits curves react to changes in risk levels. The model outlines the effects of transportation security measures and the related welfare impact. Within the broad concept of social welfare, benefits can be classified as tangible and direct, tangible and indirect, intangible and direct, and intangible and indirect.

Few attempts are made to place a quantitative value on the benefits of transportation security measures. Some indications of magnitude are reported, but few specific measures are provided. Direct measurement of security benefits is plagued by the problems of assessing risk and uncertainty and the magnitude of an incident. House insurance is always a waste of money in retrospect, if the homeowner never experiences a claim. Some broader benefits of security cannot be priced because they are social and psychological in nature. These benefits can have an important value to society, but their quantification involves subjective measures.

It is tempting to declare that the benefits of security far exceed their cost, but this study is qualitative in nature. Quantification of security benefits is more difficult. In some cases data are not readily available, and no suitable measures of a pre- and postsecurity state exist. In some cases, however, quantification may be possible. I leave the challenge of data collection and analysis to others.

## ACKNOWLEDGMENT

This chapter is based on a report prepared for Transport Canada: *A Framework for Assessing the Economic Benefits of Security Measures That Impact on Transportation in Canada* (2006). The opinions contained in this paper are the

sole responsibility of the author and do not necessarily reflect the views of Transport Canada.

## NOTES

1. Kenneth M. Mead, *Aviation Security Costs* (Washington, DC: Transportation Safety Administration, U.S. Department of Transportation, 2003).

2. Economic Analytical Unit, *Combating Terrorism in the Transportation Sector.* (Melbourne, Australia: Department of Foreign Affairs and Trade, Government of Australia, 2004).

3. Peterman, David R. *Passenger Rail Security: Overview of the Costs.* Congressional Research Service, 2006.

4. FIA International Research Inc., "Contraband, Organized Crime and Threat to the Transportation and Supply Chain Function," International Cargo Security Council, September 2001, www.cargosecurity.com/ncsc/ images/contraband.pdf.

5. Steve V. Walton and Ann S. Maruschek, "The Relationship between EDI and Supplier Reliability," *Journal of Supply Chain Management* (1999): 30–35.

6. John S. Wilson, Catherine L. Mann, and Tsunehiro Otsuki, *Trade Facilitation and Economic Development*, Development Outreach, World Bank Policy Research Paper 2988 (July 2003).

7. Evanor D. Palac-McMiken, "Economic Costs and Benefits of Combating Terrorism in the Transportation Sector," *Asian Pacific Economic Literature* 19, no. 1 (2005): 60–71.

8. World Bank, *Global Economic Prospects 2004: Realizing the Development Promise of the Doha Agenda*, *2003* (Washington, DC: World Bank Institute, 2004).

9. DAMF Consultants Inc., *The Cumulative Impact of U.S. Import Compliance Programs at the Canada/U.S. Land Border on the Canadian Trucking Industry* (Ottawa: Transport Canada, 2005).

10. Ibid.

11. FIA International Research Inc., "Contraband, Organized Crime and Threat to the Transportation and Supply Chain Function."

12. Brian D. Taylor et al. *Designing and Operating Safe and Secure Transit Systems: Assessing Current Practices in the United States and Abroad* (San Jose, CA: Mineta Transportation Institute College of Business, San José State University, 2005.

# CHAPTER 5

# The Human Element in Aviation Security

*Mohammad Karimbocus*

Aviation security is about safeguarding civil aviation from acts of unlawful interference as defined in Annex 17 to the Chicago Convention on International Civil Aviation. Such unlawful acts can be

- internal, perpetrated from inside an aircraft or the aviation infrastructure;
- deliberate acts to sabotage aircraft or infrastructure or commit other illegal acts (including airside theft) from within an aircraft; airside; and
- external, where attacks against aircraft or infrastructure are carried from an external location using mortars, missiles, rockets, and so forth.

At the inception of modern civil aviation, it was widely believed that it would be very difficult to commit illegal acts inside the cramped cabin of an aircraft, especially when aircraft capacity was quite small. In those days, the importance of aviation security was influenced by this premise. Perhaps it was not foreseen that the world aviation network would expand so dramatically, and that larger and faster aircraft would be introduced, so this belief prevailed for quite some time.

The first serious contradiction to this mindset came in the early 1970s, with the first hijackings and attempts to illegally board flights, mainly by people seeking to go into exile. It can be said that modern-day aviation security took off as a result of those events. In fact, the international community, through the International Civil Aviation Organization (ICAO), responded with the introduction of Annex 17 to the Chicago Convention on international civil aviation. Over the years, there have been a number of enhancements to Annex 17, especially in light of security-related events.

While some of the amendments to Annex 17 may have had a proactive nature, a different, recurrent pattern can be observed when we analyze aviation security. This pattern has almost always been thus:

- An event occurs.
- A sort of hysteria ensues and a reaction follows in the form of more stringent measures.
- Risks of recurrence decrease.
- The security system goes into "cruise" mode, implying a relaxation of safety defenses.
- The wake-up call is in the form of the jolt delivered by the next occurrence.

This gives credence to the perception that aviation security is mostly in a reactive mode. We have to face the facts. All was going on normally on the security front when the first spate of unlawful interferences occurred in the 1970s. There was a reaction in the form of Annex 17, which meant more serious measures. Then as the situation "normalized," and the industry got down to its more pressing needs to cater for its sustained growth. Then came the events of September 11, 2001, and the industry went into utter shock. The event naturally resulted in a reaction in the form of even harsher measures. The London scare of 2005 followed, and the reaction was in the form of the now-famous acronyms of LAGs (global restrictions on the carriage of liquids, aerosols, and gels) and STEBs (sealed tamper evident bags). If this pattern prevails, we could be in for some further nasty surprises and even harsher reactions in the future. It is worth noting that more than a handful of U.S. airports recently failed security detection tests even after the implementation of the above measures.

This pattern has not been without consequences. First, it has caused ever-increasing annoyance to users. But, more importantly, at a time when the long-term sustainability of air transport is a matter of concern, all the security measures have seemed to overlook the cost implications for the industry.

The air transport industry has to bear the responsibility for this state of things. All the responses in the aftermath of security-related events have been decided upon by state authorities in their legitimate quest to protect populations and national and international sovereignty. Civil aviation has eventually had to toe the line and adopt the measures decided upon. One is tempted to think that the air transport industry has always adopted a fatalistic approach to aviation security.

In order to ensure its long-term sustainability, the industry must adopt a fresh approach to security, which should be from an angle other than that of enforcement and repression. The guiding factor should be the contributory role of aviation security toward the achievement of the industry's objective.

## THE BROAD OBJECTIVE OF AIR TRANSPORT

The objective of air transport is simply to provide safe arrival to the user. The achievement of this objective depends upon

- affordability and timeliness for the user;
- assurance of the safety of affected third parties and mitigation of adverse effects to them; and
- protection of the sovereignty of all states involved.

Civil aviation enlists the support of a number of stakeholders in the achievement of this objective. Each service contributes to the objective. These services operate in a global system and are in interconnected. This means that the ripple effect of any failure in one service would be felt all the way down the line. Therefore, aviation security should not be regarded in isolation. It does not operate in a stand-alone manner. And the evolution of aviation presents previously unknown challenges to all services.

## THE CHALLENGES TO AIR TRANSPORT

Air transport has been affected by a number of factors, and the effects have been felt by all support services, including aviation security. These factors include the following:

- Significant and unrelenting growth, which shows no sign of receding any time soon
- operators paying greater attention to costs (especially with regard to escalating fuel costs, arbitrary increases in user charges, and factors such as environmental taxes, carbon emission trading, etc.)
- better user awareness on quality of service
- more acute environmental awareness
- harsher competition for limited resources (land use, finance, etc.)

The fat days of aviation are dead and buried, and the industry should itself ensure its long-term sustainability. All support services should play their part responsibly in the achievement of the primary objective of safe arrival. Aviation security is no exception.

## THE TRADITIONAL VIEW OF SECURITY

Classical wisdom would argue that aviation security is sacrosanct and should not be fiddled with. There could not possibly be a limit on the resources needed. At the present time, such an attitude would be simplistic and a refusal to face up to the stark reality. The industry needs to reinvent itself in its quest for long-term sustainability. The limitation of resources applies to security as well as everything else.

In the wake of recent events, a number of measures have been implemented. These include the following:

- Preflight check-in times have been prolonged.
- Aircraft cockpit doors have been reinforced.
- Air marshals have been introduced in the United States.
- The Transportation Security Administration (TSA) has been introduced, also in the United States.
- Advance profiling of passengers has been introduced in some areas.
- Passenger "backtrack" after check-in is no longer allowed at most airports.
- Carriage of liquids and similar items is strictly controlled.

Whether these measures have really enhanced aviation security is open to debate. While the annoyance to the user has definitely increased, there have also been "collateral" effects. Examples of these include the following:

- Air marshals have been convicted for using their positions to indulge in illegal acts. At least one inoffensive passenger has been gunned down.
- A least one passenger has sneaked into the cockpit when cabin crew opened cockpit doors.
- Passenger profiling has resulted in aircraft being diverted after they have completed much of their flight, while the targeted passengers have eventually been found innocent.
- The combination of longer preflight registration times and the impossibility of backtrack presents the potential for unruly behavior by passengers left idle inside sterile zones for long periods.
- The cooling-off period for cargo is perceived as unproductive by many users.

Quite naturally, any new measure initially appears successful. But the increased annoyance to users and the cost implications gradually become evident. One thing is certain: all the measures implemented, and the sight of heavily armed personnel within airport premises, can be daunting to the average traveler. However, the odds are high that the very small fraction of the population that is intent on inflicting damage would be absolutely undaunted by these measures. In fact, such people are constantly on the lookout for any breaches in safety (including security) arrangements.

Dishearteningly, it seems that while only very few air travelers are intent on unlawful acts, the associated costs and annoyance are being passed on to all users.

## SHIFTING THE PARADIGM

Given the fragile state of the aviation industry, the sector will find it hard to accept the further addition of security measures. The financial costs and

strains on the system may be to much to bear. The onus is therefore on the industry itself to seek ways to reconcile costs with its primary objective, to get passengers to their destinations safely and on time. Aviation security is thus in need of major rethinking.

Most of the services that support civil aviation can be put into two categories, namely, those that are safety-sensitive, such as flight operations and air traffic control; and those that have a commercial bias. Aviation security, in contrast, has always been viewed as an enforcement and repression function. It is precisely this view that has to be broadened.

## BROADENING THE VIEW: SECURITY AS A CONTRIBUTOR TO OVERALL SAFETY

Just looking at the objective of air transport, we note that safety is the key word. But safety has to be reconciled with affordability and efficacy. Therefore, all services should be geared to contribute to the broad objective in the most efficient manner. Security should then be viewed from the perspectives of both safety and efficiency, in addition to its traditional enforcement and repression perspective.

There is no need to reinvent the wheel in the quest for the much-needed mindset change. The concept of safety management has been implemented to a large extent in areas such as flight operations, air traffic control, aircraft maintenance, and so forth. As the name implies, safety management is about optimizing the allocation of resources to achieve or even surpass preset safety goals. Whatever the principles of safety management have helped achieve in other services can also be achieved in aviation security.

As defined in *ICAO Document 9859*, "safety is the state in which the risk of harm to persons or damage to property is reduced to, and maintained at and below, an acceptable level through a continuing process of hazard identification and risk management." Therefore, when talking of safety, we are concerned with (the elimination or mitigation of) risk. Risks are either assessed proactively through hazard identification, or reactively in the light of occurrences and ensuing investigations.

Risks are an inherent component of any activity, and at the center of any activity, there is the human element. Therefore, the quest for safe and efficient aviation security inevitably leads to studying human performance, which is itself influenced by human behavior. The human element is the most flexible resource in any activity, but it is also subject to the influence of social, cultural, and other psychological factors that can significantly affect performance.

Security-related occurrences can largely be traced to inappropriate human behavior. In all the mishaps that have beset civil aviation over the years, investigations have shown that human error has been a major contributing factor. Therefore, the assurance of optimum operating conditions for the humans involved is pivotal in the management of risks.

## MANAGING RISKS

We can look at the risks that are of concern to aviation security as a service. The two major risks are

- the potential for unlawful acts during boarding, by people with ill-intent, arms, noxious substances, and so forth; and
- unauthorized access to restricted, sterile, or other protected zones.

Ideally, these risks should be zero at all times. But this is utopian. Therefore, it is necessary to identify and properly assess all risks, and implement ways and means to eliminate them or mitigate their effects to the best possible extent. The study of human behavior in aviation security operations, then, has to cater for two situations, the proactive and the reactive. On the proactive front, the objective is to identify all possible hazards (including those from previous occurrences) and implement elimination or mitigation measures. Reactive situations can be subdivided into two areas: response in the aftermath of contingencies and the implementation of measures to prevent a recurrence of such occurrences in the light of investigations and analyses.

## THE THREE STEPS

It can be said that any activity primarily consists of three steps:

- acquisition of data
- analysis of the data
- decision making and action based on the analysis and in line with the organization's objectives

Any mishap can then be traced to one or a combination of the above three steps. It may be the result of failure to acquire data, or inappropriate analysis and decision making. In aviation security, data is acquired through screening, access control, or profiling. Decision making is required regarding access to aircraft or restricted and protected zones. All information should be acquired and analyzed and effective decision making should be carried out at all times. The quest for this objective requires organizations to provide both physical and administrative safety defenses to enable operatives to achieve the targeted safety goal.

A security-affecting event is the result of an active or latent failure, and a failure is the consequence of breaches in safety defenses. Factors involving deficient human behavior need to be identified and addressed. In transport, including its security services, supervision in traditional terms is not possible, and operatives almost always have to make decisions on their own.

## FACTORS INFLUENCING AVIATION SERVICES

While it has always been seen from a repression and enforcement angle, aviation security has been affected by the same factors as all other services. The most relevant of these factors are

- an increased (and ever-growing) workload;
- progressively increased reliance on automation; and
- better customer awareness on the part of users.

The most striking effect of the relentless growth of air transport has been an increase in workload right across the whole civil aviation spectrum. This situation inevitably generates significant stress for the people involved at operational level, and there should be concern about the long-term occupational health of personnel exposed to such a situation in a sustained manner.

Security processing, whether it is screening or access control, involves a series of functions (normally in a given sequence) that lead to appropriate decisions to allow access to aircraft or other secure areas. A work overload situation implies the repetitive performance of the same sequence of functions over and over again. This inevitably leads to monotony and boredom. Boredom in turn fuels the temptation to cut corners. When such a temptation sets in at operational level, the security process is reduced to a ritual. The aggravating aspect of such a situation is that as long as there is no security scare, the corner-cutting attitude will continue, that is, until a significant event occurs. Investigations of some major accidents and incidents in aviation have shown that when departure from established practices and procedures was cited as a causal factor, operational personnel (whether flight crew or others) were found to have been regularly and knowingly cutting corners and had been departing from procedures well before the accident or incident took place.

Low workload situations can also potentially trigger significant mishaps. In fact, quite a few have occurred in slow periods. During periods of work underload, personnel are inevitably drawn away from their main assignment and gradually become engrossed in other preoccupations. Alternatively they may fall into lethargy. The result is again the weakening of safety defenses.

It would be grossly unfair to state that insignificant or inadequate attention has been given to the increasing workload issue over the years. Attention has long been given to automation. However, over the past two or three decades, phenomenal progress has been made in the information technology (IT) field, with the consequence that automation tools have been significantly enhanced in terms of quality and capability.

Automation has contributed enormously to civil aviation. Automation has greatly enhanced the capability to acquire and analyze data; and as artificial intelligence has developed, there has also been the possibility of "assistance" in decision making. automation has enabled the handling of ever-growing workloads by "taking over" the tedious and repetitive tasks performed previously by humans. The ability to repeatedly perform the same task without any

psychological effect has led to the elimination of some previously common errors. It would be impossible to think of an environment devoid of some sort of automation. For instance, baggage screening machines and metal detectors are standard at almost any airport. And the quality of these items of equipment is constantly becoming enhanced. Moreover, the major security-related occurrences of the recent past have spurred designers and manufacturers to aim for even greater heights in terms of the quality and capability of these tools.

The greatly enhanced quality of automation may lead us to think that the machine can ultimately take over from the human, who may take up an observer role. Designers and manufacturers are constantly hailing the extraordinary virtues of their machines, giving the impression that there will be no need of human resources. If this were true, the human could just sit back and relax while the machine does all the work. System designers often believe that the human element is very unreliable and inefficient and should be eliminated. Whatever the level of automation, however, the human element is irreplaceable.

## HUMAN FLEXIBILITY: THE GREATEST ASSET

While machines are limited in flexibility depending on the programming of their systems, the human element is the most flexible resource available. While the machine depends on the right program to ensure that the right action is taken at the appropriate time, the human has the ability to take the initiative in facing up to situations of uncertainty that can be difficult to predict. This is of special relevance in transport operations (including civil aviation), where all parameters are highly dynamic and constantly call for immediate decision making.

The advent of automation in aviation had a two-pronged objective, namely, to address the workload issue and to reduce human error. However, the success achieved has not been without adverse consequences. While there has been a definite enhancement of the capability to handle greater workloads, the introduction of the machine has generated a whole new set of challenges for the human worker. A wider competency base is necessary to appropriately manage machines that are growing both in capability and complexity. The human's workload has not been effectively reduced. The errors that occurred in manual systems have been drastically reduced. However, it would be wrong to state that risks have been eliminated. In fact, a totally new series of risks have come to the fore with automation. With the constant upgrading of the reliability levels of machines, overreliance on them may gradually set in, triggering boredom and complacency. Also, there is the possibility of a human-machine mismatch that may generate distrust and discomfort with the automation tool. All these factors have serious potential for breaching safety defenses. Rather than effectively addressing the issues of workload and potential for error, automation has simply relocated them.

## THE TARGET: OPTIMUM HUMAN PERFORMANCE

The issues of the ever-growing workload and recourse to automation are the biggest challenges in achieving the safe arrival of the user in a timely and affordable manner. Concern about the long-term sustainability of this industry gives added importance to these challenges.

Assuring the contributory role of aviation security in meeting the primary objective of the industry requires the fostering of optimum operating conditions for the human element. This can only be achieved by ensuring that the human maintains its cognitive capability at all times. Again, there is no need to reinvent. The study of operating conditions for the human worker has attracted attention for quite some time, especially in safety-sensitive services. Topics such as human factors, crew resource management, and emergency response have been widely studied in services such as flight operations and air traffic management. The idea is to adapt the results of such studies to the very specific environment of aviation security.

Every security organization has to pay regard to its human resources. Psychological screening and background checks are standard prerequisites for recruitment. Postrecruitment training is meant to impart the required level of operational and technical competency, and recurrent training is considered necessary for the preservation of such competency. We might think this is adequate. Major recent occurrences compel us to question this notion. Security operations are influenced by the same factors as all other services, namely, an ever-increasing workload and a gradually increasing use of automation. It has been proven that under such conditions, the ability to maintain cognitive capacity becomes difficult. Therefore, the creation and maintenance of conditions that preempt any impairment to the human's cognitive capacity are imperative. Significant work has been done in this respect in safety-sensitive services such as flight operations and air traffic management. Using these as a benchmark, sustained high-level human performance can be achieved in aviation security by

- addressing the issue of human factors in coping with the demands of aviation both during normal operations and during contingencies;
- fostering an environment of advance information flow;
- ensuring a broad training curriculum that would include, in addition to the usual operational and technical aspects, the development of the ability to be proactive;
- instilling a culture of collaboration with other services that support air transport, as well as within the aviation security organization itself.

## SHIFT OF FOCUS: FROM TECHNOLOGY TO HUMAN

In the early years of civil aviation, the prevailing mindset was that safety should be fostered through technological improvements, and the focus was primarily on the operational and engineering aspects. This was broadly

successful as can be demonstrated by the significant reduction in accident and incident rates. Also, in those days, it was widely accepted that frontline operational personnel had to bear responsibility for any safety-related occurrence. Put otherwise, whenever an accident or incident occurred, the question was *who* made the error. However, as time went on and increasing recourse was made to technology, human-machine relationships become more complex, and it was noted that the human was capable of getting around even the most sophisticated safety device. Thus, attention shifted from the engineering and technology aspects and became focused on the human element in the aviation system. It became evident that safety could not be fostered purely by addressing either technical aspects or human behavior. Investigations of some major safety events have clearly shown that preconditions did exist for their occurrence and could be traced back to organizational deficiencies that had not been addressed in time.

Attention to human factors is concerned with the fundamental capabilities and limitations of the human element and aims at creating and maintaining conditions in which the human's cognitive ability is not impaired by the stress associated with an activity. Possible sources of stress in air transport can be

- work overload;
- boredom due to work underload or the repetitive performance of the same functions for prolonged periods;
- inappropriate human-machine interactions;
- inadequate systems awareness through ignorance of the capabilities and limits of machines; or
- the occurrence of contingencies.

Human factors are not a new issue. In fact, attention to the operating conditions of the human element has always been prevalent. Criteria such as rostering arrangements, the physical nature of working environment, and so forth. have always been of concern. However, humans have had to adapt to changes originating from elsewhere, such as increased workload and recourse to automation.

All activities can be classified by importance and urgency. Hence an activity can be

1. important and urgent;
2. important but not urgent;
3. not important but urgent; or
4. not important and not urgent.

Research has shown that the best performance is obtained in category 2. In fact, proactive people will make every endeavor to shift all activities under category 1 to category 2 through anticipation or otherwise. The priority would

therefore be to enable security processing to achieve lower urgency levels most of the time by being highly proactive. This can be achieved by addressing a number of areas.

Aviation security training, like all services, is primarily concerned with the acquisition of proper operational and technical training. However, this needs to be supplemented by psychological training (aided by attention to human factors), so that personnel do not give in easily to emotion when the going gets tough. Recurrent training needs to be given renewed impetus, and simulation in this area should become standard. In fact, present-day IT capability can simulate the most extreme aviation security scenario. Exposing staff to such situations in a nonoperational environment would allow them to develop the capacity to stand up to any level of contingency. This has been proven in flight operations and air traffic control (ATC), and will definitely prove beneficial to security.

## FOSTERING ADVANCE FLOW OF INFORMATION: THE NEED FOR COLLABORATION

The starting point of any activity is the acquisition of information. Optimum performance is dependent on how far in advance such information is obtained and to what extent good use is made of it. The advance acquisition of information is not a new concept and is prevalent in a number of services in air transport, which may not all be safety-sensitive. For instance, preflight briefing is standard in flight operations, as is coordination in air traffic control. In the same way, airlines acquire data such as dietary preferences, seat allocation, and so forth, in good time to allow for adequate flight preparation. The idea behind this concept is that information is available well ahead of the actual performance of a function, thus ensuring proactive performance. In fact, the principle of advance data acquisition is used to some extent in aviation security in the form of selective profiling of travelers and through monitoring systems. The idea is to expand this concept to enable pertinent data to be obtained at every preflight step and conveyed to security well ahead of actual processing taking place. However, the implementation of a significant advance information system is dependent to a great extent on yet another issue, namely, the fostering of a collaborative culture in the aviation industry in general.

In practical terms, collaboration would imply the ability to achieve information interchange between the various service providers. To some extent, collaboration has always existed in civil aviation. However, as air transport has maintained its unrelenting growth, every service has had to deal with ever-growing workloads, and it has become extremely difficult to maintain collaboration (though, paradoxically, it is required more than ever before). When we survey airport operations, it becomes clear that no one pays much attention to knowing what the other stakeholders are doing. For instance, it is widely believed that aviation security is the sole responsibility of the

organization providing the service. On the contrary, a decent knowledge of security could be helpful in preemptively detecting the potential for unlawful acts. Putting in place a dynamic and pragmatic collaborative culture involving all the various stakeholders would involve a means of information interchange that would not generate additional workloads in an already stretched environment. This would then have to be complemented by the notion of "know your neighbors."

For security, this would imply the enlargement of the locus of knowledge and the locus of data, though the locus of control would primarily rest in the security organization. These enlargements would improve the detection of the potential for illegal acts well ahead of security processing. They would make available a broader pool of resources in the detection, avoidance, and mitigation of security threats, with a clear gain in effectiveness and efficiency. There are similarities here to crew resource management (CRM), which is about the pooling of resources on flight decks in the quest for safe operations, especially during contingencies.

## REACTING TO CONTINGENCIES

Human behavior is not confined to the proactive assessment of security (or more broadly, safety). Since zero risk is an elusive target, errors are bound to happen from time to time. Error management involves setting three lines of defense, namely

- the avoidance line, where proactive assessment and addressing of errors are made;
- the error-trapping line, which means the isolation of errors just as they are to happen; and
- the mitigation line, which requires action to mitigate the consequences of errors that have already happened.

As part of a broad safety management drive, every organization should have a certain level of preparedness to face emergencies. This is usually in the form of an emergency response plan (ERP), which is a widespread regulatory requirement nowadays. The ERP normally lays out the appropriate actions to be initiated in the aftermath of a safety-related occurrence, and personnel are expected to be well trained in these actions. A review of most ERPs would lead to the assumption that humans have been adequately prepared to respond in the event of a safety-related event. However, this is not the case. An emergency is not a normal condition and the sheer size and consequence of an aviation accident or incident may prove overwhelming to the humans involved. Also, it has been shown time and again that when faced with an emergency, humans will always tend to shift attention from their primary assignment and concentrate more on the situation at hand. Under these conditions, it will be very difficult to preserve cognitive functions, and mitigation efforts can also be adversely affected. And, paradoxically, aggravating

circumstances have been generated by the substantial success on the safety front over the years. In fact, the lowering of accident and incident rates has resulted in reduced exposure to contingencies, resulting in lower preparedness.

## HUMAN EMPOWERMENT: THE ONLY WAY FORWARD

The empowerment of the human element is therefore of primary importance in the quest for efficient and effective aviation security. It is imperative to develop both the proactive and reactive capacity of the personnel. The achievement of such a capacity in human resources depends on attention being paid to a number of issues.

First, it is necessary to create the conditions conducive to the proper conduct of security operations. This involves addressing human factors issues, including the interfacing between the human, the machine, and the environment, and the ability to operate efficiently under constrained conditions.

Second, there is a need to pay renewed attention to training. In addition to the need to provide appropriate technical and operational knowledge, there is also the need to build leadership skills and mental strength. Perhaps security personnel should be licensed, with a focus on the maintenance of relevant competency levels at all times through recurrent training including regular simulation. The benefits of simulation are well known in the fields of flying and air traffic control. Extending this concept to aviation security appears to be a natural step in the drive to enhance human performance. The provisions of ICAO Annex 1 could provide a benchmark for licensing, or else they could be extended to include aviation security among the nonflying activities subject to personnel licensing. As part of aerodrome licensing, regulators do assess aviation security, and security audits are prevalent worldwide, mainly with regard to adherence to Annex 17. The idea would be to enlarge the scope of such audits, and also adopt the licensing of security personnel as a standard.

Third, a profoundly collaborative culture should be fostered within the air transport industry. In practical terms that would mean the ability to exchange information and the willingness to do so. Some might express reservations on the basis that workload increases would not allow time for exchanging information with other services. However, we live in a world where the high capability of IT is well known. This can take care of the advance capture, exchange, and processing of large volumes of data if the right environment and network are created. As a catalyst for this collaborative culture, the principle of "know your neighbors" should also be adopted. From the aviation security perspective, this attitude could be ensured by certifying personnel from other stakeholders who are of direct relevance to security organizations. This certification would be an assurance of sufficient general knowledge of aviation security.

Another measure, which is in line with safety management principles and is applied to some extent in some organizations is the adoption of a just culture

regarding security mishaps, with a culture supporting voluntary reporting and in which investigations are meant to prevent recurrence rather being than solely focused on sanctions against culprits. In fact, aviation is moving away from the traditionally punitive focus of occurrence investigations and is getting more focused on the pedagogical value of these investigations as a risk management strategy.

## FINAL THOUGHTS

Since the early 1970s, significant emphasis has been laid on aviation security, and attention has grown substantially since September 11. Quite legitimately, authorities (whether local, national, or international) have shown serious concern in the aftermath of major events and have reacted accordingly by strengthening security measures. However, these measures have come at a high cost and with increased constraints to both operators and users. Also, the efficacy of such measures can be questioned when we note a recurring pattern that generally culminates in another occurrence. Therefore, it is imperative that a paradigm shift be made regarding aviation security. This would require moving away from the narrow-minded view of enforcement and repression, and thinking of aviation security as a contributor to the broad objective of air transport, which has to do with safety, timeliness, and affordability. This would require security services to operate using the principles of contemporary safety management. And the most appropriate path would be to adopt a generative safety culture where awareness of safety, business strategy, and sustainability permeates an organization. In addition to having a very significant proactive effect, this culture would also require risk assessment processes, and more generally, operational audits (which are inherent to most security organizations) to be focused on further empowering the human element rather than just laying blame.

Every stakeholder must understand that no service operates in isolation in aviation. As such, each and every service is required to participate in the achievement of the objective of the user's safe, timely, and affordable arrival. And the question of affordability inevitably points to sustainability. Aviation was already in the midst of serious concern for its long-term sustainability when the major security events and scares occurred. The present-day focus is on such aspects as environmental taxes, carbon emission trading, capacity constraints, and so on; and more stringent security measures have added to the prevailing concerns. There will most certainly be other issues that will bear on civil aviation in the future.

One striking fact is that the authorities have, in their legitimate quest for overall protection against unlawful acts, resorted to police and other enforcement agencies to implement security measures, though many organizations have lately resorted to massive recruitment. While the "muscle" provided by these agencies is important, and enforcement and repression capacity should be available, the onus should be on the air transport industry to restrict

recourse to them to extreme conditions only. Here an analogy could be made to the regulatory requirement for the existence of rescue and firefighting services in aviation. The aviation industry has the primary obligation to allay the security concerns of the authorities and all other parties. This can only be made possible through the application of safety management principles to security. Given the pivotal nature of the human element, the success of aviation security lies with the qualitative enhancement of the human capital.

## REFERENCES

ICAO Annex 1 to the Personnel Licensing Convention on International Civil Aviation (Montreal: ICAO, 2006), 10th ed., including amendment 168, Chapters 1, 4.
ICAO Annex 17 to the Security Convention on International Civil Aviation (Montreal: ICAO, 2006), 8th ed.
ICAO Document 9859: Safety Management Manual. 2006. 1st ed. Chapters 4 to 11, 13.
ICAO Human Factors Digest No. 8. Chapters 3, 5, 1985.
ICAO Human Factors Digest No. 10, 1985.
ICAO Human Factors Digest No. 11. Chapters 1 to 5, 1985.
ICAO Safety Management Manual Doc 9859 AN 1760 (Montreal: ICAO, 2006), p. 7.
Bechet, Thomas P. 2002. *Strategic Staffing* Chicago: Amacom, chapter 14.
Billings, Charles. "Issues Concerning Human-Centered Intelligent Systems." Presentation to University of Illinois Champaign–Urbana, September 1995.
Dekker, Sidney W. A. 2004. *Ten Questions about Human Factors.* London: CRC Publishing.
Forster, Nick. 2005. *Maximum Performance.* New York: Edward Elgar Publishing. Chapters 2, 4.
Goodwin, Paul, and George Wright. 2004. *Decision Analysis for Management Judgement.* New York: John Wiley & Sons. Chapters 2, 5, 11.
Helmreich, Robert L., Ashley C. Merritt, and John A. Wilhelm. 1983. *The Evolution of Crew Resource Management Training in Commercial Aviation.* Austin: University of Texas Press.
Lewis, David, Dr. 1999. *10-Minute Time and Stress Management* (London: Piatkus Books).
Molino, Louis N., Sr. 2006. *Emergency Incident Management Systems.* New York: Wiley Interscience. Chapter 2.
Rothwell, William J. 2003. *Beyond Training and Development.* 2nd ed. Chicago: Amacom, Chapter 2.
Schultz, Duane, and Sydney Ellen Schultz. 2001. *Psychology and Work Today.* 8th ed. New York: Prentice Hall, Chapters 6, 7, 8, 10, 12, 13.
Smith, Geoff. 2004. *Leading the Professionals: How to Inspire and Motivate Professional Service Teams.* London: Kogan Page. Chapters 1, 6.

# CHAPTER 6

# The International Civil Aviation Security Program Established by ICAO

*Moses A. Alemán*

Following the adoption of the Convention on International Civil Aviation in 1944, the world experienced a remarkable degree of safety, regularity, and standardization through vast technological advancements in the area of aviation safety, an achievement that is unparalleled in other modes of transportation. However, during the past four decades a new type of danger to international civil aviation has emerged, one that was not foreseen when the convention was drafted and signed. During this period, commercial aviation has become a victim of violent human acts against the safety of commercial flights in the form of unlawful seizure of aircraft, acts of sabotage, and the use of commercial airliners as weapons of mass destruction.

These violent criminal acts are a worldwide problem and are not limited by geographical or political boundaries. No airline in the world is immune to such acts. In response to this threat, the Council of the International Civil Aviation Organization (ICAO) responded by sponsoring international conventions dealing with aviation security matters and by adopting international standards and recommended practices designed to prevent acts of unlawful interference with international civil aviation.

"South American Getaway" is the title of the second chapter of David Phillips's *Skyjack—The Story of Air Piracy*. This chapter is an account of the world's first unlawful seizure of an aircraft, which occurred in Peru in 1931. It describes the experiences of Byron Rickards, the first pilot to fall victim to an aircraft hijacking. Rickards was the pilot of a Panagra Airways Ford trimotor flying over the Andes Mountains carrying the mail when the aircraft was seized by revolutionaries. Thirty years later, in 1961, Rickards became the first pilot to be hijacked twice. By then Rickards was flying jetliners in the

United States for Continental Airlines, in an era in which aerial hijacking was becoming common.

## EVOLUTION OF ACTS OF UNLAWFUL INTERFERENCE

Beginning in 1958, a few sporadic incidents of aircraft hijackings occurred in various parts of the world. That year, two Cubana Airlines DC-3s were hijacked in Cuba and were taken to a clandestine location in the Province of Oriente. In 1961, the first U.S.-registered commercial aircraft was hijacked in the United States and was taken to Cuba. Between 1961 and 1967 a total of 12 aircraft seizures occurred in the United States, but aircraft seizure was not yet considered a serious threat to commercial air transportation.

Suddenly, in 1968, a dramatic increase in the unlawful seizure of aircraft began to develop, in the United States as well as in the Middle East. The United States alone suffered 22 aircraft hijackings in 1968, and according to U.S. Federal Aviation Administration (FAA) statistics, the period between 1968 and 1972 became the worst period in aviation history for air piracy incidents. Hijackings of U.S. registered aircraft during the period averaged 29 per year. The worldwide statistics for the same period recorded an average of 40 unlawful seizures per year, the majority for political reasons and a few with criminal motives such as extortion or involving fugitives escaping from authorities.

### The First Actions Taken

In 1968, at the ICAO Assembly held in Buenos Aires, Argentina, the Cuban delegation, led by their deputy minister of transportation, appealed to the president of the ICAO Council to do something to stop the hijackings. This resulted in a resolution being adopted by the assembly. At the same time, action was instituted in the United States with the establishment of the FAA Anti-hijacking Task Force in 1969.

### Incidents in the Jordanian Desert

On September 6, 1970, several dramatic incidents of aerial piracy occurred almost simultaneously. This caused a huge reaction throughout the world, resulting in the most significant development of antihijacking measures and procedures. These events included the following:

September 6, 1970: A TWA B-707 was hijacked by two Palestine Liberation Organization (PLO) men who had boarded in Frankfurt, Germany. The aircraft was taken to Dawson Field, Jordan, where the empty aircraft was blown up on September 12, 1970.

September 6, 1970: A Swissair DC-8 was hijacked by two PLO men who boarded it in Zurich, Switzerland. The aircraft was taken to Dawson Field, Jordan, where the empty airliner was also blown up on September 12 1970.

September 6, 1970: A Pan Am Airlines (PAA) B-747 aircraft was hijacked by three PLO men who had boarded the airplane in Amsterdam, Holland, and who were later joined by seven other hijackers in Beirut. This aircraft was taken to Cairo, Egypt, where the empty aircraft was blown up on September 7, 1970.

September 6, 1970: An El Al B-707 flight from Tel Aviv to New York was nearly hijacked by a PLO man and woman. The male was killed and the female was overpowered. The flight was then aborted and landed safely in London, England.

September 9, 1970: A BOAC flight from Bombay to London was hijacked by three PLO men who had boarded it in Bahrain. The aircraft was taken to Dawson Field, Jordan, where the empty aircraft was also blown up on September 12, 1970.

## Initial Aviation Security Measures

In September 1970, following these events, U.S. President Richard Nixon issued a White House statement announcing special actions, including the immediate assignment of armed sky marshals on U.S. commercial airliners and the establishment of the FAA Office of Air Transportation Security, which immediately assumed the duties of the antihijacking task force. The air marshals were utilized by the United States from 1970 to 1972. The program ended when a task force study led to the issuance of new federal aviation regulations (FARs) on aviation security matters. This resulted in the development of a "profile" screening system to be used on a voluntary basis by the airlines. The use of FAA security officers and metal detectors was also initiated. However, since the screening of passengers was on a voluntary basis, only a few airlines opted to utilize such procedures.

Meanwhile, the international aviation community also responded, in the form of the ICAO's sponsorship of new international conventions dealing with aviation security matters. In addition, the 1970 bombing of a Swiss Convair 990A passenger aircraft en route from Zurich to Tel Aviv, in which 47 persons died, resulted in an extraordinary session of the ICAO Assembly. An ad hoc group of security experts from five nations was directed to quickly develop a security manual to provide some preventive security guidance to ICAO Member nations.

The Convention on Offenses and Certain Other Acts Committed on Board Aircraft, signed in Tokyo, Japan, in 1963, had just entered into force on December 4, 1969, but this early international instrument was insufficient to cope with the problems being faced. Thus, the ICAO Legal Bureau set out to prepare international agreements dealing specifically with the unlawful seizure of aircraft (The Hague Convention of 1970) and dealing with the sabotage of aircraft and aviation facilities (Montreal Convention of 1971). Further explanations of these international instruments are provided later.

At the same time, the United States abandoned the idea of eliminating hijackings in the air with air marshals and instead issued federal aviation regulations requiring the establishment of airport security programs and airline security programs in 1972 and required mandatory preboarding passenger screening effective January 6, 1973.

At ICAO, the newly developed ICAO Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference (Doc. 8973—Restricted) was issued in 1971. This was the only technical guidance available to ICAO contracting states at the time on preventing hijackings and sabotage of aircraft.

## DEVELOPMENT OF THE ICAO CIVIL AVIATION SECURITY PROGRAM

A combination of the 1973 U.S. requirement of 100 percent preboarding screening of passengers and carry-on items, the end of the Vietnam War, and the signing of a treaty by the United States and Cuba caused a dramatic decrease in the number of hijackings. The average of 29 per year from 1968 to 1972 went down to no hijackings in 1973 and only one in 1974.

This encouraged the Council of ICAO to adopt international standards and recommended practices to safeguard international civil aviation against acts of unlawful interference. Thus, the ICAO Council action in pursuance of Assembly Resolutions A17–10 and A18–10 resulted in the adoption of the first edition of Annex 17 to the Chicago Convention on March 22, 1974.

The implementation by ICAO contracting states of the new international standards in their respective airport security programs and airline security programs served to temporarily deter and prevent successful attacks against commercial airliners. It was not until 1976 that the United States suffered its next successful hijacking of a commercial airliner.

There are two aspects of the International Civil Aviation Security Program that are a result of ICAO conventions, both of which play important roles in responding to the threats against commercial aviation on an international basis. These are the judicial aspects and the technical aspects.

### Judicial Aspects of the ICAO Civil Aviation Security Program

The legal program of international civil aviation security consists of international conventions and agreements dealing with aviation security matters. An international convention is an agreement between parties in the form of a legal document which can become the basis for international law. The international conventions described below represent the judicial aspects of the International Civil Aviation Security Program established by ICAO.

*Convention on Offences and Certain Other Acts Committed on Board Aircraft* (known as the Tokyo Convention because it was signed in Tokyo, Japan, on September 14, 1963, and came into force on December 4, 1969). This convention provides "that the state of registry is competent to exercise jurisdiction over offenses committed aboard an aircraft when it is in flight, on the surface of the high seas, or in any other area outside the territory of any state." The convention applies only "to offenses committed by a person who is on board

the aircraft, thereby excluding acts or offenses committed by persons such as saboteurs who remain on the ground." Article 11 deals with the unlawful seizure of aircraft and obligates states to permit the passengers and crew of a hijacked aircraft to continue their journey as soon as practicable and to return the aircraft to its rightful owner. (This convention called for ratification by 12 member states before entering into force.)

*Convention for the Suppression of Unlawful Seizure of Aircraft* (The Hague Convention, also known as the Hijacking Convention, signed in The Hague on December 16, 1970, came into force on October 14, 1971). The Hague Convention defined the unlawful seizure of aircraft "as a separate offense." It obligates states "to punish or to extradite offenders and also provides for concurrent jurisdiction over the offenses covered and makes these offenses punishable by severe penalties (that is, the state of registry, the state of operator, and/or the state in which the aircraft next landed with the offender still on board)." (This convention called for ratification by 10 member states before entering into force.)

*Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (Montreal Convention, also known as the Sabotage Convention, signed in Montreal, Canada, on September 23, 1971, came into force on January 26, 1973). This treaty deals with sabotage and armed attacks against international civil aviation facilities and creates the same obligations for the states with respect to these offenses as The Hague Convention created with respect to hijacking (punishable by severe penalties, extradition, jurisdiction, and entering into force after ratification by 10 member states).

*Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (signed in Montreal, Canada, on February 24, 1988, entered into force on August 6, 1989). This protocol is supplementary to the Montreal Convention and specifies "that the convention and the protocol shall be read and interpreted as one single instrument. It amends the definition of the offense to include performing an unlawful and intentional act of violence against a person at an international airport that causes or is likely to cause serious injury or death, or an offense that destroys or seriously damages the facilities of an international airport or aircraft located there but not in service, or disrupts the services of the airport if such an act endangers safety at that airport." (This convention also required 10 member state ratifications to enter into force.)

*Convention on the Marking of Plastic Explosives for the Purpose of Detection* (signed in Montreal, Canada, on March 1, 1991, entered into force on June 21, 1998). This convention requires "each state to prohibit and prevent the manufacture of unmarked plastic explosives in its territory. Plastic explosives are to be marked during the manufacturing process by introducing any one of the four detection agents agreed upon by the international air law conference and defined in the technical annex to this convention. (To enter into force. this convention required to be ratified by 35 member states, of which five had to be producing states, meaning states with manufacturers of plastic explosives.)"

The International Aviation Security Conventions adopted under the auspices of the ICAO have the following main objectives:

- Definition of the offenses
- Apprehension or arrest of the perpetrators and the imposition of severe penalties
- Granting of certain powers to the aircraft commander
- Defining the competence of states with regard to prosecution
- Exchange of information

The Tokyo (1963), The Hague (1970), and Montreal (1971) conventions and the protocol supplementary to the Montreal Convention (1988) are international instruments that seek to establish universal jurisdiction for a number of specified offences related to aircraft, international airports, and other aviation installations. These instruments require

the states that are parties to the instruments to prosecute or extradite alleged offenders, to impose severe penalties, and to facilitate the safe and expeditious return of aircraft and passengers diverted from their route. Furthermore, the Convention on the Marking of Plastic Explosives for the Purpose of Detection (1991) requires the states who are parties to it to prohibit and restrict the manufacture and transport of unmarked plastic explosives and destroy existing stocks in an effort to facilitate the detection of plastic explosives prior to their being brought aboard an aircraft. This convention also requires each state to exercise strict and effective control over the possession of unmarked plastic explosives.

A very important step in the processing of international instruments is their ratification by states. Ratification means transforming an international agreement into national law. Once a state ratifies a convention, it becomes a party to it, and it is interesting to note that aviation security conventions have been ratified and adhered to by more nations than most other international conventions. This highlights the importance placed by the states on this subject. All five aviation security international legal agreements have entered into force. In 2007, there were 189 member states in the ICAO, and as of July 2007, the official count of ratifications was as follows:

- Tokyo Convention of 1963: 182 parties
- The Hague Convention of 1970: 182 parties
- Montreal Convention of 1971: 185 parties
- Protocol of 1988 (supplementary to the Montreal Convention): 161 parties
- Convention on the Marking of Plastic Explosives of 1991: 134 parties

States that have become parties to the relevant conventions, or intend to do so, should, through existing legal instruments such as a national criminal code or through dedicated aviation security legislation, introduce and define as a minimum the acts of unlawful interference against civil aviation such as

hijackings, acts of violence aboard aircraft or at an international airport, and acts of sabotage or attacks against aircraft and air navigation facilities. The states should also establish jurisdiction in relation to these offenses when they are committed in the territory of the state, against or on board an aircraft registered in the state, and on board an aircraft that lands in the territory of the state while the alleged offender is still on board.

It is also important for states that are parties to the various conventions to establish procedures for extradition and the surrender of offenders to other states and take the necessary steps to ensure that an alleged offender is submitted to the competent authority for the purpose of prosecution when extradition is not requested or is refused. states should also empower an aircraft captain to perform his or her responsibilities like a chief of police on the flight, maintaining good order and discipline on board and protecting the persons and property on board.

Finally, the states that have become parties to the Convention on the Marking of Plastic Explosives for the Purpose of Detection should establish the necessary provisions to ensure the prohibition and prevention of the manufacture and transport of unmarked explosives, strict and effective control over possession of unmarked explosives, and the destruction of unmarked explosives in accordance with the provision of the convention.

## National Aviation Security Program Legislation

National legislation in every ICAO member state is also required to designate a national authority to be responsible for aviation security matters. This includes developing, implementing, and maintaining a national aviation security program, issuing regulations necessary to carry out the national program, and allocating responsibility among government agencies and elements of industry for specific aspects of the national program.

It may also be helpful for states to insert provisions into their legislation to assist in the implementation and enforcement of the policies contained in the National Civil Aviation Security Program that relate to passengers carrying firearms in the cabin of an aircraft or in their baggage, and provisions regarding the travel of persons who are in custody or subject to administrative procedures. Likewise, the national laws should also cover all areas of the requirements relating to airport security measures and procedures.

## Technical Aspects of the ICAO Civil Aviation Security Program

The technical aspects of the ICAO Civil Aviation Security Program consist of the states' use of the ICAO Security Manual (Doc. 8973—Restricted), Annex 17 to the Convention on International Civil Aviation, the work of the ICAO Aviation Security Panel of Experts, audit initiatives on technical aspects, ICAO seminars and workshops, and the ICAO Technical Cooperation

Bureau's assistance to states on aviation security matters through consultancies and training.

The Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference (Doc. 8973—Restricted) was first published in 1971. It was developed by an IACO Secretariat study group composed of members nominated by five states and four international organizations (the International Air Transport Association [IATA], the International Federation of Air Line Pilots' Associations [IFALPA], the Airports Council International [ACI], and the International Criminal Police Organization [INTERPOL]), who had been assigned the task of drafting the first manual. Subsequently, the security manual was revised in 1983, 1987, 1991, 1996, and 2002. The current sixth edition (2002) has been published in English, French, Russian, Spanish, and Arabic. The manual describes measures and procedures and contains guidelines on all aspects of aviation security. Its objective is to assist the states with the implementation of the international standards and recommended practices contained in Annex 17.

Annex 17 to the Convention on International Civil Aviation (the Chicago Convention) is entitled "Security—Safeguarding International Civil Aviation against Acts of Unlawful Interference." As previously stated, the Council of ICAO adopted international standards and recommended practices on aviation security in 1974 and these were incorporated into Annex 17 to the Chicago Convention. The objective of this annex is to provide civil aviation authorities with a comprehensive document containing all standards and recommended practices and procedures that deal with or are directly relevant to aviation security matters. Annex 17 was completely revised in 1981, 1986, 1989, 1992, 1997, 2002, and 2006 (the 8th edition is the current one).

An international standard is a specification or procedure whose uniform application is recognized as *necessary* for the safety or regularity of international air navigation and to which contracting states *will conform* in accordance with the Chicago Convention. If compliance is impossible, notification to the Council is compulsory under Article 38 of the convention.

A recommended practice is a specification or procedure whose uniform application is recognized as *desirable* in the interest of safety, regularity, or efficiency of international air navigation. Contracting states *will endeavor* to conform to it.

In accordance with Article 38 of the Chicago Convention, contracting states are required to file a "difference" with regard to a standard they cannot implement, and inform ICAO what procedures they plan to implement as an alternative. Differences are published in a supplement to Annex 17 and distributed to member states. An attachment to Annex 17 (green pages) contains excerpts from other annexes such as 2, 9, and 14. These contain standards and recommended practices from the other annexes that relate to aviation security matters.

### Implementation of the Technical Aspects

The implementation of the technical aspects of the ICAO Civil Aviation Security Program has been accomplished through regional aviation security seminars in all ICAO regions since 1973 and also through aviation security technical cooperation projects that began in 1977. These projects consist of technical and training missions organized and administered by the Technical Cooperation Bureau of ICAO and financed by various funding programs such as the United Nations Development Program (UNDP), the World Bank, and trust funds.

Implementation was also accomplished through the use of ICAO regional office aviation security coordinators who functioned from 1986 to 2003. An additional method of implementing the technical aspects of the ICAO aviation security program has been through the ICAO Mechanism for Financial, Technical, and Material Assistance to States with Regard to Aviation Security, an initiative that resulted from the bombing of Pan Am Flight 103 over Lockerbie, Scotland, in 1988. This mechanism was initiated in 1990 and is still ongoing at the time of writing. I was privileged to be assigned as the first chief of the ICAO Section SIA, which was responsible for the implementation of this mechanism.

As a result of the worldwide international ministerial conference on aviation security following the events of September 11, 2001, ICAO adopted and developed the Universal Security Audit Program (USAP) for implementation by all member nations of ICAO. This program calls for the training and certification of aviation security auditors selected from member states and for aviation security audits to be conducted in all member states to determine and report deficiencies in the countries audited, with follow-up audits to check the implementation of corrective measures by the states concerned.

## DRAMATIC CHANGE IN TERRORIST ATTACKS AGAINST CIVIL AVIATION

The year 1985 was a significant year for aviation security at ICAO as well as in the United States. Following the terrorist hijacking of TWA Flight 847 on June 14, 1985, the hijackers executed a U.S. military man and threw his body down the airport tarmac in full view of television cameras, a sight seen all over the world. Another violent event occurred on June 23, 1985, when Air India Flight 182 was blown up over the Atlantic Ocean killing 329 passengers and crew members. The ICAO Council rapidly named an ad hoc group of aviation security experts from 16 countries and four international organizations to convene and recommend revisions to Annex 17 in order to challenge the rapidly increasing threat to international civil aviation.

The ad hoc group formally became the ICAO AVSEC Panel in 1986 and this forum has been meeting annually since then to upgrade the standards and recommended practices in Annex 17, and also to recommend changes to

the ICAO Security Manual. As of 2007, the AVSEC Panel was composed of delegates from 22 states and four international organizations (IATA, IFALPA, ACI, and INTERPOL).

The United States also reacted promptly in following the TWA hijacking when the U.S. Congress quickly passed the International Security and Development Cooperation Act of 1985. This law requires the U.S. government to dispatch aviation security specialists from the FAA (now the TSA) to assess the security at international airports at foreign locations served by U.S. air carriers and foreign carriers departing from that airport to a U.S. destination. These visits are made with the concurrence of the foreign government and they continue to the date of writing.

Also in 1985, there were simultaneous attacks at the international airports in Rome and Vienna on December 27, 1985, committed by the same terrorist organization, and these events led to the signing of the Protocol Supplementary to the Montreal Convention, previously described.

The mid-air explosion of Korean Air Flight 858 over the Andaman Sea, killing 115 souls, in 1987, the sabotage of Pan Am Flight 103 over Lockerbie, Scotland, in 1988, in which 270 lives were lost, and the destruction of UTA Flight 772 in 1989 over the North African desert, in which 171 persons were killed, all served as a grim reminder that the new threat to civil aviation was now the in-flight sabotage of commercial airliners as opposed to the unlawful seizure of aircraft.

These events were instrumental in the signing of the Convention on the Marking of Plastic Explosives for the Purpose of Detection in 1991. Specifically, this came about as a result of a ministerial conference of the ICAO Council on February 15 and 16, 1989, during which the council adopted a 13-clause resolution, one of these clauses dealing with the explosives aboard aircraft.

Also, as previously described, the ICAO Civil Aviation Security Program shifted gears by adopting measures and procedures to prevent acts of sabotage of aircraft and air navigation facilities, because it appeared that unlawful seizure of aircraft was now becoming a thing of the past.

## THE EVENTS OF SEPTEMBER 11, 2001

The terrorist attacks New York and in Washington, DC, on September 11, 2001, are known to the entire world and need not be further elaborated on here. But essentially, 19 hijackers affiliated with al Qaeda seized two United Airlines (UA) and two American Airlines (AA) aircraft shortly after takeoff on the east coast of the United States. The airliners were fully fueled, having departed for destinations in California.

The hijackers were divided into four teams, and at least one member of each team had pilot training. The hijackers' intent was not to seize the aircraft to hold hostages and make demands, but to turn the airplanes into flying bombs and crash them into buildings.

The failure of the U.S. Civil Aviation Security Program's measures and procedures to prevent these events can best be explained by a U.S. official's response to questions asked by U.S. congressmen. U.S. Secretary of Transportation Norman Mineta told the National Commission on Terrorist Attacks upon the United States (also known as the 9/11 Commission) that, prior to the September 11 terrorist attacks, aviation security officials had not considered that a hijacker might commandeer an airplane for any reason other than taking hostages.

The United States, ICAO, and the whole world now were in shock as the new threat appeared to be the use of commercial airliners as weapons of mass destruction by terrorists willing to commit suicide. The reaction, of course, was dynamic, as ICAO immediately set the stage for a ministerial level meeting of all member nations to discuss and propose new and effective initiatives in the Civil Aviation Security Program. These initiatives are continually being refined as they consist of revised international standards as required by Annex 17 and the aviation security audits of all ICAO member states' national programs, along with enhanced training capabilities to meet the new challenges posed by terrorism against civil aviation.

The U.S. government also set up a new Transportation Security Administration (TSA) to take over the U.S. Civil Aviation Security Program, and the creation of a new Department of Homeland Security in which the TSA was organizationally structured along with other security-related administrations and agencies.

## CONTINUING TERRORIST EVENTS

Not long after the events of September 11, 2001, a would-be saboteur flying on an American Airlines airliner from Paris to Miami, Florida, was overpowered by passengers and crew members when it was noticed that he was trying to light a fuse inserted in his shoe. The aircraft made an emergency landing and the FBI arrested the subject, after which they discovered an explosive device in his shoe containing enough plastic explosives to destroy the aircraft.

United Kingdom authorities reported in August 2006 that they had succeeded in disrupting an alleged terrorist plot against civil aircraft over the North Atlantic. The terrorist attack, judged to be imminent, would have involved bringing the component parts of an improvised explosive device (IED), including a home-made liquid explosive, through the passenger and cabin baggage security checkpoint for assembly on the aircraft. The device would have been detonated aboard the aircraft while in flight in an act of suicide.

In 2007, a terrorist plot to sabotage the aviation fuel facilities at New York's JFK International Airport was foiled by U.S. law enforcement authorities. Also in 2007, United Kingdom. law enforcement authorities made arrests and investigated incidents at Glasgow Airport as well as car bomb discoveries in London. This caused an increase in security measures at U.S. and British airports, mass transit systems, and other transportation facilities.

As a result of continuing threats of this nature against civil aviation, ICAO issued security control guidelines for screening liquids, gels, and aerosols, recommended as interim measures by the ICAO Council. The United States and the United Kingdom instituted their own screening requirements for to liquids and gels.

It appears that the threat of terrorism against international civil aviation is here to stay. No longer is it believed to be a temporary phenomenon. Consequently it behooves all nations to boost their efforts to strengthen their national civil aviation security programs. With a strong political will and with cooperation worldwide as ICAO partners states (i.e., states that agree to comply to ICAO standards) comply with all international standards on aviation security, it will be possible to save lives and restore public confidence in air travel throughout the world.

## REFERENCES

AVSEC, Inc. 2008. Training Files. McKinney, TX.

CNS News. 2003, May 24. "Officials Never Thought of an Airplane Being Used as a Missile." Top Headlines. Available at: www.cnsnews.com.

ICAO Legal Bureau. 2008. "International Conventions—Ratifications." Available at: www.icao.int.

Phillips, D. 1975. *Skyjack—The Story of Air Piracy.* London: George G. Harrap & Co.

# CHAPTER 7

# How the Hijackers on September 11 Approached American Aviation Security and Evaded It

*Stephen E. Atkins*

The hijackers on September 11, 2001, easily circumvented American aviation security because the security systems at American airports were deficient, and the al Qaeda hijackers had done their homework to take advantage of a weak American aviation security system. It had become more difficult over the years for terrorists to seize control of aircraft by smuggling weapons aboard an airliner to hijack it or planting bombs to blow an airliner up. But it was still widely accepted that there were deficiencies in airline security both on the ground and in the air. Moreover, the approved plan for handling aircraft hijackers was to passively accept the hijacking until the plane landed. Negotiators would then assume responsibility, and, if negotiations broke down, force could be used against the hijackers.

What was new on September 11, 2001, was the use of commercial airliners as flying bombs. This tactic was new and unexpected because it depended on highly motivated individuals willing to give up their lives in a suicide mission.[1] It also meant that prospective hijackers had to be able to pilot a commercial airliner for long enough to direct it to a designated target. Despite some warnings about possible use of aircraft on terrorist missions from various intelligence sources, American authorities were caught completely flat-footed on September 11. Why this was the case has never been adequately explained.

## HISTORY OF WEAKNESS IN AVIATION SECURITY

Long before September 11, it was widely known that the aviation security at American airports was lax. In 1993, a journalist, Roger Simon, reported

the story of various incidents from 1979 to 1993, proving that weapons and bombs could be smuggled on board a commercial aircraft. The most notable example of this was the December 7, 1987, incident in which a fired airline employee at Los Angeles International Airport smuggled a gun aboard a commercial aircraft. He fired the gun several times, killing the pilots and causing the plane to crash.[2] This incident led the FAA to require all airline employees to go through metal detectors.[3] Despite strong opposition from both airline and airport organizations over the requirement and the $169 million price tag, this requirement was in place by the early 1990s.[4] In 1993, an FAA report concluded that airport security in the United States remained "seriously flawed" and "still not adequate."[5] It had not improved since the summary of aviation security weaknesses given in a 1989 report:

> Interrogation of passengers boarding international lights is erratic. Hand searches of carry-on bags are often cursory. It is not uncommon for checked luggage to slip on board without being X-rayed. The X-rays cannot detect plastic explosives used in the modern bomb.[6]

The problem was that the situation had not improved significantly by September 11, 2001. Technology to ferret out bombs had been improved by 2001, but the equipment necessary to do so had not been made available at all major airports, let alone smaller, local airports.

A rigorous security system had been opposed for decades by the American aviation industry. The industry wanted as few impediments as possible to the cheap and efficient movement of passengers. More rigid security cost money. Allied to the aviation industry was its regulatory agency—the Federal Aviation Administration (FAA). Instead of regulating the aviation industry, the leaders of the FAA had developed a casual, cozy relationship catering to the airline companies' desire for profit over security. The FAA's leaders had taken the promotion of the commercial airline industry as more important than providing for security. This overemphasis was never official, but over the course of time it developed.

Further, the airline industry appeared interested only in short-term, inexpensive solutions. Often, these were paper solutions. This deficiency was noted by Brian Sullivan, a retired FAA special agent, in an e-mail to Michael Canavan, associate administrator of civil aviation security to FAA federal security managers, on August 16, 2001:

> Your intent was to work with the regulated parties and develop action plans to permanently correct problems. Here's what's really happening. A problem is identified. Instead of opening a case, we work with industry to develop the required plan. The agents go out and find that the problem persists, but field management won't allow them to open a case, incorrectly citing your May 30th memorandum as the basis for their decision. As a result we have a paper fix. Nice looking plans, but no real fix. The façade of security continues. Our line agents continue to experience the frustration of not being allowed to do their jobs.[7]

To counter demands for improved aviation security, the airline industry maintained that the aviation security system before September 11, 2001, was working. Spokespersons pointed out in early 2001 that there had been no hijackings or bombings of American airliners in more than a decade. In their opinion, the current security system was operating well enough to prevent such happenings. Most FAA attention was directed toward the threat of hijackings and bombings on the international flights of foreign carriers.

Attempts to improve security were sometimes blocked. Logan International Airport in Boston had one of the poorest aviation security records of any major airport in the nation.[8] It was notorious for failing to detect illegal weapons and for the ease of access to so-called secure areas. Joseph Lawless, public safety director at Massport (the Massachusetts Port Authority), noted that terrorists were operating in the Boston area and there was a need to improve security at Logan International Airport in a memo dated April 27, 2001.[9] Efforts by Lawless and State Police Major John Kelly to test aviation security at Logan International Airport in the summer of 2001 were opposed by the airlines and the FAA. The FAA's position was that Massport lacked the "legal authority to conduct these tests."[10] The FAA had conducted some testing at Logan International Airport, but the test results had been kept secret between the FAA and the Airlines.[11] This policy of keeping aviation security information from airport authorities was evidently universal throughout the United States.

Another roadblock to improvements in aviation security came from Congress. Efforts to implement the recommendations of the commission headed by Vice President Al Gore after the incident involving TWA Flight 800 had been blocked, but lobbyists for the aviation industry were effective in persuading congressmen and congresswomen to encourage government agencies to aid the aviation industry. Just weeks before September 11, the Transportation Committee of the U.S. House of Representatives held a hearing to castigate Norman Mineta, the transportation secretary, about the lack of federal action on delays experienced by passengers at airports.[12]

## HISTORY OF AVIATION TERRORISM

Hijackings of airlines had long been a tactic used by terrorist groups in the Middle East. Commercial airliners were attractive targets because they were symbols of a country and offered easy access. In the late 1960s and early 1970s, Palestinian terrorist groups became experts on aircraft hijackings. The Popular Front for the Liberation of Palestine (PFLP) came to specialize in hijackings. These, however, were political acts designed to liberate imprisoned Palestinian activists in Israeli and European prisons. Hijackings by the PFLP were intended to use passengers as bargaining chips to obtain freedom for the PFLP's compatriots. Hijackers received specialized training in PFLP training camps in smuggling weapons into aircraft and seizing control of aircraft. The heyday of hijackings was the 1970s, when news of such events seemed common.

An analysis of hijackings from 1947 to 1996 found that terrorist hijackers had an 85 percent chance of success.[13] There were, of course, occasional casualties during these hijackings, caused by the actions of the hijackers and sometimes by rescue attempts.

Most of the early hijackings produced results through bargaining until the United States and other countries decided that bargaining with the terrorists was counterproductive. During the period of the Reagan administration, the policy that the United States would conduct no bargaining with terrorists was implemented. Most European countries soon followed the lead of the United States. This policy decision and the building of specialized assault forces to combat the hijackings helped end the first phase of aircraft hijackings. Other steps were taken to upgrade security at airports, with the Israelis taking the most drastic measures. Once it became obvious that hijacking for political gain no longer produced results, the number of such hijackings declined. By the end of the 1970s, this type of hijackings had virtually ceased. The exception was the April 5, 1988, hijacking of a Kuwaiti airliner with more than 110 people aboard by the terrorist group Hezbollah. This attempt failed to win the release of terrorists in Kuwaiti jails, but the hijackers were released by the Algerian government even though they killed two of the passengers.

Those early hijackings made heroes of the hijackers that survived. Perhaps the most famous of the aircraft hijackers was the PFLP's Leila Ali Khaled. She participated in two hijackings—those of TWA Flight 840 in August 1969 and El Al Flight 291 in September 1970. Casualties among the hijackers, however, were heavy. They increased dramatically, particularly after the Western countries and Israel began to form specialized rescue teams.

The next phase was to plant a bomb and destroy the aircraft, rather than hijacking a commercial airliner. Such bombings were intended to prove that no one was safe from terrorism. Several airliners were blown out of the sky. Various terrorist groups used this method to advance their cause. The most famous of these bombings was that of Pan Am Flight 103. A bomb exploded in the aircraft over Lockerbie, Scotland, on December 21, 1988, killing all 258 people on board and another 11 people in Lockerbie. An investigation concluded that the bomb had been placed in a radio-cassette player and packed in with the luggage in Frankfurt, Germany. Throughout the 1980s, terrorists directed their attention to planting bombs on commercial aircraft, with Hezbollah, Libyans, North Koreans, and Sikhs participating. But it was the explosion on board TWA Flight 800 on July 17, 1996, causing it to crash and the creation of the Gore Commission, that galvanized the U.S. government to take action.

## AMERICAN RESPONSES TO AVIATION TERRORISM IN THE CLINTON ADMINISTRATION

Shortly after the crash of TWA 800, President William Clinton created the White House Commission on Aviation Safety and Security under the

chairmanship of Vice President Al Gore. The 18 members of the Gore Commission members deliberated and came up with a number of ways to improve aviation security. One of the commission's major proposals was to make aviation security a federal government responsibility, and for the FAA to provide certification of security companies. The goal was to provide better training for security guards and screeners. The commission also recommended that new explosives detection technology be deployed as soon as possible. Another recommendation was the need to implement a system to match a passenger with his/her baggage. Most of these recommendations were aimed at preventing aircraft bombings. After all, in the previous 30 years there had been more than 70 known attempts to plant bombs on commercial airlines. Bombs had caused 15 crashes and killed 1,732 people.[14] Finally, the Gore Commission recommended that $100 million a year be made available for aviation security.

The work of the Gore Commission met with mixed reviews. Shortly after the commission's recommendations were reported, the airline industry initiated a massive campaign against them. As part of this campaign, the aviation industry gave the Democratic National Committee $585,000 for the 1996 congressional elections.[15] Consequently, most of the Gore Commission's recommendations were either ignored or watered down due to opposition from the airline industry and/or by lobbyists for other constituencies.[16] The recommendations were the last attempt to improve aviation security before September 11, 2001.

The Gore Commission recommended the deployment of new explosives detection technology in part because machines that could detect explosives were being developed. It was not until 1994 that technology had finally caught up with bomb detection. Earlier machines were unable to detect plastic explosives, leaving an immense hole in screening for bombs. In 1994, however, InVison Technologies introduced a CT-scan technology to detect explosives including plastic bombs.[17] At the time of its introduction, the CTX5000 machine cost $1 million and was huge. Only three airlines bought machines—Delta, United, and Northwest.[18] They ordered five of them, but only three were in operation by 1996 at Atlanta and San Francisco.[19] Besides being very costly, these machines were so slow in handling baggage that only about 100 bags could be checked an hour.[20] The airline industry used this issue as a reason not to buy the machines.

Another approach was the use of bomb-sniffing dogs. The use of dogs to sniff out bombs was considered effective because in tests held in 1990, the dogs were successful in 100 percent of 340 tests.[21] The problem with this approach was the lack of enough available trained dogs.

## EFFORTS BY THE FAA TO PROVIDE AVIATION SECURITY

The FAA made periodic aviation security checks. One such check in 1987 found that 20 percent of mock weapons and bombs passed through screen-

ing.[22] Periodically, teams of FAA security personnel, Red Teams, would test the aviation security system with varying results. The problem was that the aviation industry disliked these inspections. Consequently, the FAA developed a program that would inform the airline company of inspections in advance, and, with this foreknowledge, screeners caught 95 percent of the mock weapons and bombs. FAA inspectors complained about this practice but to no avail. Sometimes journalists would test the screening system and negative publicity would ensue. One such test was conducted by the Fox Network at Logan International Airport in the spring of 2001, and it resulted in the exposure of the weakness of the aviation security system there. When Joe Lawless, the security chief at Logan International Airport, wanted to upgrade security, his bosses turned him down.

In the case of both hijacking to seize hostages and bombs planted in commercial aircraft, the Federal Aviation Agency never seemed to act until there was a tragedy occurred. Mary Schiavo, the former Department of Transportation (DOT) Office of Inspector General (OIG) dubbed the agency "The Tombstone Agency," because it was never proactive.[23] Ariel Merari, professor of psychology at Tel Aviv University and director of the Research Unit on Political Violence at Tel Aviv University, reinforces this conclusion.

> A look at the history of attacks on commercial aviation reveals that new terrorist methods of attack have virtually never been foreseen by security authorities. The security system was caught by surprise when the airliner was first hijacked for political extortion; it was unprepared when an airliner was attacked on the tarmac by a terrorist team firing automatic weapons; when terrorists, who arrived as passengers, collected their luggage from the conveyer belt, took out weapons from the suitcases, and strafed the crowd in the arrival hall; when a parcel bomb sent by mail exploded in an airliner's cargo hold in mid-flight; when a bomb was brought on board by an unwitting passenger, and so on. True, once terrorists used a new tactic or introduced a technical innovation the aviation security complex usually adapted its procedures fairly rapidly, so as to close the hole in the system. But the terrorists have not been torpid. They have looked for new ways to circumvent the security system.[24]

## ORIGIN OF THE SEPTEMBER 11 PLOT

Leaders of al Qaeda were aware of the weaknesses in both American and international aviation security systems, and they planned to exploit them. They realized that hijacking to free prisoners was unproductive and that planting bombs was becoming increasingly difficult, so there was little interest in these tactics. But this did not mean that other terrorists with contacts with al Qaeda weren't interested in penetrating aviation security to plant bombs. Ramzi Yousef, the mastermind of the 1993 World Trade Center bombing, had been busy in Manila, the Philippines, designing a nitroglycerin bomb to be triggered by a Casio watch. His experimentation led to the killing of a 24-year-old Japanese engineer, Haruki Ikegami, during a flight from Manila to Cebu City in the southern Philippines. Yousef's bomb almost caused the airliner

to crash, but a skillful pilot landed the aircraft at Naha Airport in Okinawa. Yousef's plans for a massive bombing campaign to include as many as 12 commercial aircraft in a plot later named Operation Bojinka ended when Yousef had an accident mixing chemicals in his Manila hotel.

Yousef did not let the mishap in Manila spoil his long-range planning. Before his accomplice, Abdul Murad, was captured in Manila, Yousef and Murad had discussed the possibility of using aircraft as flying bombs in the United States. Murad had received pilot training in the United States, so he knew how easy it would be to send a number of operatives there to receive pilot training. The cost of such training was in the $30,000 range so there was a need of financial support. Yousef and Murad broached this scheme to Yousef's uncle Khalid Sheikh Muhammed sometime in 1994. Muhammed thought about the potential of the operations, but he realized that there was a need for money and volunteers so he turned to al Qaeda.

The most readily available terrorist organization in the mid-1990s was al Qaeda. Possible state sponsors of terrorism were either out of business or maintaining as low a profile as possible to avoid sanctions from the western world. Also, al Qaeda had the financial resources that would be needed. Yousef was captured in 1995, but Muhammed made contact with Osama bin Laden in 1996 at the Tora Bora complex and discussed the issue.[25] Bin Laden was interested in the concept because it would target what he considered his greatest enemy, the United States.

Various plans were considered over the next two years. Muhammed's first plan, which was to involve 10 hijacked airliners, was too simply too ambitious. It also had Muhammed piloting one of the 10 airliners. He wanted to make a grand statement after landing one of the hijacked planes. First he would kill all of the male passengers and then make a public statement justifying his actions. But this plan posed too many problems to merit for serious consideration.[26] Another version had five planes attacking American targets in the United States, and another five planes hitting targets in Southeast Asia, but this plan was also dropped because it was too complex and there were timing issues.

Bin Laden delayed a decision on the September 11 plot until the spring of 1999. At a meeting in Kandahar, Afghanistan, bin Laden, Khaled Sheikh Muhammed, and Mohammed Atef finalized the plans for the mission.[27] Once al Qaeda's leaders approved the concept of the operation, they made Muhammed operational leader. They soon realized that the original plan calling for 10 aircraft to be used in the operation was unworkable. It was decided that the optimum number was four or five aircraft because of the difficulty of finding pilot candidates.

In the meantime, news had already reached the United States of a plot to use an aircraft as a flying bomb. While in police custody in the Philippines and undergoing interrogation, Murad mentioned an early version of a plan to use an aircraft to crash into CIA Headquarters in Langley, Virginia. The police office conducting the interrogation has maintained

that this information was passed to American authorities. There is no collaborating evidence to support his claim, but there is enough circumstantial evidence to show that this information was communicated in some form to American authorities. The report was lost somewhere in the bowels of the American bureaucracy.

Further confirmation that the idea of using a commercial airliner as a flying bomb was floating around in terrorist circles was the failed attempt to use an airliner for this purpose in late 1994. The Algerian terrorist group, the Armed Islamic Group (GIA), hijacked an Air France aircraft in Algiers in December 1994 with the intention of flying it into the Eiffel Tower in Paris.[28] Hijackers had the airliner flown to Marseille in southern France where they ordered more aviation fuel in order to produce more damage at the target. French Special Forces were able to stop the hijackers in Marseilles, but the intention of the hijackers became public knowledge.

Once Osama bin Laden had decided to back Muhammed's plan, the most difficult task for al Qaeda's leadership was to select the participants for the September 11 operation. Those selected had to be highly motivated and willing to be part of a martyrdom operation. The participants had to be able to function without suspicion in Western society with acceptable language skills and unobtrusive behavior. They also had to be intelligent enough to successfully complete a pilot training program in the United States. Finally, both the pilot candidates and the support operatives had to be able to obtain visas and pass the scrutiny of the American immigration authorities. The first four candidates were picked on the basis of their loyalty but they were unable to pass the other tests. Two of them, Walid Mohammed bin Attash and Abu Bara al-Yemeni, were unable to obtain U.S. visas because of their Yemeni background.[29] The others, Khalid al-Mihdhar and Nawaf al-Hazmi, could obtain the necessary visas and did so, but they were poor pilot candidates because of poor language skills and lack of experience of living in the West.[30] Both al-Mihdhar and al-Hazmi participated in the September 11 plot but only as secondary leaders, providing logistical support and then participating as members of the hijack teams.

Al Qaeda solved the problem of participants able to function in Western society without suspicion by recruiting the leaders of the Hamburg cell. These leaders, Mohammed Atta, Ramzi bin al-Shibh, Ziad Jarrah, and Marwan al-Shehhi, were highly motivated religious individuals of the type that al Qaeda was looking for. Moreover, they were intelligent and able to function without being noticed in Western society. Once these members of the Hamburg cell joined al Qaeda, it was easy to recruit them for the September 11 plot. After arriving at al Qaeda's Khalden Training Camp in November 1999, they soon became star products of its training.[31] Osama bin Laden met with them in December 1999 and broached the idea of their participation in a martyrdom mission.[32] He also asked for and received a loyalty oath (*bayat*) from them. After they agreed to participate in the plot, Mohammed Atef, then the military commander of al Qaeda, briefed them on the details of the plan.[33]

Bin Laden then appointed Atta to head the group. It only took a few weeks to prepare them for the mission.

The Hamburg cell had already attracted the attention of the German authorities. Security officials were keeping track of potential Muslim extremists in Germany and ran across this. They were content to monitor the activities of its members. German law was extremely tolerant of political activities in Germany unless they endangered the state. At this time the Hamburg cell seemed to pose no such threat. Thomas Volz, an American CIA agent stationed in Germany, was not as tolerant. He was adamant that the Hamburg cell was a terrorist cell and that the German authorities should arrest its members. His calls for action became so strident that German officials considered deporting him from Germany. In the meantime, the German authorities continued to monitor the activities of the members of the Hamburg cell from a distance, even after most of its leaders left for the United States.

## IMPLEMENTATION OF THE SEPTEMBER 11 PLOT

After returning to Germany, the Hamburg cell conspirators began to make preparations to travel to the United States and begin pilot training. A problem arose when Ramzi bin al-Shibh was unable to obtain an American visa after four tries because he was Yemeni. The others had no problem entering the United States. Since consular officers were not trained to detect terrorists in a visa interview, they had little trouble obtaining visas, despite numerous irregularities in their documentation.[34] Other attempts to have al Qaeda operatives to enter the United States and train in pilot training programs failed because at least two were denied visas and another, Mohammed al-Katani, was denied access at Orlando International Airport because the immigration agent became suspicious of him. These failures left only three pilots in training until al Qaeda was able to recruit a fourth pilot, Hani Hanjour. Hanjour had previously completed pilot training in the United States, but his piloting skills were so poor that he had been unable to find a job as a commercial pilot.

In the year before September 11, 2001, the conspirators spent most of their time training for the mission at American pilot training schools. They attended various schools in Florida and elsewhere, building up their skill level in flying commercial aircraft. Their emphasis was in becoming familiar with flying Boeing 757s and Boeing 767s. The reason was that both aircraft were relatively new versions and with upgraded instrumentation they were easier to fly. They had what is known as glass cockpits. A plane with such a cockpit "relies on a much smaller number of multi-function displays, television screens in the cockpit."[35] These cockpits provide a simpler interface system so that hijackers do not need as much training and experience as they would need to fly other aircraft. There are also fewer people in the cockpit of these airliners, and it is easier to overwhelm one or two people as opposed to three or four in non–glass cockpit aircraft. Given the level of automation involved, learning to pilot a glass cockpit aircraft into a target should have taken only

about a week of simulation training.[36] Actually it took longer for the conspirators because they had so little experience or interest in flying before starting pilot training.

By the middle of the summer of 2001, the plot was gathering steam. In May and June, the muscle men had arrived in the United States. These were the men trained to provide the physical side of the hijacking. They had received training in al Qaeda's Afghanistan training camps in hand-to-hand combat, to enable them to overpower flight crews.[37] Most of them were from Saudi Arabia, because it was easy for a Saudi citizen to obtain a visa to travel to the United States.[38] All that was needed was to fill out an application form and show up at the American Embassy to pick up the visa. It was an express system, in which little or no checking of people applying for visas was carried out. Moreover, it was easy to attract Saudis to take part in a martyrdom mission against the United States.

Once the pilot training was over, the conspirators began to study the weak spots in American aviation security. Each of them had flown in American commercial airliners before, but now they conducted a systematic investigation of what they could get away with. In a series of 12 flights across the United States, the leadership team investigated the way the security system operated and the way in which to gain access to a cockpit. On one occasion, a flight attendant reported that a member of the al Qaeda team, Abdul Aziz al-Omari, requested access to the cockpit; he was allowed in and was able to talk to the pilots.[39] On another occasion, the actor, James Wood, because suspicious of the erratic behavior of a number of Middle Eastern men on a flight. He reported their actions to the flight attendant and the first officer.[40] They reported the incident to the FAA, but nothing came of this report. Only after September 11 did the report resurface.

From their flights, the al Qaeda team came to certain conclusions. First, it was relatively easy to pass small items like knives, box cutters, and Mace containers through security checkpoints. Knives under three inches long and box cutters proved to be no problem because they were legally allowed. It was relatively easy to get Mace through the security checkpoints despite its banned status. Second, it was necessary to purchase seats in the first class section in order to be close to the cockpit for a successful hijacking. This location cut the time necessary for the hijackers to obtain access to the cockpit, and made it easy to overpower a flight attendant near the cockpit entrance. Third, they must have seen that the flight attendant in the first class section always had a key to the cockpit, because the attendant would have used it during all of the flights. Fourth, they determined that Tuesday was the best day for a hijacking because of the low volume of traffic on that day and the planes would be nearly empty of passengers. They were not concerned with the passengers, except for the ways in which they might interfere with the hijacking and the completion of the mission.

By August 2001, the 19 conspirators had been assigned their respective tasks. They had been divided into four teams—three teams with five members

and one team with four members. To ensure that nothing went wrong on September 11, it was necessary to obtain fraudulent identification papers for several of the new arrivals. Obtaining such documents proved to be easy after team members paid a Salvadorian immigrant to sign an affidavit for them at a Virginia state motor vehicle office.[41] To avoid attracting attention, the conspirators frequently moved to different residences. Money was no problem, because al Qaeda was constantly supplying them with funds. It is estimated that the plot cost around $500,000.[42]

Atta was in charge, and he was in constant contact with his al Qaeda handlers. On July 8, 2001, Atta flew to Spain to meet with Ramzi bin al-Shibh and others to finalize plans for the September 11 attacks. They met in the tourist town of Salou, in Spain. Over the following week, Atta met with representatives of al Qaeda and laid out plans for the attack on American targets.[43] At this time, the date of the operation had not been determined. The decision was Atta's to make, but there was pressure from Osama bin Laden to carry out the attacks as soon as possible.

## AVIATION SECURITY MEASURES THAT THE HIJACKERS HAD TO OVERCOME

For the hijackers to accomplish their mission, they had to overcome a number of security measures designed to thwart it. The first was intelligence. The mission of the civil intelligence division of the FAA was to gather intelligence on threats to American aviation. The division operated 24 hours a day. The FAA assigned members of the division to the CIA, FBI, and the U.S. State Department to gather and interpret intelligence data relating to aviation security. Members of this division were aware of the potential for terrorist suicide hijackings as early as 1998, but FAA officials downplayed the possibility to the American aviation community in 2000 and 2001.[44] There was other intelligence information that never made it to the FAA's intelligence division—the Phoenix memo, about a suspicious number of persons from the Middle East taking pilot training and the presence of two al Qaeda operatives in the United States, Khalid al-Mihdhar and Nawaf al-Hazmi. FAA agents did learn about Zacarias Moussaoui, but it had little impact on them. There was no information available from any intelligence source about the other September 11 conspirators, because they had been able to escape detection.

In the summer of 2001, the FAA received a variety of warnings about possible terrorist activity. Increased activity by al Qaeda and al Qaeda–affiliated groups was noted by American intelligence, but the consensus was that terrorist operations would be directed to American targets in foreign lands. Nevertheless, the FAA passed the warnings along to the airlines. Fifty-two warnings were issued between April 1, 2001, and September 10, 2001.[45] These warnings became so routine in the summer of 2001 that the airline industry noted them but did nothing proactive in response.

The al Qaeda operatives also took precautions to avoid suspicion. The candidates had been screened to ensure they were able to operate in Western society. They had also been trained to avoid attention. Beards were forbidden, as was attendance at any mosque in the United States. They were not to carry copies of the Koran, nor quote from it. Typical Muslim greetings were also forbidden. They were also taught to avoid public places where they might attract attention, such as libraries. There was to be no contact with family members, including wives. No more than three members of the conspiracy were to be together at any one time. Anything that would attract attention was to be avoided. This attention to detail became more important when the 13 muscle men began arriving in the summer of 2001, because they lacked the plot leaders' sophistication and experience of living in Western society.

The next layer of aviation security was passenger prescreening. Prescreening starts with the ticketing process and ends with passenger check-in at the airport's ticket counter. Most passengers buy tickets in advance, allowing the passenger to be examined for anything suspicious. Advance ticketing also allows the airline company to check the FAA list of individuals known to pose a threat to commercial aviation. Individuals on the list were to receive special treatment, ranging from refusal of boarding to special screening. The problem was that on September 11, FAA intelligence had only 12 names of potential terrorists on its list. None of the September 11 hijackers were on it. In contrast, the U.S. State Department's TIPOFF list had over 40,000 names. The FAA's truncated list was in response to the airline industry's wishes, since a longer list would cause passenger delays.

The next step in prescreening was the examination of luggage. Beginning in 1998, the FAA required air carriers to screen passengers with the Computer-Assisted Passenger Prescreening Program (CAPPS). CAPPS's main role was to evaluate each passenger's security risk in order to isolate passengers needing further screening.[46] Because almost all attention was given to detecting explosives, those identified by the CAPPS system usually just had their luggage inspected.

Since the conspirators had no intention to use explosives, they had little trouble getting through the CAPPS system. At Logan International Airport, CAPPS selected three of the five hijackers on American Airlines Flight 11 for examination. They got through with no further screening. CAPPS selected none of the United Flight 175 hijackers for screening, also at Logan International Airport. All five of the American Airlines Flight 77 hijackers at Dulles International Airport received security attention. Three of them underwent CAPPS inspection, and the others were queried for inadequate identification information. In the end, they all passed prescreening. Only one of the United Flight 93 hijackers at Newark International Airport had his checked bag screened for explosives.

The next layer of aviation security is airport access control. This layer is meant to keep weapons or bombs out of airports by screening the persons authorized to work at the airport. It is also designed to keep outsiders from

bypassing security checkpoints. Although most employees at airports hold low-paying jobs, there have only been a few cases in which they have presented problems. After all, employees have also had to undergo screening since the 1980s. Airport access control remains an aviation security problem, but before September 11 it was an even bigger problem. Air cargo does not go through a systematic screening process, even since September 11, and it remains a problem that al Qaeda operatives could exploit.[47] Despite this weak link in aviation security, there is no indication that the September 11 hijackers had any assistance from either authorized personnel or other employees, or anyone else who had penetrated airport security. In fact, it would have been uncharacteristic of the hijackers to risk their mission by trying to recruit insiders. They had a plan and kept to it.

Perhaps the most important aviation security feature was preboarding screening, but it had its flaws. Areas in airports had been set aside for screening involving detection machines and personal searches. Huge numbers of people had to be screened at peak hours. The system depended on alert and knowledgeable screeners, because the X-ray machines were unable to detect explosives.[48] Instead, the machines detected suspicious objects as possible explosives. It took the subjective judgment of the operator to determine the course of action. Despite constant pressure from the airline industry, the U.S. government refused to assume responsibility for airport security. Consequently, the airline carriers contracted out the screening to security firms.

There were four aviation security companies handling the bulk of the passenger screening in the United States before September 11, 2001. The largest of these companies was Argenbright Security, with 40 percent of the business. It had the security contract at Dulles International Airport for American Airlines. Argenbright Security also had the security contract at Newark International Airport. Globe Security had the American Airlines contract at Logan International Airport. Huntleigh USA had the security contract for United Airlines, also at Logan International Airport. The fourth and smallest company in the business was International Total Services (ITS). Security firms won contacts by winning lowest-bid competitions.[49]

The private security firms hired personnel to run the screening system, but there were problems. At Dulles International Airport, 87 percent of the passenger screeners were foreign nationals, mostly from Muslim countries.[50] Efforts to discipline or fire workers by the airport security companies were restrained by the federal government. This practice led to a lament by a former FAA inspector at Dulles International Airport, Steve Elson, in 2001:

> Airport-security contractors can't win. On the one hand, the government slams them for hiring foreigners. But if they don't hire them, or [if they] fire them the government nails them for discrimination. . . . The only standard government enforcement is making every minority happy and comfortable and not offending anybody.[51]

Furthermore, cost cutting by the airline carriers meant continuous pressure on the security firms to do more with less. One company, ITS, was preparing to declare bankruptcy on the morning of September 11.[52]

The FAA mandated that the screening system use metal detectors and more sensitive handheld sensors. Although the aim of the screening system was to detect weapons and explosives, the issue of detection of drugs and other contraband complicated the role of the screeners.[53] Metal detectors had to meet FAA specifications and have a false alarm rate limit of not more than 15 percent.[54] The detectors had to be tested weekly, and, if the machine was turned off and/or left unattended for a significant period of time, it had to be retested.[55] Those individuals setting off metal detectors were subject to further screening by handheld wands. Among the things prohibited were firearms, explosives, incendiary devices, Mace, and knives longer than three inches.

Almost from the beginning there were problems with the screeners because of the nature of their jobs. On September 10, 2001, there were approximately 28,000 security guards and screeners employed at American airports. The average employee, however, stayed only around six months.[56] Low pay and boring working conditions caused this high turnover. A General Accounting Office report in 2000 documented that the turnover rate among baggage screeners at large U.S. airports between May 1998 and April 1999 was 125 percent.[57] Pay averaged $5.85 an hour, which was less than most fast-food jobs paid in the airports.[58] Also the screeners had few if any benefits. There were also hiring problems and training issues that produced additional problems. Many of the screeners had problems speaking English with sufficient fluency.

Every expert in aviation security knew that screening was a potential weakness in the system and that there was a need to keep testing the screening system. At first, the FAA issued hefty fines for failures in screening testing, but protests from the air carriers led to the end of fining in 1990.[59] From that time onward, the FAA allowed the airline companies to handle problems at their convenience, the only stipulation being that they were to produce a written document promising corrective action.

A further issue was the lack of background checks on the screeners. Until 1995, several states, particularly Florida and Louisiana, had mandated strict background checks. A 1995 federal court case ruling ended state background checks by citing the 1978 Airline Deregulation Act, which gave the responsibility for airport screeners to the airlines and forbade the states from interfering by a law, rule, regulation, or standard.[60] Airline carriers then delegated the background checking to the aviation security firms they hired. In the rush to maintain their workforce, which was constantly changing, background checks were sometimes overlooked.

The hijack teams had no difficulty passing through screening. Despite the FAA's list of prohibited weapons, there was uncertainty about what constituted a dangerous weapon. FAA guidelines informed the screeners that common sense should prevail.[61] Representatives of the air carriers issued a

checkpoint operations guide that made box cutters a prohibited item, but it gave no guidance on how to distinguish between "box cutters" and "pocket utility knives."[62] The hijackers were able to use this ambiguity in the rules to pass through screening. It almost certain that they carried pocket knives under four inches long, and probably box cutters. They were able to smuggle Mace aboard at least one of the airliners.[63] Although the hijackers on several of the airliners proclaimed that they had a bomb, it is unlikely that this was so. Part of the problem of ascertaining what happened at screening was that Dulles International Airport was the only airport with a video system operating at the screening stations. Interviews with screeners after September 11 indicated that only three of the 19 received secondary screening, and they were all at Dulles International Airport.[64] They triggered the metal detector after passing through initial screening. Metal-detecting handheld wands were used to test them. Since the hijackers had tested the screening systems during their 12 test flights, they had made certain to pass through the screening system by not challenging it with prohibited weapons. Their entire mission depended on successfully passing through the screening process.

Onboard security on American commercial aircraft before September 11 was almost nonexistent. There were four vulnerabilities of which any hijackers could take advantage to seize control of an airliner. First, the standard operating procedure (SOP), the "Common Strategy" was to offer no resistance to a hijacking based on the premise that once the airliner landed, negotiations would follow on the ground.[65] This policy meant that the crew would not prevent the hijackers from taking over the plane. It also meant that the hijackers on American Airlines Flight 11, American Airlines Flight 77, and United Airlines Flight 175 had no impediments to gaining control of the airplanes relatively easily. Only on United Airlines Flight 93 did the crew and passengers react differently, when it became apparent that the hijackers were on a suicide mission. Second, the fact that all flight attendants carried keys to the cockpit meant that all the hijackers had to do was attack the flight attendant in the first class section and claim her key. It was an FAA regulation that all flight attendants carry keys to the cockpit.[66] During the conspirators' 12 exploratory flight, they undoubtedly saw flight attendants use their keys to the cockpit. At least three of the flight attendants were reported to have been attacked on September 11, probably to obtain their keys, because otherwise they were no threat.[67] On United Airlines Flight 93, the flight attendant was captured and held captive in the cockpit. Third, it was mandated by FAA rules that a pilot or first officer would investigate any disturbance in the aircraft. This practice meant that either a pilot or first officer would open the cockpit door to investigate, making it easy for a potential hijacker to gain access to the cockpit. While there is no evidence that this practice contributed to the successful hijackings on September 11, it was still a weakness. Fourth, the weak cockpit door made it possible for hijackers to gain access by simply knocking down the door. It would take only about 150 pounds of pressure to break down the door. Many experts believe that this approach was used by the hijackers

on September 11, but there is no confirmation of this. The best witness was Betty Ong on American Airlines Flight 11, and she reported that the hijackers forced their way into the cockpit, but because she was in the back of the aircraft her evidence does not indicate exactly how the cockpit door was opened. She did report that once the hijackers were inside the cockpit with the pilots, the cockpit door was locked.[68] This fact would indicate that the door had not been knocked down, and that the hijackers had gained access to the cockpit by other means. Besides, the noise of breaking down the door would have been noticed by at least one observer. Moreover, the time it took to knock down the door would have given the pilots time to inform the FAA that a hijacking was taking place. Finally, in previous cases of attempts to force the cockpit doors the pilots had difficulty handling the aircraft.[69] No such irregularities in flight pattern or altitude were recorded in any of the aircraft on September 11.

## ABSENCE OF AIR MARSHALS

The one factor that might have prevented the hijackings on September 11 was the presence of air marshals on the airliners, but there were none. In 1962, the FAA initiated the Air Marshall Program to prevent airliner hijackings by placing marshals on "high risk" and "special circumstances" flights.[70] A flurry of hijackings to Cuba in the early 1970s led the Nixon administration to expand the program to hundreds of agents.[71] The program was further expanded by the Reagan administration in the 1980s, after the hijacking of TWA Flight 847 in 1985. Despite the success of the program, the aviation industry opposed it, because it was costly having to give up seats on an airliner. What made it worse was that the seat or seats reserved for air marshals were in first class. The pilots' union was also opposed to armed air marshals because of a concern about possible gunfire in an airliner. Consequently, several airline carriers petitioned the government to eliminate the program, charging that it was "ineffective and risky."[72] The combination of opposition from the aviation industry and the absence of hijackings led to a contraction of the Air Marshall Program in the 1990s. A decision was made in the FAA to transfer aviation security to the ground and the screening process. By 2001, there were only 32 air marshals on duty for an average of 34,000 airline flights daily.[73] Moreover, all of the air marshals had been assigned to international flights because the FAA considered these to be more risky. The failure of the Air Marshall Program and the existence of other onboard weaknesses meant that the hijackers had little trouble seizing control of the aircraft.

Despite the lack of a air marshal on any of the flights, the hijackers were suspicious of the occupants in the first class section. They had carefully placed two team members in seats near the cockpit for rapid access to it, and the other members were seated toward the back of the first class section to control the passengers. On American Airlines Flight 11, the hijackers were suspicious that one of the passengers was a possible air marshal. This passenger was Daniel Leven, an Israeli-American and a former soldier in the Israeli Defense

Force (IDF). As soon as the hijackers made their move on the cockpit, Levin was murdered.

## CONCLUSION

The hijackers on September 11 were successful because the American aviation security system was faulty, and they had made a serious study of its weaknesses. Anybody who knew anything about aviation security knew that aviation security at American airports had systemic problems. But every attempt to fix aviation security ran into insurmountable road blocks. The full weight of the aviation industry's lobby would crash down on the reformers. The aviation lobby had friends in Congress who could block or water down any legislation. It was not much better in government. FAA administrators were more comfortable not challenging the status quo, leaving the airline carriers to do whatever they desired. In essence, the FAA was incapable of regulating the airline industry. In a highly competitive industry, the air carriers constantly tried to lower security costs by putting pressure on the security companies they employed. This pressure to maximize profit at the expense of security led to one security company being in the process of applying for bankruptcy on September 11, and to others having financial problems. The onerous responsibility for making aviation security work was placed on the lowest level of underpaid employees.

Even before studying the weaknesses of the American aviation industry planners in al Qaeda were confident that a major terrorist attack on the United States was possible. Osama bin Laden accepted Khaled Sheikh Muhammed's plan because he wanted to strike at the United States. This desire meant that symbols of American power such as the World Trade Center, the Pentagon, U.S. Capitol, and the White House were all potential targets. Al Qaeda planners knew that if they could find the right operatives it would be possible to carry out a successful terrorist operation. In al Qaeda's training camps in Afghanistan, it was possible to find intelligent, highly motivated individuals willing to carry out a martyrdom mission. Once candidates were selected, it was easy for most of them to obtain American visas. In an open society like the United States, al Qaeda operatives were able to obtain the necessary pilot training and to take flights to study aviation security at airports and in the air. They learned that it was easy to penetrate aviation security as long as none of them challenged the system by becoming too conspicuous, or by trying to pass weapons through screening too openly. They realized that confusion over the FAA's list of prohibited items meant that some weapons could pass screening. Their observations on the lack of onboard security showed that hijacking an aircraft would be relatively easy with the trained personnel on their team.

Now it is known what can happen in an environment with a weak aviation security system and determined hijackers, but what about the future? Almost immediately after September 11, federal agents descended on the screeners at

Logan International Airport, Dulles International Airport, and Newark International Airport. Screeners were soon blamed for allowing the hijackers through security.[74] However, nobody could cite what the screeners had done wrong. It didn't matter that the hijackers had been passed through security having no weapon on the prohibited list. After all, the FAA wanted the screeners to use common sense in passing passengers through security.

Almost immediately after September 11, the airline industry launched a lobbying campaign for a government subsidy. This campaign was successful in Congress, which passed legislation granting the airline industry $15 billion—$5 billion in grants and $10 billion in secured loans. Almost as important was the airlines' request to have September 11 declared an act of war, making the airlines would not be liable for damage to persons and property on the ground. Finally, the airline industry was successful in having the U.S. government assume responsibility for aviation security.

Everyone in authority, the U.S. government, the FAA, and the airline industry, evaded responsibility. The September attacks were treated as a force of nature with nobody responsible for it. Those who had made a series of bad decisions were often rewarded by promotions, and those who had warned about the possibility of terrorism in the United States were left isolated. Congress reacted with a series of antiterrorism legislation that included the abolition of several agencies and the transfer of their responsibilities to Homeland Security.

The question remains as to whether there could be another major terrorist incident take place in the United States. Although al Qaeda has lost its safe haven in Afghanistan, it still has the capability of launching a terrorist attack in the future. The major question is, will this attack have an aviation component? Despite the federalization of aviation security, the record indicates that aviation security is still a problem. Weaknesses in screening and in security checks on employees remain ongoing problems. In the past, al Qaeda planners have taken a considerable amount of time in planning for a terrorist operation. This mode of operation appears to have changed little. In Khaled Sheikh Muhammed's testimony, at his hearing in early 2007 at the Guantanamo Bay detention center, he confessed to have been engaged in planning a multitude of terrorist operations to be directed against American targets. He may have been less than honest about future operations in the United States. The next time, the hijackers may hijack a cargo aircraft or steal a small aircraft at a local airport and use either as a flying bomb. Both are variations on the September 11 theme, but they are distinct possibilities.

## NOTES

1. Before September 11, Western analysts had viewed suicide attacks as not easily exportable, because such attackers required direct observation and targeting to be effective. This analysis meant suicide bombers needed close handling and could be launched only close to the target. The September 11 attacks violated this type of

analysis. Brian M. Jenkins, "The Organization Men," in *How Did This Happen? Terrorism and the New War*, ed. James F. Hoge, Jr., and Gideon Rose (New York: PublicAffairs, 2001), 7.

2. David Burke killed his former supervisor and the cockpit crew, causing the plane to crash. Roger Simon, "Airline Security Seems to Be Getting the Gate," *Plain Dealer* (Cleveland, Ohio), December 28, 1993, 7B.

3. Kenneth C. Moore has charged that this requirement did not solve the problem because in his words, "most airline employees have numerous ways to the air operations area other than though the screening checkpoint." Kenneth C. Moore, *Airport, Aircraft, and Airline Security*, 2nd ed. (Boston: Butterworth-Heinemann, 1992), 51.

4. Ibid., 196.

5. David Usborne, "US Airport 'Loath to Pay Out for Security,'" *Independent* (London), July 27, 1996, 10.

6. Laura Parker and David Ottaway, "The Weak Link in Airline Security," *Washington Post*, April 2, 1989, A1.

7. Quote taken from e-mail from Brian Sullivan, retired FAA special agent who worked at Boston Logan until his retirement in late 2000, to Michael Canavan, the individual in charge of all aviation security at the FAA from March 2001 to September 2001, August 16, 2001.

8. Andrew R. Thomas, *Aviation Insecurity: The New Challenges of Air Travel* (Amherst, NY: Prometheus Books, 2003), 59.

9. Massport was responsible for security at Logan International Airport. Thomas, *Aviation Insecurity*, 63.

10. Sean P. Murphy, "FAA Put Security Testing on Hold Agency Backed Airline Opposition," *Boston Globe*, December 9, 2001, B1.

11. Ibid.

12. Gregg Easterbrook, "The All-Too-Friendly Skies: Security as an Afterthought," in *How Did This Happen? Terrorism and the New War*, ed. James F. Hoge, Jr., and Gideon Rose (New York: PublicAffairs, 2001), 163.

13. Ariel Merari, "Attacks on Civil Aviation: Trends and Lessons," in *Aviation Terrorism and Security*, ed. Paul Wilkerson and Brian M. Jenkins (London: Frank Cass, 1999), 23.

14. Brian M. Jenkins, "Aircraft Sabotage" in *Aviation Terrorism and Security*, ed. Paul Wilkinson, and Brian M. Jenkins, *Aviation Terrorism and Security* (London: Frank Cass, 1999), 50.

15. Of the 50 recommendations from the Gore Commission almost nonewere fully implemented. Thomas, *Aviation Insecurity*, 52.

16. Brian M. Jenkins, "Aviation Security in the United States," in *Aviation Terrorism and Security*, ed. Paul Wilkinson, and Brian M. Jenkins (London: Frank Cass, 1999), 110–11.

17. InVision Technologies had received $8 million of its $20 million in development funds from the FAA. Charles Boisseau, "Improvements Needed to Combat Airline Safety Threat," *Houston Chronicle*, August 4, 1996, 2.

18. Boisseau, "Improvements Needed to Combat Airline Safety Threat," 2.

19. Usborne, "US Airports 'Loath to Pay Out for Security,'" 10.

20. Boisseau, "Improvements Needed to Combat Airline Safety Threat," 2.

21. Moore, *Airport, Aircraft, and Airline Security*, 183.

22. Irvin Molotsky, "20% of Mock Weapons Slip by in Test of Security at Airports," *New York Times*, June 18, 1987, A1.

23. Quoted from a letter from Brian F. Sullivan to Senator John Kerry on May 7, 2001.

24. Merari, "Attacks on Civil Aviation: Trends and Lessons," 24.

25. Osama bin Laden knew of both Ramzi Youself and Khalid Sheikh Mohammed, but only by reputation. Lawrence Wright, *The Looming Tower: Al-Qaeda and the Road to 9/11* (New York: Knopf, 2006), 235.

26. Terry McDermott, *Perfect Soldiers: The Hijackers: Who They Were, Why They Did It* (New York: HarperCollins, 2005), 77.

27. Wright, *The Looming Tower*, 307 8.

28. Jack Aubry, "Eiffel Tower Targets for Similar Attack in 1994," *Ottawa Citizen* Canada, September 14, 2001, C5.

29. Yemenis had difficulty obtaining U.S. visas because the Immigration and Naturalization Service (INS) was wary allowing them to come to the United States, not because of potential terrorism but because of economic reasons. They were though to be a burden on the American economy, coming from such a poor country. McDermott, *Perfect Soldiers*, 178.

30. Wright, *The Looming Tower*, 308.

31. The Khalden Training Camp was the initial stop for al Qaeda recruits undergoing training. After they went through boot camp, the recruits were then selected for specialized training at a number of other al Qaeda camps. In the late 1990s, there were about 50 camps in which al Qaeda recruits were trained, most of them quite small. McDermott, *Perfect Soldiers*, 172–73.

32. McDermott, *Perfect Soldiers*, 173.

33. German authorities claim that the members of the Hamburg cell were already discussing the idea of using an aircraft for terrorist purposes before traveling to Afghanistan. Jason Burke, *Al-Qaeda: Casting A Shadow of Terror* (London: Tauris, 2003), 219.

34. Staff Report of the National Commission on Terrorist Attacks upon the United States, *9/11 and Terrorist Travel* (Franklin, TN: Hillsboro Press, 2004), 5.

35. Testimony of Harry Samit, FBI agent at the FBI's Minneapolis Field Office, at the Zacarias Moussaoui Trial on March 9, 2006. Evidence from the trial indicates that Moussaoui was part of a future terrorist plot, because he wanted training at the Pan Am School to pilot a Boeing 747–400 rather than the smaller Boeing 757s and Boeing 767s that the September 11 conspirators trained on.

36. Thomas, *Aviation Insecurity*, 14.

37. McDermott, *Perfect Soldiers*, 220.

38. In June 2001, the U.S. government instituted the Visa Express Program in Saudi Arabia to reduce the consular workload and reduce the size of crowds outside the U.S. Consulate. This program meant that it was easy for Saudi citizens to obtain visas. StaffReport, *9/11 and Terrorist Travel*, 32.

39. John Miller, Michael Stone, and Chris Mitchell, *The Cell: Inside the 9/11 Plot, and Why the FBI and CIA Failed to Stop It* (New York: Hyperion, 2002), 296.

40. Ibid., 294–95.

41. Ibid., 298.

42. Burke, *Al-Qaeda*, 225.

43. McDermott, *Perfect Soldiers*, 224.

44. Staff of the National Commission on Terrorist Attacks upon the United States, "The Aviation Security System and the 9/11 Attacks" Staff Statement No. 3, 2.

45. Susan B. Trento and Joseph J. Trento, *Unsafe at Any Altitude: Exposing the Illusion of Aviation Security*, rev. ed. (Hanover, NH: Steerforth Press, 2007), 19.

46. Ibid., 12.

47. Editorial Staff, "Air Cargo Remains a Glaring Weakness," *San Antonio Express-News* (Texas), January 24, 2004, 10B.

48. Thomas, *Aviation Insecurity*, 190.

49. Many of these firms had offered low bids so as to be able to compete for more lucrative contracts. Michael Moss and Leslie Eaton, "Aviation Firms Ever Mindful to Cut Costs," *New York Times*, November 15, 2001, B1.

50. Argenbright Security ran into legal problems when it tried to forbid female employees from wearing traditional Muslim head coverings. They had to reinstate the fired employees and issue an apology along with back pay. Trento and Trento, *Unsafe at Any Altitude*, 15–16.

51. Trento and Trento, *Unsafe at Any Altitude*, 17.

52. Moss and Eaton, "Aviation Firms Ever Mindful to Cut Costs," B1. The events of September 11 delayed the process, but ITS did declare bankruptcy on September 13.

53. Moore, *Airport, Aircraft, and Airline Security*, 121–22.

54. Ibid., 128.

55. Ibid., 129.

56. Jim Gallagher, "Tighter Security Still has Leaks, Experts Say," *St. Louis Post-Dispatch*, July 28, 1996, 9A.

57. Jean Heller, "Report Faults Airport Security," *St. Petersburg Times* (Florida), August 1, 2000, 3B.

58. James F. Sweeney, "Airport Screeners Get the Lowest Pay," *Plain Dealer*, April 10, 2000, 1B.

59. Moore, *Airport, Aircraft, and Airline Security*, 95.

60. Jean Heller, "Critics See Weak Link in Airport Security," *St. Petersburg Times*, February 14, 2000, 1B.

61. Staff, "The Aviation System and 9/11 Attacks," 8.

62. Ibid.

63. Betty Ong reported the use of chemical mace or its equivalent on American Airlines Flight 11. Phillip Shenon, "A Calm Voice as Disaster Unfolded in the Sky," *New York Times*, January 28, 2004, A22.

64. Thomas, *Aviation Insecurity*, 48.

65. Trento and Trento, *Unsafe at Any Altitude*, 19.

66. This was FAA Order Number 8400.10, issued on January 7, 1997. Thomas, *Aviation Insecurity*, 33.

67. Thomas, *Aviation Insecurity*, 33.

68. Shenon, "A Calm Voice as Disaster Unfolded in the Sky," A22.

69. Thomas reported that there had been some 30 cases of passengers attempting to crash through the cockpit doors in the twenty-four months prior to September 11, 2001. These cases had been classified as due to air rage. Thomas, *Aviation Insecurity*, 34–37.

70. Philip J. LaVelle, "Federal Agents Now Flying on U.S. Airliners," *San Diego Union-Tribune*, September 27, 2001, A1.

71. Ibid.

72. Moore, *Airport, Aircraft and Airline Security*, 9.

73. Transportation Secretary Norman Mineta announced this figure on October 26, 2001. Bill Adair, "U.S. Had Only 32 Air Marshals Sept. 11," *St. Petersburg Times*, October 27, 2001, 6A.

74. Trento and Trento, *Unsafe at Any Altitude*, 36–38.

# CHAPTER 8

# Modern Terrorist Threats to Aviation Security

*James J. F. Forest*

During the past half-century, there have been literally thousands of attacks and plots against aviation targets worldwide. Passenger airlines in particular have been subject to an array of attacks by criminals, terrorists, and in some cases, naval warships. Despite the diversity of the threats, however, this chapter is focused exclusively on terrorist-related threats against aviation in order to provide adequate depth in the discussion. After examining a few explanations for why terrorists are interested in attacking aviation targets, the chapter will review some of the most prominent types of attacks that have occurred throughout history and that inform our understanding of the modern terrorist threats against aviation security. Based on the historical record, it is difficult to carry an optimistic, positive tone in such a discussion. The discussion will then turn to briefly review how governments have responded to this threat spectrum, and conclude with some analysis of what the past suggests we may face in the future.

## MOTIVATIONS BEHIND TERRORIST ATTACKS AGAINST AVIATION

Terrorism—a word which comes from the Latin *terrere*, "to cause to tremble"—has become a frightening global reality.[1] While there is no firm agreed-upon definition of the term, it is most commonly used in today's mainstream press to describe acts of politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. Scholars have observed that terrorism is most often an action taken as part of a broad strategy, not a random act of violence by wild-eyed psychotic misfits as portrayed in

the typical Hollywood film. Based on historical studies of political and revolutionary violence, we have learned that individuals are drawn to terrorist organizations and violence primarily for pragmatic reasons of contributing to political or social change. Islamic militants in Afghanistan, Egypt, or Uzbekistan, for example, may seek to unite the global community of Muslims under a single Islamic authority, while in Russia and Sri Lanka, the violence is caused by groups (Chechens and Tamils respectively) who want to form their own independent state.

Terrorism has also changed and evolved in recent decades—for example, terrorists' organizational capabilities and the means and levels of violence used to achieve their objectives have all changed. It is important to examine these changes, and to gain an appreciation for the long history of terrorism,[2] when developing an understanding of the threat of contemporary terrorist organizations. For example, according to Brian Jenkins, a senior advisor to the RAND Corporation, terrorists have adopted new models of organization and are less dependent on state sponsors; they are also effectively exploiting new communications technologies and can wage global campaigns.[3]

Generally speaking, terrorism has evolved over the last century from a local threat to a transnational phenomenon, facilitated in part by the globalization of commercial aviation. Indeed, many years ago a terrorist group would have had far greater difficulties exporting its violence (and its extremist ideologies) from one geographic location to another. And yet ironically, as described in this chapter, the worldwide aviation sector has been the victim of many terrorist attacks since the mid-1930s, from hijackings to in-flight bombings and surface-to-air missiles. While in many cases, in-flight bombings were purely criminal acts perpetrated as part of insurance scams or elaborate murder plots, the majority have been linked to various terrorist organizations and in some cases even state sponsors of terrorism, including Libya and North Korea. Beyond the specific motivations behind a particular terrorist attack (which are as diverse the ideological motivations behind the terrorist groups themselves), there are at least three areas in which common rationales can be seen for targeting commercial aviation: media coverage, economic impact, and the vulnerable nature of aviation targets.

## Media Coverage

For most terrorist groups, the appeal of attacking aviation targets may stem in part from the relatively high level of publicity and media coverage each attack receives. Indeed, as terrorism expert Bruce Hoffman notes, far more people have died from car accidents, yet "there is considerably higher anxiety and fear about the possibility of being a victim of aviation terrorism than about automobile accidents."[4] Terrorists see this, and conclude that aviation targets are an effective and relatively low-cost means for gaining public attention about their grievances. According to Rick Wrona, during the 1970s and 1980s (when the most airplane hijackings took place), terrorists "adopted

the international air carrier as a podium for proclaiming their organizations' manifestos."[5]

As Brigitte Nacos observes, print and electronic media are important means to spread the terrorist "propaganda by deed" and inform, indoctrinate, and prepare some individuals for recruitment.[6] Further, she notes, terrorists learn much from other terrorists through daily news reports, video clips, and Web sites. Thus, when terrorists uses the media effectively, other terrorists learn from and follow their example. In 2003, for instance, a proliferation of highly publicized videotaped beheadings—which began in Iraq but spread rapidly to Saudi Arabia and other parts of the world—was but one of many examples of this phenomenon of mediated terrorism.[7] Cindy Combs agrees that the media provide a forum for knowledge transfer in the terrorist world, offering a "showcase" through which those carrying out terrorist acts can impress and threaten an audience, recruit and train new members, and support and coordinate an emerging network of followers.[8]

According to Alex Schmidt, violence polarizes and forces audiences to take part by choosing either the side of the victims or that of the terrorist. Therefore, the media provide "identification mechanisms," since "the terrorist's invitation to identification is brought home to us by the public and the private media."[9] Combs notes that a symbiotic relationship exists between terrorists (who seek attention from an audience) and news organizations (which seek dramatic stories to increase their readership and ratings).[10] Because of their unique role in the global strategic communications battlespace, the media have a unique set of opportunities and responsibilities in combating the threat of terrorism. Indeed, Combs suggests implications for better media self-regulation.[11] Unfortunately, recent trends indicate the very opposite path is being followed by the mainstream media, with its oversaturated coverage of Hollywood scandals and its dramatization of everyday human tragedies.

## Economic Impact

Throughout history, terrorist ideologies have frequently incorporated some form of economic dimension as a component of their political objectives. For example, the Red Army Faction (RAF, also known as the Baader-Meinhof Gang) saw itself as part of a global communist struggle against capitalism and imperialism, and its ideological goal was to topple the post–World War II economic and democratic order in West Germany.[12] Similarly, the ideology of the Revolutionary Armed Forces of Colombia (Fuerzas Armadas Revolucionarias de Colombia—FARC) combines agrarianism and pro-Soviet Marxism, and the group has systematically targeted large multinational corporations.[13]

According to Sammy Salama, the al Qaeda network's foremost strategic objective is to "bleed" the United States economically and militarily by forcing it to spend enormous amounts of money on protecting its numerous sectors and facilities.[14] An examination of primary al Qaeda operational manuals and open-source published literature reveals their ambitious desire to destroy the

economy of the United States and other Western powers by striking economic targets in the West and in the Muslim world. They rationalize that if the American economy is derailed, then the United States will crumble and will not be able to sustain its military hegemony and presence overseas.

The following excerpt from *Sawt al-Jihad* (Voice of Jihad), the official publication of al-Qaeda in Saudi Arabia, illustrates the economic focus of al Qaeda's target selection:

> We need to strike this economy with harsh attacks. . . . the enemy has built his economy on the basis of open markets and free trade [and therefore] we have to prove to these investors that the enemy's land is not safe for them, that his economy is not capable of guarding their monies, so they would abandon him to suffer alone the fall of his economy.

Further, and of particular interest to the primary topic of this chapter (and this set of volumes), the same publication directly addressed the economic dimension of aviation targets:

> Hijacking planes is a well-known tactic; people used to hijack planes and consider them a target, but those who are willing to put in the extra effort turned these planes into a method, a projectile shot in the heart of the enemy. . . . The enemy used to protect his external interests and spend exuberant sums for this protection, so he was surprised when he was struck inside his borders. The enemy used to protect a thousand interests outside his county, now he has to protect a million interests inside his country that need continuing protection! The attack on the Trade Center forced America since that day to spend billions to protect the huge economic infrastructure that runs the American economy. Using planes in this attack has forced America to spend billions to protect the planes and airports in all possible ways. This protection is not limited to the hundreds of American airports but also to every airport in the world. Anyone related to the aviation field is spending excessive amounts to guard air travel; the matter has reached protecting the skies.[15]

In many of their public statements, both Osama bin Laden and Ayman al-Zawahiri have highlighted the fact that the economy is the center of gravity for the United States and have consistently called for a sustained campaign of attacks to damage its economy. Further, in addition to attacking economic targets in the United States and other Western nations, another stated objective of the network is to hinder Westerners from conducting commerce and business in the Arab and Muslim world. The argument here, according to Salama, is that Western commerce in Muslim and Arab countries has resulted in Western military support for corrupt and apostate regimes in the region (specifically Saudi Arabia, Egypt, Jordan, and Morocco). It has also contributed to the corruption of Muslim societies with imported Western values and the "theft" of Muslim natural resources including oil.[16] Thus, al Qaeda seeks to discourage travel by Western businessmen, diplomats, politicians, tourists, entertainers, and others to the Middle East.

Al Qaeda's ideology and economically oriented political objectives have clear implications for aviation security. Air transportation is inextricably linked to global commerce and economic growth, in addition to being a primary conduit for cross-cultural interaction. We can thus anticipate that globally minded terrorists—like those of al Qaeda and its affiliates—would be interested in using violence to deter flights from the West to other parts of the world, or perhaps even drive Western airlines into bankruptcy (which was the case for Sabena and several others after September 11), and overall constrain the forces of globalization while puncturing a vital artery of many nations' economies.

### Vulnerable Targets of Opportunity

In addition to the publicity and economic dimensions, airplanes are attractive targets because of the low cost-to-casualty ratio they offer to terrorists. As with buses (a common target of Palestinian suicide bombers in Israel), commuter railways (the target of attacks in Madrid, Spain), and subway systems (with attacks in London, Moscow, and Mumbai), commercial airplanes offer dozens if not hundreds of unarmed people cramped into a relatively small enclosed space. Providing security for any kind of public mass transportation is tremendously challenging, particularly given the competing demand of ensuring convenience for passengers. In other words, airplanes (as well as airports) are inherently soft targets. By the very nature of commercial aviation, the largest airplanes travel to and from the largest cities on predictable routes, with flight schedules published well in advance. The planes are full of highly combustible fuel, and during flight, the cabins are pressurized, amplifying the effects of even a small explosion—a mere tear in the fuselage at 36,000 feet could lead to a fatal deterioration of the plane's structural integrity, resulting in a crash. Airports are typically near centers of population and commerce, and planes leave and arrive at airports via a limited number of runways in predictable patterns. And, as discussed later in this chapter, as globalization leads to an increasingly ubiquitous presence of airplanes worldwide, the interconnected global aviation system is exposed to a diversity of security environments, some of which are inherently substandard.

In sum, terrorists will undoubtedly continue to target aviation because of the potential damage that can be caused to a nation's economy, along with the psychological impact derived from the relatively high level of visibility and media coverage that every aviation disaster receives. These are not the only rationales for targeting commercial aviation, but they do help illustrate the nature of the threat. We now turn to a discussion of the most common forms of these attacks from a historical perspective and will conclude the chapter with a look at what this history suggests for the future of terrorist threats against aviation security.

## COMMON FORMS OF TERRORIST ATTACKS AGAINST AVIATION

Four of the most prominent types of aviation attacks are reviewed here: hijackings, in-flight bombings, the use of surface-to-air missiles, and the use of airplanes as guided missiles.

### Hijackings

Beginning in the 1960s, aircraft hijackings became an increasingly common form of attack against the aviation sector.[17] One of the most prominent incidents occurred on July 22, 1968, when three armed Palestinian terrorists belonging to the Popular Front for the Liberation of Palestine (PFLP), one of the six groups that then constituted the Palestinian Liberation Organization (PLO), hijacked an Israeli El Al commercial flight en route from Rome to Tel Aviv.[18] This was the 12th airplane hijacking in seven months, but unlike previous incidents, the terrorists' objectives were not to simply divert the plane's flight path to a different destination (the most common form of plane hijacking at the time). Rather, the explicit objective of this attack was to acquire Israeli hostages who were then offered in trade for Palestinian terrorists held in Israeli prisons.

Further, while there were several different multinational commercial flights to Tel Aviv that the terrorists could have chosen for their attack, they specifically targeted Israel's national airline. This attack was also different in that, unlike previous diversionary-type hijackings, the terrorists succeeded in forcing the government to communicate directly with them, which in a sense acknowledged their grievances and (via the media circus surrounding the drama of this event) granted them recognition on a global stage. In essence, as Bruce Hoffman notes, a single airplane hijacking had brought more attention to the Palestinians' cause than decades of pleading on the floor of the United Nations.[19]

Replication of strategy and tactics is an honored tradition in the terrorist world,[20] and before long other groups were following the airline hijacking example set by PFLP. On September 6, 1970, a PFLP subsidiary known as Black September conducted two simultaneous hijackings, diverting Swissair Flight 100 and TWA Flight 741 to Zarqa, Jordan. They demanded the release of fedayeen (members of the Palestinian movement) imprisoned in Germany, Switzerland, and Israel. A few days later, the same group hijacked Pan American Flight 93, which was flown to Cairo, Egypt, emptied of its passengers and blown up. Then a fourth Black September hijack attempt failed when air marshals on El Al Flight 219 overpowered both terrorists. On December 17, 1973, Pan Am Flight 110—scheduled to fly from Rome to Beirut—was preparing to taxi when between 6 and 10 Palestinian terrorists stormed the terminal building and began firing submachine guns before proceeding directly to the plane and throwing as many as five hand grenades through the open

front and rear doors of the aircraft. Thirty-two passengers and crew members were killed in the attack, including four Moroccan officials heading to Iran for a visit, and 14 Aramco and employee family members.

For some groups, hijacking proved quite successful and occasionally lucrative. For example, on September 28, 1977, Japan Airlines Flight 472 en route from Paris to Tokyo was hijacked by the Japanese Red Army (JRA) after stopping for fuel in Mumbai, India. The terrorists ordered the plane to land in Dhaka, Bangladesh, where they took the passengers and crew hostage, demanding $6 million and the release of nine imprisoned JRA members. On October 1, then-Prime Minister Fukuda announced that the Japanese government would accept the hijackers' demands, on the principle that "human life is more important than the world."[21]

Similarly, in an event that captured global media coverage, a group of Lebanese Shia terrorists belonging to Hezbollah hijacked TWA Flight 847 and held the passengers and flight crew hostage for over two weeks.[22] On the morning of June 14, 1985, the plane departed the Athens airport en route to Rome and was hijacked shortly after takeoff by two Lebanese men who had smuggled pistols and grenades through the Athens airport security system. They forced the pilot to divert the flight to Beirut, Lebanon, which at the time was embroiled in a civil war. Beirut was divided into sectors with different militias controlling different areas, and the Beirut International Airport (surrounded by a Shia neighborhood) had no perimeter security; virtually anyone could simply drive onto the runway. After 19 passengers were allowed to leave in exchange for fuel, the plane left Beirut and landed in Algiers, released 20 additional passengers, and then returned to Beirut that night.

The initial demands of the hijackers included the release of all Lebanese captured by Israel in Lebanon; international condemnation of Israeli military activity in southern Lebanon; and condemnation of U.S. actions in the Middle East. Separately, the hijackers agreed to release eight Greek citizens aboard the plane in return for Ali Atwa, an intended hijacker who had been bumped from the flight and was later arrested in Greece. During the first days of the ordeal, the hijackers identified an American Navy diver, Robert Stethem, among the passengers. They beat him, shot him in the head, and dumped his body out of the plane onto the tarmac. On Saturday, June 15, nearly a dozen armed men joined the hijackers in Beirut before the plane returned to Algiers, where an additional 65 passengers were released. It again returned to Beirut, for a third and final time, on Sunday, June 16. The passengers were then removed from the plane and taken to various locations around the city. By Monday afternoon, June 17, most of the hostages had been taken from the plane to a secure location. They were held by various Lebanese Shia militia factions until June 30, when they were driven to Syria and released. Shortly thereafter, Israel released 735 Lebanese Shia prisoners.[23]

And in another example, Pakistani members of a Kashmiri separatist group, Harkat-ul-Ansar (HUA), hijacked Indian Airlines Flight 814 while it was en route to New Delhi, India, from Kathmandu, Nepal, on December 24,

1999. The Airbus A-300 aircraft carried 174 passengers and 15 crew members. About 30 minutes after takeoff, an armed masked person stood up and announced the hijacking. At about the same time, four other hijackers wearing red masks took up positions throughout the plane. Although they demanded to be flown to Lahore, Pakistan, Pakistani officials refused permission to land there and the plane was flown instead to Amritsar, India. However, the plane was not refueled before taking off again. After the plane made an emergency landing in Lahore, food, water, and fuel were provided. The plane took off again and landed in Dubai on December 25, where 27 passengers were released in exchange for food and fuel. The plane then departed for Kandahar, Afghanistan, where it remained until December 31, when the Indian government released Maulana Masood Azhar (the general secretary of HUA) and Ahmed Saeed Omar Sheikh from custody, along with two other terrorists.[24]

Despite the publicity and concessions that resulted from some airplane hijackings, however, the tactic was not always so successful for the terrorists. On June 27, 1976, Air France Flight 139 en route from Athens to Paris was hijacked by a team of Palestinian (PFLP) and German ("Revolutionary Cell") terrorists.[25] The plane was first diverted to Benghazi, Libya, and after refueling was flown to Entebbe International Airport in Uganda, where the 258 passengers and crew members were held hostage by additional members of the terrorist group and supported by the pro-Palestinian forces of Uganda's president, Idi Amin. They demanded the release of 40 Palestinians held in Israel and 13 people, some of which were Palastinian and some not, imprisoned in Kenya, France, Switzerland, and Germany, and claimed that if these demands were not met they would begin killing hostages. The terrorists eventually released all non-Israeli passengers, who were flown aboard a separate Air France flight to safety in Nairobi, Kenya.

On July 3, following a week of tense negotiations, the Israelis organized a risky mission to rescue the hostages. A team of commandos boarded four C-130 cargo planes and flew at low altitudes to avoid Arab and Soviet radar systems. As the first plane touched down at Entebbe airport around 11 P.M., the cargo hatch opened and a black Mercedes (similar to the one driven by President Amin) drove out, accompanied by two Land Rovers. Under the cover of darkness, the Israeli commandos drove slowly but directly toward the terminal where the hostages were being held. Their trick worked, as they caught the terrorists and the Ugandan soldiers unprepared for the assault on the terminal. While the remaining three C-130s landed with reinforcements, who engaged and defeated the Ugandan soldiers, the terrorists inside the terminal were quickly neutralized, and within 25 minutes all the hostages were freed and aboard an Israeli aircraft ready for departure. Intelligence—including aerial reconnaissance and satellite imagery—provided to the Israelis by the governments of Canada, France, Germany, Kenya, the United Kingdom and the United States, as well as from the hostages who had been released earlier, was critical in the success of this mission. Thirteen terrorists were

killed in the rescue, as well as one passenger, one commando, and 35 Ugandan soldiers.[26]

A combined team of German and Palestinian terrorists were also involved in the October 13, 1977, hijacking of Lufthansa Flight 131 to Mogadishu, Somalia. In this instance, a West German team of Grenzschutzgruppe Neun (GSG-9) commandos were deployed on October 17 after negotiations with several mediators proved fruitless. Under the cover of darkness, a sniper and reconnaissance team took up positions around and beneath the aircraft and began radioing the whereabouts of each terrorist aboard the plane. While a team of negotiators kept the terrorists' attention, Somali soldiers started diversionary fire and then the GSG-9 commandos stormed the plane through all six exits, quickly disabling the terrorists and evacuating the aircraft. Within seven minutes, all 86 hostages were outside the airplane and headed to safety.[27] A month later, the PFLP attacked an Israeli aircraft at the Athens airport, but the Israelis refused to accede to the demands of the hijackers to release Palestinian fighters in their prisons and retaliated by attacking Beirut airport and destroying 13 parked aircraft.[28]

Overall, the spate of international airline hijackings that occurred from the 1960s through the 1980s had two common themes, according to Hoffman: either the purpose of the hijacking was to divert the plane from its intended destination (often with Cuba as the new destination), or the intent was to use airline passengers as pawns in a high-stakes negotiation to compel governments to do something that would benefit the terrorists or their cause.[29] Sometimes the terrorists succeeded, other times they failed, but in all these instances, the terrorists' intention was not necessarily to harm the passengers. However, a number of attacks also took place during the twentieth century that involved bombings and shoulder-fired missiles—attacks in which the terrorists meant very much to harm the passengers, as well as others if possible, with no allowance for negotiating.

### In-Flight Bombings

Over the past 75 years, detonating explosives on planes while in flight has been the most common and deadly form of attack against the aviation sector. Although most researchers point to the 1960s and 1970s as the height of aviation attacks, airplane bombings have a much deeper history.[30] For example, on October 10, 1933, a United Airlines Boeing 247 was en route from Cleveland to Chicago when a nitroglycerin bomb exploded in midair, killing 10 passengers and crew members. On September 9, 1949, a dynamite bomb in the forward baggage compartment of a Canadian Pacific flight from Montreal exploded in midair, killing all 23 aboard. On April 11, 1955, an Air India flight carrying 19 people—including delegates from China and Vietnam as well as several journalists from Asia and Europe bound for the Asia-Afro Bandung Conference—crashed in the sea following an in-flight explosion. Investigators concluded that the explosion was caused by a bomb most likely placed

aboard to assassinate the premier of China, Zhou Enlai, who was due to be on the flight but canceled at the last minute. And on November 1 of the same year, United Airlines Flight 629 en route from Denver to Portland was destroyed when a bomb caused the plane's tail to disintegrate, sending it out of control and killing all 44 aboard.

During the 1960s, in-flight bombs destroyed National Airlines Flight 2511 (34 killed), Air France Flight 406 (78 killed), Continental Airlines Flight 11 (45 killed), Canadian Pacific Airlines Flight 21 (52 killed), and British European Airways Flight 284 (66 killed), among many others.[31] Overall, in-flight bombings occurred throughout the early decades of commercial aviation. And yet, as Guillaume de Syon noted, by the early 1970s, luggage placed on board aircraft unaccompanied was still a common occurrence; none of it was searched or checked, providing an opportunity for terrorists to insert a bomb in unaccompanied or unmatched luggage.[32] Thus, the bombing continued, and as passenger planes became bigger, the number of casualties from these bombings also grew.

On February 21, 1970, Swissair SR330 left Zurich, Switzerland, for Tel Aviv, Israel, carrying 47 people. The Convair CV-990 suffered an explosion about nine minutes after takeoff, due to a bomb triggered by change in atmospheric pressure that had been placed in the aft cargo hold. As the crew attempted to turn the plane back toward the airport for an emergency landing, smoke clouded the cockpit and electrical power was lost. The aircraft crashed shortly thereafter with no survivors. The militant Popular Front for the Liberation of Palestine claimed responsibility for the bombing. On the same day, an Austrian Airlines flight from Frankfurt, West Germany, to Vienna was damaged by an explosion that tore a six-foot hole in the fuselage, but the pilot managed to return safely to the airport and no one was reported hurt. Here again, the PFLP claimed responsibility.[33]

The bombing of these two flights in a single day made headlines, and airports all over Europe responded as if they were under siege. Gun-toting police and even armored cars patrolled runways; Israeli and Arab airliners were shunted to separate service areas. Baggage was X-rayed, stethoscoped, or simply scrutinized top to bottom, and some passengers were frisked for weapons. Briefly, 9 of the 16 airlines that served Israel suspended airmail and freight services. But Israel complained that such restrictions seemed to punish the victims more than the victimizers, and by week's end all but two lines had resumed full service.[34]

Sadly, the bombings continued into the 1970s and 1980s. On October 6, 1976, Cubana Airlines Flight 455 crashed into the sea minutes after taking off from Barbados, killing 73 people, including 24 members of the Cuban national fencing team. In one of the worst aviation disasters in history, Air India Flight 182 on its way from Toronto to Bombay blew apart off the coast of Ireland on June 22, 1985, killing all 329 people aboard. The subsequent investigation by Canadian officials led to a group of Sikh militants who were believed to have planted the suitcase bomb in retaliation for the storming of a

Sikh shrine in India by government troops. On November 29, 1987, a bomb placed by two North Korean agents on Korean Airlines Flight 858 en route from Baghdad to Seoul killed all 115 people aboard.[35] On December 21, 1988, Pan Am Flight 103 exploded over the village of Lockerbie, Scotland, claiming the lives of all 259 passengers aboard as well as 11 people on the ground. A subsequent investigation linked the attack to two Libyan intelligence agents.[36] And in August 1989, an in-flight bombing of a French UTA passenger jet over Chad killed 171 people and was claimed by Islamic Jihad.[37] But one of the most deadly aviation attacks ever planned is one that few people knew of, at least prior to September 11, 2001.

Dubbed "Operation Bojinka," this plan to destroy up to 12 U.S. airliners over the Pacific in January of 1995 was developed by Ramzi Ahmed Yousef, who had led the bombing of the World Trade Center in 1993, and his uncle Khalid Sheikh Muhammad, the operational mastermind behind the attacks of September 11.[38] Details of this plot—revealed in court testimony and other records after both men were apprehended, in 1996 and 2003, respectively—indicate not only the sophisticated nature of al Qaeda operations in general but also the consistent manner in which terrorists seek to exploit vulnerabilities in the global aviation system.[39] In order to test airport and aviation security, Yousef and Muhammad decided to rehearse the operation in airports in Hong Kong, Taiwan, Korea, and the Philippines.

According to Muhammad's testimony, they poured out the contents of 14 contact lens solution bottles and then filled them with concentrated nitromethane, an inexpensive explosive chemical, readily available in the Philippines.[40] Muhammad described how he had carefully removed the tops of the contact lens solution bottles without breaking the plastic seals, and then put back the tops after filling the bottles. While he traveled through airport security carrying 13 of the nitromethane-filled bottles in his bag, Yousef carried one. Muhammad and Yousef decided not to check any luggage, since they did not plan on doing so during the operation they were planning. To test his ability to clear airport security carrying a detonator, Muhammad decided to carry a bolt, which he taped to the arch of his foot and then covered with a sock. When searched by airport authorities, he was asked to undress, but while he was asked to remove his shoes, the police did not insist that he take off his socks. To deceive airport security, both men also decided to wear clothing with metal in it, such as buttons and accessories, and jewelry.

For his rehearsal, Yousef boarded Philippines Airlines Flight 434 from Manila to Narita, Tokyo (via Cebu, in the Philippines) on December 12, 1994. From the components he carried on board—nitromethane in contact lens solution bottles, a detonator in his shoe, and a Casio watch with a timer—he improvised an explosive device, placed it under his seat, and deplaned in Cebu. Although the explosion made a hole in the fuselage, resulting in the death of one passenger and injuries to several others, the plane did not explode. Afterward, while Yousef continued to refine the effectiveness of a miniature explosive device, an accidental fire led the police to raid his apartment in Manila.

The police arrested Abdul Hakim Murad, an al Qaeda accomplice of Yousef's who had trained in several aviation schools,[41] and Murad's testimony revealed the full scope of the plot.

Shortly after September 11, another affiliate of the al Qaeda network also attempted to detonate a bomb in flight, this time over the Atlantic. On December 22, 2001, Richard Reid boarded American Airlines Flight 63 from Paris to Miami, carrying 197 people. When the flight was halfway across the Atlantic, Reid tried to light a fuse connected to explosives concealed in the hollowed-out heel of his shoe. He was quickly overpowered by passengers and crew members and then sedated by an onboard doctor until the flight was diverted to Boston's Logan Airport, where he was arrested.[42] At his trial, Reid pleaded guilty to trying to blow up an airliner with explosives hidden in his shoes, declaring himself a follower of Osama bin Laden and an enemy of the United States.[43]

On August 24, 2004, Siberia Airlines Flight 1047 left Domodedovo International Airport in Moscow, bound for Sochi, and roughly an hour later, Volga-AviaExpress Flight 1303 left the same airport bound for Volgagrad. At approximately 11 P.M. local time, according to the official investigation, a Chechen female suicide bomber named Satsita Dzhebirkhanova blew up the Siberia Airlines flight, and another Chechen female suicide bomber named Amanta Nagayeva blew up the Volga-AviaExpress flight. Chechen field commander Shamil Basayev took responsibility for the bombings in an open letter published on the Chechen separatists' Web sites less than a month later, noting that the bombings had cost his organization roughly $4,000—a small price to pay for killing 89 people, and an indication of how terrorists will continue to try and exploit any weaknesses they can identify in the aviation sector.[44]

Another example of the innovative tendencies of terrorists was seen in the attempt to blow up several transatlantic flights in the summer of 2006. While details are still emerging from this ongoing investigation, information already revealed by authorities indicates the frightening sophistication of this plot. This was very different from the amateurish Richard Reid attempt to detonate a shoe bomb aboard a flight in mid-Atlantic. Here, the terrorists intended to simultaneously detonate homemade bombs on at least 10 U.S. airliners while en route from London to the United States. According to U.S. Homeland Security Secretary Michael Chertoff, the suspects planned to smuggle a relatively small amount of homemade liquid explosives on board disguised as sports drinks.[45] "If they had succeeded, there could have been thousands of lives lost and an enormous economic impact with devastating consequences for international air travel."[46]

The plot was disrupted after arrests in Pakistan led United Kingdom and U.S. officials to a British Muslim terrorist cell planning to attack American targets. Airports in the United States and the United Kingdom were put on red alert (meaning that an attack could be imminent) and all liquids were banned from carry-on luggage as suspects were picked up, including 24

British-born Muslims and seven Pakistanis.[47] After government authorities tested the explosive liquids, they determined what quantity of liquid explosives could pose a risk if smuggled on board flights, leading to a three-ounce limit for carry-on bags. Passengers are still restricted when bringing liquids on board, and those rules may remain in place forever.[48]

Following the attempt to carry out simultaneous suicide attacks on commercial aircraft, U.S. airports remained on high alert for nearly a year. Among law enforcement professionals, the plot resulted in a heightened awareness of the creativity and innovative thinking of today's terrorists. Thus, when an Arabic-language video clip was discovered on the Internet in October 2007, illustrating how to convert a remote-control toy car into a detonator for a bomb, Transportation Security Administration (TSA) officers nationwide stepped up their scrutiny of passengers carrying remote-control toys aboard airplanes.[49] Indeed, we should not be surprised in the future when other ordinary items that passengers would expect to carry on board without difficulty are suddenly given additional scrutiny because new intelligence indicates they could possibly be used in a terror plot. The dimension of creativity and innovation is a hallmark of the most lethal terrorist groups and has been demonstrated by another type of in-flight attack: the surface-to-air missile.

### Surface-to-Air Attacks

Violent groups have used (or at least attempted to use) shoulder-fired surface-to-air missiles (SAMs) against military aircraft for several decades.[50] During the Soviet occupation of Afghanistan, the Mujahideen fighters found progressively more success each year in shooting down military aircraft with U.S.-made Stinger missiles. Other examples include the IRA's attempt to use SAMs against British helicopters in Northern Ireland (an effort that was actually centered around a small handful of talented and well-connected sympathizers in the United States) and the infamous 1993 "Black Hawk Down" event in Somalia. And more recently, we have seen numerous instances of SAMs used by insurgents in Iraq and Afghanistan to damage—and in some cases destroy—U.S. and coalition aircraft.

Unfortunately, we have also seen numerous attempts by terrorists and others to use SAMs against civilian aircraft as well. Like in-flight bombings, SAMs have been used by groups that are clearly more interested in killing than negotiating. For example, on September 3, 1978, an Air Rhodesia flight was shot down by guerrillas using a Strela 2 missile (a Russian-made, man-portable SAM); 18 of the 56 passengers survived the crash, but 10 of the survivors were summarily executed by the guerrillas at the crash site. On February 12, 1979, another Air Rhodesia plane following the same flight path was shot down using the same type of weapon; none of the 59 passengers or crew members survived.

More recently, in November 2002, an Israeli charter jet departing the Mombasa, Kenya, airport narrowly avoided being hit by two shoulder-fired missiles

fired by assailants believed to be affiliated with al Qaeda.[51] A year earlier, according to Israeli and Czech officials, a terrorist plan to bring down an El Al jet carrying Israeli Foreign Minister Shimon Peres failed when the weapon malfunctioned.[52] In August 2003, the FBI announced the arrest of a British arms dealer on charges that he tried to complete the sale of a SAM with the understanding that it was going to be used to shoot down an American commercial airliner.[53] The Russian-made SA-18 shoulder-fired missile had been loaded onto a ship in Russia and then smuggled into a port in Newark, New Jersey. Two other defendants were arrested—a New York City jeweler and a Malaysian businessman, who had helped arrange the money transfer for the sale of over 50 more of these missiles.

And in March 2007, a Belarusian flight charted by the United Nations and loaded with humanitarian aid and supplies was shot down as it approached the airport at Mogadishu, Somalia. Just two weeks earlier, a UN flight carrying Ugandan peacekeepers to Mogadishu had made a successful emergency landing after being struck by a rocket-propelled grenade (RPG). In short, the global proliferation of missile technology has contributed to another critical area of vulnerability for commercial aviation. As a result, firms in Israel, the United States, and elsewhere are developing new kinds of missile-warning systems for passenger airplanes (based on systems widely used for military aircraft) and are exploring technology that will deflect missiles that have been launched. But there is much work to be done before the threat from surface-to-air missiles is adequately mitigated.

### Airplanes as Guided Missiles

The use of airplanes as guided missiles is yet another example of the type of aviation attack in which terrorists have no concern for negotiating. As with in-flight bombings and missiles, the purpose of this tactic is to kill all the passengers and as many others on the ground as possible. These are also suicide terrorist attacks, which are themselves a vicious form of violence that is becoming increasingly deadly and more difficult to counter effectively. As a weapon of asymmetric warfare, the obvious attraction to terrorists is that a plane loaded with jet fuel can be converted into a guided missile and used to cause tremendous damage and loss of life, as demonstrated so aptly on September 11, 2001. But what most Americans don't realize is that September 11 was not the first instance of this type of attack.

For example, in 1986, a Pan Am flight in Karachi was hijacked by four members of the infamous Abu Nidal Organization; reportedly, the terrorists' intention was to crash the plane into the Israeli Defense Ministry in Tel Aviv.[54] And in December 1994, four members of the Algerian Armed Islamic Group (GIA), posing as airline employees, hijacked Air France Flight 8969 from Algiers to France. French authorities deceived the terrorists into thinking the plane did not have enough fuel to reach Paris, and diverted it to Marseille, where a French antiterrorist force stormed the plane, freed the

plane's 283 passengers, and killed all four terrorists.[55] During the hijacking, an anonymous informant had warned the French consulate in Oran, Algeria, that the plane would be used as a "flying bomb that will explode over Paris."[56] The French authorities believe that the terrorists' intention was to crash the aircraft into the Eiffel Tower.

But the attacks of September 11, 2001, are considered by most scholars as a watershed event in both terrorism and aviation security. Here, a relatively small group of 19 al Qaeda members (with a supporting cast of maybe a few dozen more, who provided the logistics and financing necessary for the attack) exploited the vulnerabilities in our airport and airline security procedures to smuggle relatively small (but very lethal) box cutters aboard four airplanes. Once in flight, each team proceeded to kill one or more passengers in order to control the others by fear; then they stormed the cockpits and killed the flight crew. Three of the teams succeeded in their mission, flying the planes into the World Trade Center and the Pentagon; the fourth plane was en route to Washington, DC, when a brave group of passengers attempted to regain control of the plane, to which the hijackers responded by sending the plane into a terminal nose dive and crashing it in a field near Shanksville, Pennsylvania.[57]

Certainly, lessons have been learned from September 11 and previous attempts to use airplanes as guided missiles. And yet by some measures, the threat remains. In September 2005, a university student from Egypt was ordered held without bond after authorities found a pilot's uniform, a chart of Memphis International Airport, and a DVD titled *How an Airline Captain Should Look and Act* in his apartment. According to FBI testimony, Mahmoud Maawad, who is in the United States illegally, had also ordered $3,000 in aviation instructional materials, including DVDs titled *Ups and Downs of Takeoffs and Landings*, *Airplane Talk*, *Mental Math for Pilots*, and *Mastering GPS Flying*, from Sporty's Pilot Shop in Batavia, Ohio.[58] More recently, authorities from the Saudi Arabian interior ministry arrested 172 suspected terrorists in April 2007, after uncovering a plot to hijack several airplanes and fly them into oil facilities and other critical infrastructure targets in that country.[59] Overall, the use of airplanes as guided missiles has been very rare, perhaps because of the complex challenges this tactic poses to terrorists. Nonetheless, given the lessons of the past, we should anticipate that others will attempt this type of attack at some point in our future.

### Attacks against Airports

In addition to the many forms of attacks against airlines, it must be recognized that airports have also been targets of political violence. The Israeli national airline El Al was a target at the Lod airport in Tel Aviv in 1972. Pan Am and Lufthansa airlines were targets of attacks at the Rome airport in 1973, and several airliners were targeted that same year at the Paris-Orly airport. The trend continued into the 1980s, with airport attacks in Greece, Sri Lanka, and the Philippines and a pair of very dramatic terrorist strikes against

the Vienna and Rome airports in 1983.[60] In 1999, a plan to bomb the Los Angeles International Airport (LAX) on New Year's Eve was uncovered when an al Qaeda operative from Montreal—Ahmed Ressam—was apprehended by customs officers as he attempted to cross the border from Canada into the United States at Port Angeles, Washington. In July 2002, a gunman stormed the El Al ticket counter at LAX and killed two Israelis before being shot by security guards. And on June 30, 2007, a burning car loaded with gas cylinders was driven by al Qaeda–Muslims into the front door of the main terminal building at Glasgow International Airport in Scotland.

These busy hubs of commerce, particularly international airports, present their own unique security challenges. According to a recent study by the National Academy of Sciences, airports were designed to facilitate travel and trade, not enforce security.[61] After decades of violence, airports in Europe and some parts of the Middle East have come to rely on heavily armed police officers in terminals in order to have a dissuading effect on potential terrorists. In contrast, prior to September 11, U.S. airlines relied on standard airport police measures, and security at major airports remained generally lax, especially in terms of apron access through unguarded cargo areas.[62] But things are very different today.

For example, in Phoenix, Arizona, new concrete barriers have been installed to shore up the perimeter fence at Sky Harbor International Airport.[63] Officials set up hundreds of the blockades along portions of the fence line after a June 2005 incident in which a man drove through an open gate into a fire station parking lot and smashed through a wrought-iron fence to get onto the taxiway.[64] Similarly, in August 2005, Massachusetts Port Authority (Massport) officials unveiled a $14.5 million upgrade of security at Logan Airport in Boston (the departure point of two of the hijacked planes on September 11). In addition to constructing a 1.6-mile-long, 10-foot-high concrete wall, topped with razor wire (replacing the chain-link fence that currently surrounds the airport), Massport will also begin using infrared cameras to monitor Boston Harbor and will give GPS-outfitted cell phones to shell fishermen in the harbor, to help ensure that potential terrorists can't pose as fishermen to conduct surveillance on Logan in preparation for a possible attack.[65] Indeed, throughout the history of attacks against aviation targets, governments have responded with an increasing diversity of security measures.

## GOVERNMENT RESPONSES TO AVIATION SECURITY THREATS

Government responses to the many kinds of threats to the aviation sector range from baggage screeners and air marshals to "target hardening" (physical terminal security) measures. In all the cases of thwarted plots described in this chapter, as well as many that have not been reported publicly, quality intelligence has been a critical part of the government's success in averting potential disasters and will undoubtedly continue to play a vital role in the

response to the increasingly broad array of potential threats to the worldwide aviation sector.

The result of the 1970 bombings of the Tel-Aviv bound Swissair and Austrian Airlines flights was the immediate implementation of measures for all Israel-bound aircraft belonging to El Al and other international airlines. This included the use of air marshals. Yet, as Guillaume de Syon observes, despite a series of hijackings in the early 1960s between the United States and Cuba, no metal detectors were installed at airports, and luggage searches, when carried out, were often done for the purpose of finding contraband, not weapons.[66] The intervention of the Israeli commandos during the 1984 hijacking of Air France Airbus A300 was, in a way, an acknowledgment of failure to maintain airline security. In 1989, Pan Am 103's crash at Lockerbie, Scotland, proved a watershed in the development of new security measures for airlines in Europe. It became clear that airlines, U.S. or foreign, needed to closely follow governmental threat assessment directives, implement positive passenger-baggage reconciliation, and X-ray or search any piece identified as unaccompanied.[67]

In August 1989, following the Lockerbie incident, President George H. W. Bush established the President's Commission on Aviation Security and Terrorism.[68] The report of this commission, issued in May 1990, provided 64 recommendations, which were incorporated into the Aviation Security Improvement Act, signed into law in November 1990. This act established the position of director of intelligence and security within the (then) Office of the Secretary of Transportation, with responsibility for transportation security strategic planning, policy formulation, countermeasure coordination, interagency liaison, and a variety of intelligence duties. However, throughout the 1990s, checked baggage and passenger screening, explosive trace detection devices (ETDs), and other critical components of the aviation security system were the responsibility of the airline industry. According to Guillaume de Syon, the federal government subsidized the costs of training in ETDs and the installation and maintenance of ETDs and their operators, and by December 2000, over 700 devices and systems had been installed at airports throughout the United States.[69] After September 11, a new raft of measures were taken to strengthen aviation security, including new TSA screeners and machines, armed pilots, and an increased presence of air marshals.

And yet, challenges remain, as evidenced in the many news stories that have appeared in the past few years. For example, in June 2005, an unidentified woman placed her carry-on bags on the X-ray machine at the security checkpoint at Pittsburgh International Airport and then squeezed through an open space, not more than a foot wide, between the machine and the walk-through metal detectors.[70] Unnoticed, she then successfully boarded a plane to Houston, Texas. As a result, TSA officials installed chains between the checkpoint's detectors and X-ray machines to prevent people from slipping between the two pieces of equipment, and the agency eventually plans to install Plexiglas in any open areas that could potentially be used to slip past security.[71]

In December 2003, a Northwest Airlines mechanic discovered a startling vulnerability in the high-tech cockpit doors that had been installed in all planes as a barrier to prevent a repeat of September 11, when terrorists entered cockpits and commandeered four planes. The maintenance mechanic working inside an Airbus A330 jet on the ground in Minneapolis pushed the microphone button to talk into his handheld radio.[72] Though he hadn't touched the cockpit door, he heard the sound of its lock operating. Radio interference from his walkie-talkie had scrambled the electronics inside the door's locking mechanism. This discovery sparked a secretive and expensive engineering effort to fix a security glitch that affected the Airbus-designed fortified cockpit doors of nearly 400 airplanes. In May 2004, Boeing learned from three airline customers that the same problem was affecting an additional 1,700 jets.[73] While these problems were eventually fixed, they revealed once again that our propensity to rely on technology for security is, at best, an imperfect solution.

Meanwhile, in November 2005 a Government Accountability Office (GAO) report revealed that nearly all of the cargo in the nation's aviation system goes unchecked for explosives, and that policies aimed at thwarting the placement of cargo bombs on passenger planes are flawed.[74] According to the report, passenger planes carried 6 billion pounds of cargo in 2004, and only "a very small percentage" is inspected. The GAO called upon the TSA to close cargo security loopholes, including conducting a study to track the steps through which cargo goes from shippers to the belly of an airplane. In 2004, members of the House of Representatives requested that the TSA consider mandating the inspection of all cargo before it is put on passenger planes, but the TSA objected, noting that it would cost the government $3.6 billion over 10 years and could delay cargo shipments.[75]

Clearly, significant strides have been made in aviation security in response to various kinds of terrorist attacks throughout the last four decades. The aftermath of the September 11 attacks reflected the most dramatic changes yet. According to the *9/11 Commission Report*, government officials suffered from a "failure of imagination" that precluded a consideration of the possible threat of terrorists using planes as guided missiles. Even more disturbing is the fact that, as described earlier in this chapter, an incident in 1994 clearly demonstrated the intention among Islamic radical terrorists to carry out this very kind of attack against the people of France. We should have known from history and from intelligence that the use of planes as missiles was a possibility. Thus, when it comes to the future of aviation security, perhaps the most pressing question is this: What will the "failure of imagination" of tomorrow be?

## CONCLUSION AND IMPLICATIONS FOR THE FUTURE

Despite the broad array of security measures that governments have implemented in response to attacks over the past several decades, there is little reason to believe that terrorists will not continue to target commercial aviation.

The present analysis of the historical record suggests at least three primary reasons why aviation security is still threatened: (1) the nature of terrorist organizations; (2) the modern aviation environment; and (3) the nature of our response to the threat.

First, terrorists—at least the most sophisticated and lethal ones—learn from each other and are continually devising new and creative ways to wreak havoc and murder.[76] Attacks that have not yet occurred but that we are ill prepared for could include using an aircraft's in-flight oxygen circulation system to infect the passengers and crew with biological pathogens, or unleashing a deadly chemical agent in the cockpit that renders the pilot and crew unconscious and causes the plane to crash. One could imagine a rash of in-flight food poisonings (furthering the notion of in-flight meals as pointless) or attempts to corrupt signals from the air traffic control system in order to redirect planes into each other or crash land in low-visibility conditions. As mentioned earlier in this chapter, TSA officials were alerted in October 2007 about the possibility that common remote-control toys could be used to detonate a bomb as part of a terror plot. The additional scrutiny was put in place in part due to intelligence but also because—as one federal official noted—remote-control toys might have been used already by terrorists in Sri Lanka and India.[77] Overall, as Bruce Hoffman recently observed, we should anticipate that terrorists are constantly searching for new vulnerabilities and adapting and adjusting to our countermeasures.[78]

Second, the contemporary aviation environment—an ever-expanding global system, with growth in the number of airplanes in the sky carrying passengers and cargo, the size of these airplanes (like the new Dreamliner), and the number of locations to which you can now fly—offers more soft targets of opportunity. Terrorists—much like criminals, insurgents, and other violent nonstate actors—exploit vulnerabilities in the systems they target, and these systems are only as strong as their weakest link. Thus, as the commercial aviation system became more globally interconnected, the overall impact of the measures taken at U.S. airports had an important but relatively decreased impact over time in terms of strengthening the aviation sector worldwide. While airports in Europe and North America responded to the rash of hijackings and bombings during this period, many other countries—particularly in Africa and Asia—found it difficult to impose most of the costly security measures, thus providing vulnerabilities that could be exploited. Any system is only as secure as its weakest link, and a globalized aviation system that includes numerous developing countries plagued with substandard security capabilities, corruption, bribery, and weak governance is inherently weak. At the same time, the Internet provides worldwide access to all types of information that could be useful to terrorists, including flight schedules, specific details and diagrams of both aircraft and airports, and reports of successful terrorist tactics and countermeasures developed by governments.

Finally, and in a related area of concern, the nature of our response to the global threat to aviation relies on the strength of the partnership between governments and the private sector and on what each of these partners is willing

to do. In general, the aviation sector is driven by free market competition, and thus airlines must maintain an emphasis on convenience and cost savings, making investment in costly security measures relatively difficult. Among governments, we have seen bloated bureaucracies, a lack of intelligence sharing across borders (and often even across agencies within a single nation), and an overarching tendency to implement security policies in response to an attack that has already occurred, rather than to embrace preventive measures that might help avoid a type of attack that has not yet occurred.

Beginning in the late 1960s, increasingly robust layers of security measures were put in place in response to the kinds of hijackings described earlier in this chapter. Yet, after four decades of such efforts the aviation sector was still vulnerable, as demonstrated by the events of September 11, 2001. Since then, we have seen additional security layers such as reinforced cockpit doors, armed pilots, more air marshals, and an overall increased awareness of the threat worldwide. So, perhaps the post–September 11 security environment may be one in which the threat to aviation is lower than it has been in the past, but in-flight bombings are still occurring, and in the summer of 2006 a major plot to destroy multiple transatlantic flights was narrowly averted. Responding to events is insufficient; modern aviation security requires preventive measures, even some that may inconvenience passengers and create some inefficiencies, as well as a breadth and depth of intelligence gathering and sharing worldwide.

Further, there has too often been a tendency among government officials to underestimate the innovative nature of terrorists. Terrorism is a form of asymmetric warfare. In any asymmetric warfare situation, the statistically weaker enemy will try to attack its stronger opponent in ways the opponent does not expect. The threat posed by thinking enemies requires a robust government response that does more than harden targets. In addition to examining the potential capabilities of terrorists to do harm to others by targeting airplanes and airports, we must commit ourselves to the study of terrorist ideologies, strategies, and motivations, and we must educate both law enforcement and intelligence agencies in all countries about how our enemies might try to "game the system" and exploit new, perhaps even hidden, vulnerabilities in aviation security. Only then will we be able to respond to the threat with greater sophistication and success.

## ACKNOWLEDGMENTS

The views expressed in this chapter are those of the author and do not purport to reflect the position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. government.

## NOTES

1. Mark Juergensmeyer, *Terror in the Mind of God: The Global Rise of Religious Terrorism* (Berkeley: University of California Press, 2000).

2. For example, see David C. Rapoport, "The Four Waves of Rebel Terror and September 11," *Anthropoetics* 8, no. 1 (Spring/Summer 2002), for an excellent description of four waves of modern terror and the ways in which the evolution of certain technologies has shaped these waves.

3. Brian Jenkins, "The New Age of Terrorism," *The McGraw-Hill Homeland Security Handbook*, ed. David G. Kamien (New York: McGraw Hill, 2006).

4. Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), 189.

5. Richard M. Wrona, Jr., "Beginning of a War: The United States and the Hijacking of TWA Flight 847," in *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, vol. 3, ed. James J. F. Forest (Westport, CT: Praeger, 2007), 38.

6. Brigitte L. Nacos, "Communication and Recruitment of Terrorists," in *The Making of a Terrorist*, vol. 1, *Recruitment*, ed. James J. F. Forest (Westport, CT: Praeger Security International, 2005).

7. Brigitte L. Nacos, "Mediated Terrorism: Teaching Terror through Propaganda and Publicity," in *The Making of a Terrorist*, vol. 2, *Training*, ed. James J. F. Forest (Westport, CT: Praeger Security International, 2005).

8. Cindy R. Combs, "The Media as a Showcase for Terrorism," in *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*, ed. James J. F. Forest (Lanham, MD: Rowman & Littlefield, 2006).

9. Alex Schmid, "Terrorism and the Media: The Ethics of Publicity," *Terrorism and Political Violence* 1 (1989): 539–65.

10. Combs, "The Media as a Showcase for Terrorism."

11. Ibid.

12. Joanne Wright, "Countering West Germany's Red Army Faction: What Can We Learn?" in *Countering Terrorism and Insurgency in the 21st Century*, vol. 3, ed. James J. F. Forest, 27591 (Westport, CT: Praeger, 2007).

13. Nicolás Urrutia Iriarte and Román D. Ortiz, "A Slow Road to Victory: Counterinsurgency and Strategic Innovation in Colombia," in *Countering Terrorism and Insurgency in the 21st Century*, vol. 3, ed. James J. F. Forest, 310–33 (Westport, CT: Praeger, 2007).

14. Sammy Salama, "Unraveling Al-Qaida's Target Selection Calculus," in *Terrorism and Political Islam: A Textbook for the FBI New Agent Training Program*, ed. James J. F. Forest, 41–51 (Quantico, VA: FBI, 2007).

15. Akhu Man Ta'a Allah, "What Else Is There to Say about September 11," *Sawt al-Jihad* (Voice of Jihad), vol. 26, 35–42, quoted in Salama, "Unraveling Al-Qaida's Target Selection Calculus," 42.

16. Salama, "Unraveling Al-Qaida's Target Selection Calculus."

17. An extensive chronology of aviation attacks is provided in the chapter by Mary Schiavo in this volume.

18. This description of the event is from Hoffman, *Inside Terrorism*, 63–66, 68.

19. Ibid.

20. For more on the organizational learning attributes of terrorist groups, see *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*, ed. James J. F. Forest (Lanham, MD: Rowman & Littlefield, 2006), especially 1–109.

21. Guillaume de Syon, "Aviation Security," in *Homeland Security: Protecting America's Targets*, vol. 3, ed. James J. F. Forest (Westport, CT: Praeger, 2006), 270. An online description of this event is also available at http://en.wikipedia.org/wiki/Japan_Airlines_Flight_472.

22. For a complete account of this event, see Wrona, "Beginning of a War," 35–51.

23. Ibid; Also see Hoffman, *Inside Terrorism*, 174–79, 186–87, 190, and 194.

24. "Indian Hijack Drama Over," *BBC News*, December 31, 1999, http://news.bbc.co.uk/2/hi/south_asia/584729.stm (cited in de Syon, "Aviation Security").

25. For a complete account of this hijacking and the rescue operation, see J. Paul de B. Taillon, *Hijackings and Hostages: Government Responses to Terrorism* (Westport, CT: Praeger, 2002), 109–25.

26. Ibid.

27. For a complete account of this hijacking and the rescue operation, see Taillon, *Hijackings and Hostages*, 125–38. it is referenced in Hoffman, *Inside Terrorism*, 77.

28. See http://middleeastfacts.com/middle-east/popular-front-for-the-liberation-of-palestine.php.

29. Hoffman, *Inside Terrorism*, 234–35.

30. In addition to the chapter by Mary Schiavo in this volume, ee the list and descriptions of commercial airliner bombings available on the Aerospace Web site, http://www.aerospaceweb.org/question/planes/q0283.shtml.

31. See the list and descriptions of commercial airliner bombings available on the Aerospace Web site, http://www.aerospaceweb.org/question/planes/q0283.shtml.

32. De Syon, "Aviation Security."

33. "Bombings in Air: From Barbados to Scotland," *New York Times* in coordination with the Associated Press, December 29, 1988, p. A1. See also the list and descriptions of commercial airliner bombings available on the Aerospace Web site, http://www.aerospaceweb.org/question/planes/q0283.shtml.

34. "Closely Watched Planes," *Time*, March 9, 1970, http://www.time.com/time/magazine/article/0,9171,878779,00.html.

35. Hoffman, *Inside Terrorism*, 262–66.

36. Ibid., 189.

37. Ibid., 262–66.

38. For a complete account of this plot, please see Rohan Gunaratna, "Oplan Bojinka," in *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*, ed. James J. F. Forest (Boulder, CO: Rowman & Littlefield, 2006).

39. Further, following his capture in Rawalpindi, Pakistan, in March 2003, Khalid Sheikh Muhammad told his American interrogators that the genesis of September 11 was Oplan Bojinka. Debriefing of Khalid Sheikh Muhammad, Central Intelligence Agency, April 2003. Cited in Gunaratna, "Oplan Bojinka."

40. This account is from Debriefing of Khalid Sheikh Muhammad, Central Intelligence Agency, April 2003. Cited in Gunaratna, "Oplan Bojinka."

41. Debriefing of Abdul Hakim Murad, Special Investigations Group, National Police Commission, February 13, 1995, 2 and 3. For more on this, see national Commission on Terrorist Attacks upon the United States, *Report of the National Commission on Terrorist Attacks upon the United States (9/11 Commission Report)* (Washington, DC: Government Printing Office, 2004), 507, note 8. Available online at http://www.gpoaccess.gov/911 and http://www.911commission.gov.

42. "U.S. Crew Recalls 'Shoe Bomb' Ordeal," *BBC News*, June 20, 2002, http://news.bbc.co.uk/2/hi/europe/2055003.stm.

43. "'Shoe Bomber' Pleads Guilty," *BBC News*, October 4, 2002,http://news.bbc.co.uk/2/hi/americas/2298031.stm.

44. Nick Paton Walsh, "Russia Blames Chechen Sisters for Suicide Bombings," *Guardian*, April 22, 2005, http://www.guardian.co.uk/international/story/0,,1465936,00.html;

and "Explosions Led to Russia Crashes," *CNN World Edition*, August 30, 2004, http://edition.cnn.com/2004/WORLD/europe/08/30/russia.planecrash/index.html.

45. According to authorities, the formula included three components that would be assembled in flight. The main explosive was to be hexamethylene triperoxide diamine (HMTD), a homemade explosive that has been used in several recent terrorist attacks. Another homemade explosive was to be used as an explosive initiator: triacetone triperoxide (TATP), which can be made from ordinary commercial items like hair treatments, a car battery, drain cleaner, and nail polish remover. The third part of the formula involved an improvised detonator made from disposable cameras. Scientists at Sandia National Laboratory conducted a test using the formula, and when a small amount of liquid in a container was hit with a tiny burst of electrical current, a large explosion followed. See "Plot Would Have Killed Thousands: Homeland Security Secretary Michael Chertoff Offers Chilling Details about 2006 Airplane Plot and Current Terror Threats," *ABC News*, 6 August 2007, http://abcnews.go.com.

46. "Plot Would Have Killed Thousands."

47. Ibid.

48. Ibid.

49. Eric Lipton, "Airport Security Alert for Toys with Remotes" *New York Times*, October 2, 2007, http://www.nytimes.com/2007/10/02/us/nationalspecial3/02tsa.html?th&emc = th.

50. Of course, it must be recognized that far more commercial airplanes have been shot down by military forces (usually—but not always—by mistake) than by any terrorists or other nonstate actors.

51. A statement attributed to al Qaeda claimed responsibility. See "Kenya Missile Attack Sparks New Urgency," *CNN*, December 4, 2002,http://archives.cnn.com/2002/WORLD/meast/12/03/missile.defense/index.html.

52. "Kenya Missile Attack."

53. FBI Press Release, August 13, 2003, http://www.fbi.gov/pressrel/pressrel03/igla081303.htm.

54. Hoffman, *Inside Terrorism*, 280–83.

55. Senate Intelligence Committee Testimony, September 18, 2002; Thomas Sancton, "Anatomy of a Hijack," *Time*, December 26, 1994; and Hoffman, *Inside Terrorism*, 87, 281.

56. Senate Intelligence Committee Testimony, September 18, 2002.

57. A full account of these events is provided in the official *9/11 Commission Report*, http://www.911commission.gov.

58. "Student Arrested after Pilot Uniform Found," *Washington Post*, 16 September 2005, http://www.washingtonpost.com/wp–dyn/content/article/2005/09/16/AR2005091601286_pf.html

59. "Saudis Foil 'Air Attack Plotters,'" *BBC News*, April 27, 2007, http://news.bbc.co.uk/2/hi/middle_east/6599963.stm.

60. De Syon, "Aviation Security," 269.

61. These characteristics were drawn from a major study by the National Academy of Sciences, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, DC: National Research Council, October 2002), 21213. Cited in Hoffman, *Inside Terrorism*.

62. De Syon, "Aviation Security."

63. Portions of this discussion have appeared in the introductory chapter of *Homeland Security: Protecting America's Targets*, vol. 3, *Critical Infrastructure*, ed. James J. F. Forest (Westport, CT: Praeger, 2007).

64. "Permanent Barriers to Go Up at Arizona Airport," *Arizona Republic*, October 17, 2005, http://www.azcentral.com/news/articles/1017security17.htm.

65. "Massport Plans Logan Airport Security Upgrade," Associated Press, August 24, 2005, http://www.boston.com/news/local/massachusetts/articles/2005/08/24/massport_plans_logan_security_upgrade.

66. De Syon, "Aviation Security."

67. Ibid.

68. This section on aviation security is drawn directly from the Transportation Security Administration's *Report to Congress on Transportation Security*, March 31, 2003, http://www.tsa.gov.

69. De Syon, "Aviation Security," 264.

70. "Chains Go Up to Prevent Airport Security Lapses," *Pittsburgh Post-Gazette* (PA), July 7, 2005,http://www.post–gazette.com/pg/05188/534086.stm.

71. Ibid.

72. "Glitch Forces Fix to Cockpit Doors," *Seattle Times*, October 6, 2005, http://archives.seattletimes.nwsource.com/display?20051006cockpitdoor.

73. Ibid.

74. Thomas Frank, "Report: Most Airline Cargo Isn't Checked for Explosives," *USA Today*, 16 November 2005.

75. Ibid.

76. For more on this, see Forest, ed., *Teaching Terror*.

77. Lipton, "Airport Security Alert for Toys with Remotes," http://www.nytimes.com/2007/10/02/us/nationalspecial3/02tsa.html?th&emc=th.

78. Bruce Hoffman, personal communication and presentation at West Point, September 14, 2007.

# CHAPTER 9

# Aviation Security and the Legal Environment

*Mary F. Schiavo*

Before undertaking any analysis of the aviation security legal environment, we need to remember three important things about aviation security. First, on September 11, 2001, the airlines were responsible for the security screening checkpoints and the screening of all persons and objects passing through the checkpoints into the "sterile" areas of the airport. They were responsible for the security of their passengers, their aircraft, and all parts of the airport under their control.[1] The government's role was merely to approve, disapprove, or require modification of the security program submitted by the aircraft operators.[2] The airports were responsible for the remainder of the security.[3]

Second, the September 11, 2001 hijackers were copycat killers. Everything the September 11 hijackers did had been done before. The September 11 hijackers were not the first terrorists to seize multiple aircraft and employ them as tactical weapons in suicide hijackings, to smuggle weapons and other dangerous items banned by the checkpoint security rules past security checkpoints to carry out hijackings, to force their way into cockpits, to be trained as pilots, to become anti-Western Islamist extremists, or to aim to destroy highly significant symbolic buildings inside the United States. And because everything they did had been done before, there were laws in place to thwart such criminals and, to varying degrees before September 11, 2001, the laws were thwarted.

Third, had the existing security laws in place on September 11, 2001, been followed and enforced, September 11 would not have happened. What's more, in the days and weeks and months before September 11, there had been multiple warnings to the airlines and airports, as in the July 17, 2001, *Federal Register*,[4] which warned of a likely terrorist attack on aviation but projected

the loss of 0.5 persons on the ground for each downed aircraft. A 2000 U.S. Government Accountability Office (GAO) report warned that "serious vulnerabilities in our aviation system exist and must be adequately addressed."[5]

The numerous weaknesses in the aviation security system, which were successfully exploited on September 11, 2001, by the 19 hijackers, included an inadequate prescreening process, lax checkpoint screening, and nonexistent in-flight security measures, among other vulnerabilities. Despite numerous attempts by the U.S. Department of Transportation Office of Inspector General and the Government Accountability Office to call attention to the problems, congressional oversight activities prior to September 11 had "focused overwhelmingly on airport congestion and the economic health of the airlines, not aviation security."[6] Despite years of warnings by the U.S. Department of Transportation and others regarding the failure of airline and airport security, and despite warnings of the coming attacks, many of which were posted publicly on official federal Web sites and elsewhere, the airlines and others remained more concerned about expense than about security.

Aviation security methodology, structures, and technology did not substantially change following the tragedy of September 11, 2001. The Transportation Security Administration (TSA) uses the methodology that the airlines used, but the TSA was tasked with developing a more professional armed security workforce obtaining the best available technology. Thus, the TSA and its parent agency, the Department of Homeland Security, presided over the federalization of the screener workforce, whose members, as federal employees, must be made up of citizens or other legal workers.

Federalization was perhaps the most visible manifestation of the massive shift away from an aviation security system based on airline responsibility to one in which primary responsibility rests with the federal government. But the most sweeping and insidious legislative change was that the shift in responsibility from the airlines to the government also carried with it an almost wholesale abrogation of liability. Responsibility that is not cloaked in federal officer qualified immunity and discretionary function immunity may be cloaked in contractor immunity. These immunities from, or limitations on, liability were bequeathed in a host of new laws passed with little or no notice given, even by the authorizing senators or members of Congress. The only operatives who were fully cognizant of these provisions were those special interest organizations and sponsoring elected and appointed officials who successfully placed such provisions in various pieces of legislation. Armed with names designed to dispel dissent, such as the SAFETY Act or Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, such legislation usually sailed through Congress with little scrutiny or dissent.

Therefore, one major effect of post–September 11 legislation is that there will be significantly less legal recourse for victims and the flying public when the next terrorist attack occurs. The insulation from liability of negligent or otherwise unsuccessful security providers is a result not only of the transfer of responsibility from private airlines to the federal government but also of

the liability protections granted to private individuals and companies under the SAFETY Act and other such legislation. We will examine the major legislative actions that have fundamentally transformed the legal landscape of aviation security since September 11 and the general state of aviation security law today.

## THE AIR TRANSPORTATION SAFETY AND SYSTEM STABILIZATION ACT OF 2001

Less than two weeks after the hijackings, President Bush signed into law the Air Transportation Safety and System Stabilization Act (ATSSA).[7] The effort to get this passed started on September 11, 2001, with what media reports describe as one of the largest, if not the largest, lobbying force ever assembled.[8] While senators and members of Congress watched the Pentagon burn, the World Trade Center towers fall, and a large dark hole spread in a field in Pennsylvania, special interest lobbyists dusted off a plan to avoid liability, a plan that had been hatched following the crash into the Atlantic Ocean of TWA Flight 800 on July 17, 1996, a crash that was initially thought to have been caused by a terrorist attack. The premise of the new legislation was that victims of terrorist attacks on aviation would seek payment from a government fund and would therefore not seek liability and accountability from the airlines that failed to meet their security requirements and allowed terrorist hijackers, saboteurs, air pirates, or bombers to board the aircraft. Another important part of the new legislation was a wholesale reform of the tort liability system, which had previously failed to be inserted into any state laws, much less subjected to public scrutiny or U.S congressional debate. Thus, while the hijackers may have failed to hit their Capitol Hill mark, the lobbyists did not miss.

To the public, the legislation was sold as legislation designed to save the airlines from bankruptcy due to the victims' lawsuits and to provide a benevolent fund for those hurt or killed in the attacks. In fact, the airlines, including most of those involved in the September 11 attacks, had been in seriously weak economic condition long before the hijackings. Well before September 11, 2001, the debt-to-capitalization ratios of many of these carriers were tantamount to functional bankruptcy. No airlines, security companies, airports, and/or any other aviation entities that failed to perform their jobs on September 11 will ever pay for their negligence. Congress left only one security company without liability protection—Argenbright Security. However, Argenbright was folded after September 11 with the goal of limiting any liability the company might pose to its parent firm, Securicor.[9]

Under hasty post–September 11 legislation, air carriers were to receive $10 billion in loans and $5 billion in compensation for direct and indirect financial losses incurred as a result of the attacks. The actual amounts of direct and indirect aid to carriers were many times greater. The draft legislation was modified to include the establishment of a Victim Compensation Fund (VCF) to

compensate the September 11 families. But the fund exacted a quid pro quo from the families of victims. Anyone completing an application for payment from the VCF would have to give up the right to sue the airlines, security companies, airports, aircraft manufacturers, and other such aviation entities, and the victim's life insurance, worker's compensation, and any other death or injury benefits would be subtracted from any VCF award.[10] In every state in the United States, the collateral source rule prohibits such deductions from victims' recovery from tort feasors. With no debate and little or no real cognizance of the actual provisions of this law, House members, senators, and the president injected tort reform into the compensation for the dead and injured.

Apart from these compensation provisions, the act also aided air carriers by temporarily capping their liability from lawsuits arising from other acts of terrorism occurring during the 180-day period following the enactment of the act. Air carriers could not be liable for victims' losses exceeding $100 million and the U.S. government would be responsible for liabilities above that amount.

## THE AVIATION AND TRANSPORTATION SECURITY ACT OF 2001

Two months after the attacks, in November 2001, Congress passed the comprehensive Aviation and Transportation Security Act (ATSA),[11] to improve aviation security and to attempt to correct the vulnerabilities exposed by the security breaches of September 11. At the core of this legislation was the establishment of a massive new federal organization, the Transportation Security Administration (TSA), within the Department of Transportation. In addition, ATSA federalized the screener workforce and expanded the Federal Air Marshall Program by requiring deployment of air marshals on all high-risk flights, as determined by the secretary of transportation. Prior to September 11, there were only 33 air marshals,[12] and they were directed almost exclusively to international flights. Cockpit doors were also required to be hardened.

ATSA contained general provisions for cargo security, including 100 percent screening of checked baggage with explosive detection systems no later than December 31, 2002, or if unavailable, by alternative means such as a bag-match program, manual search, or search by canine explosive units. ATSA also mandated a cargo security system for all-cargo aircraft "as soon as practicable," but all-cargo security plans have lagged behind security plans on passenger aircraft and have still not been fully implemented as of fiscal year 2008.[13]

## THE HOMELAND SECURITY ACT OF 2002

In the aftermath of the September 11 attacks, a massive reorganization of the federal government was undertaken one year later. Under the provisions of the Homeland Security Act (HSA) of 2002,[14] the TSA was transferred to

the newly created Department of Homeland Security (DHS), whose objectives included guarding the nation's borders and preventing domestic terrorist attacks. The Immigration and Naturalization Service was also reorganized under the DHS as two separate agencies: one agency for immigration, naturalization, and visa services and another dedicated to border security and law enforcement. The nation's capability to identify and assess threats to the homeland was centralized within DHS under Information Analysis and Infrastructure Protection (IAIP).

Even more extensive than the organizational changes put in place by the HSA, although overshadowed by them, were far-reaching provisions limiting legal responsibility and liability for negligence and other failures. With the sunsetting in March 2002 of the provisions of the Air Transportation Safety and System Stabilization Act, which had provided for a $100 million tort liability limitation of air carriers for acts of terrorism and barred punitive damages, Section 1201 of the HSA extended these provisions through the end of 2003. In addition, Section 890 extended tort liability limits to air transportation security companies and their affiliates for claims relating to the September 11 hijackings.[15] The liability of such companies, whose contracts were assumed by the federal government in February 2002, is limited to the amount of liability insurance they held at the time of the attacks.

Section 1402 established a program of federal flight deck officers (FDOs), who are classified as employees of the federal government with respect to tort claims.[16] This section also immunized air carriers from damages arising from actions brought in federal or state court with respect to the "use of or failure to use a firearm" by flight deck officers. FDOs are similarly protected, except in the case of gross negligence or willful misconduct, in which case claims can be made against them under the Federal Tort Claims Act (FTCA).

The most sweeping preemption of state tort law in the Homeland Security Act is contained in Subtitle G, the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 or SAFETY Act. This protects sellers (more aptly described as suppliers) of qualified antiterrorism technology (QATT).[17] Among the dozens of corporations currently appearing on DHS's "Approved Product List for Homeland Security" are companies that provide airport security services and equipment, such as Securitas Holdings, Inc., Rapiscan Systems, Inc., Reveal Imaging Technologies, Inc., and Verified Identity Pass, Inc. QATT encompasses both services and products, ranging from vaccines to bomb and anthrax detection systems. QATT suppliers are protected against claims made under state tort law arising from an act of terrorism when such technology was "deployed in defense against or response or recovery from such an act." Plaintiffs are prevented from seeking redress in state courts. Instead, federal district courts have "original and exclusive jurisdiction" arising from such claims. Individuals may bring suit against the federal government, but they must surmount the many limitations on government liability imposed by the FTCA. Most notable is the discretionary function exception, protecting the government from liability whenever the government is allowed

to use discretion in deciding whether or not to take action, or when to use enforcement powers, investigate, or take other corrective action against a contractor or other entity.

The SAFETY Act dramatically reduces the tort liability of manufacturers and suppliers of homeland security technology. If an action is brought against a QATT seller or provider, regardless of whether it involves a federal or a nonfederal government customer, the act's "special rules" apply. Punitive damages may not be awarded, and noneconomic damages, such as damages for emotional pain, suffering, or loss of enjoyment of life, can be recovered only if the plaintiff suffered physical harm and only in an amount proportionate to the defendant's share of noneconomic damages for any such harm.

The collateral source rule, which prohibited the introduction at trial of evidence that a victim's damages had been partially compensated by a third party, such as personal life insurance or workers' compensation, some form of which is the law in every state, was eliminated under Section 863. Thus, any amount recovered by a plaintiff is reduced by the amount of any compensation, such as insurance payments or government benefits, that a plaintiff has received or is entitled to receive from a third party that is not a party to the legislation. The collateral source rule prevented tort feasors from undercompensating plaintiffs or avoiding personal responsibility altogether by arguing that the plaintiff had already been fairly compensated by a third party, such as the victim's own life insurance or other indemnity. In fact, many collateral source payors (such as for workers' compensation) do have rights to recover all or part of their payments, and some insurance policies have subrogation clauses, which provide for a lien against damages ultimately recovered.

Under the SAFETY Act, there is an explicit presumption of a government contractor defense, which can be rebutted only by proving that the seller had acted fraudulently or with willful misconduct when applying for QATT certification. Broadly defined, the government contractor defense protects government contractors from liability caused by failure to warn against a hazard or design defect in products meeting government specifications. This defense has traditionally been employed by government contractors defending against state tort claims involving equipment design defects. In *Boyle v. United Technologies Corp.*,[18] involving a state tort action for wrongful death of a pilot killed in a helicopter crash, the Supreme Court held that "liability of independent contractors performing work for federal government is [an] area of uniquely federal concern, despite absence of legislation specifically immunizing government contractors liable for design defects."

QATT sellers are covered by an individually determined liability cap based on their insurance coverage limits. Sellers are required to obtain liability insurance to satisfy potentially compensable third-party claims, but only up to a maximum amount "reasonably available from private sources on the world market *at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies*" (emphasis added). Liability for claims against a seller cannot exceed the amount of liability insurance coverage required by

the SAFETY Act, which may be set artificially low in order to avoid distorting the technology's sales price.

## THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

In the wake of the failure of those responsible to stop the September 11 hijackings and the fiasco regarding alleged information about Saddam Hussein's weapons of mass destruction (WMD) programs, landmark legislation was enacted in 2004 to restructure the U.S. intelligence community. Among other things, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 created the position of director of national intelligence (DNI), who was tasked with revamping the 16 agencies that make up the U.S. intelligence community.[19] In addition, a National Counterterrorism Center (NCTC) was established within the Office of the DNI.

The legislation included a number of significant provisions relating to aviation security as well. The new measures included the use of biometric identifier technology, expedited deployment of in-line baggage screening equipment, and replacement of trace-detection equipment with improved explosive detection system equipment. Other provisions intended to implement the recommendations of the 9/11 Commission dealt with improvements in air cargo security, as well as the prescreening and screening of passengers.

## SECURE FLIGHT

Computer Assisted Passenger Prescreening II (CAPPS II) was a terrorist watch list program designed and administered by the TSA to crosscheck all ticketed passengers against government records, such as other watch lists and law enforcement databases, as well as some private sector databases. With its introduction in 2002, CAPPS II was to be an improvement over its airline-administered predecessor, CAPPS I, which was only partially in place on September 11, 2001. Airline and security companies were only completing some of the CAPPS steps. CAPPS II was criticized by the Government Accountability Office (GAO) for errors in the targeting of passengers for additional screening, and by civil rights and other organizations for privacy concerns. It was terminated by the TSA in 2004 and replaced with a new domestic passenger screening program dubbed Secure Flight.

The purpose of Secure Flight is to prevent suspected terrorists from boarding aircraft. Watch list matching responsibility was transferred from aircraft operators to the TSA. Currently, the TSA performs passenger and baggage screening at U.S. airports, and aircraft operators perform watch list matching for passengers on domestic flights against government No Fly and Automatic Selectee lists. Under Secure Flight, airlines forward all flight passenger data, including reservation and itinerary information, to the TSA for screening and matching and then continue to update passenger information as it is received.

After encountering delays due to privacy concerns and security vulnerabilities in system software and hardware, DHS issued a Notice of Proposed Rulemaking (NPRM) for Secure Flight in August 2007. Under the NPRM, air carriers are required to provide passenger data to the TSA approximately 72 hours prior to departure and to immediately transmit or update information received inside the 72-hour window.

Air carriers will continue to conduct watch list checks for domestic flights until the full implementation of Secure Flight, which is expected to take place in late 2008. During the operational testing phase, air carriers that volunteer to participate will transmit passenger data to the TSA for comparison with the results of its own watch list matching.

## WATCH LISTS

The 9/11 Commission made several recommendations regarding passenger prescreening, including improving the use of No Fly and Automatic Selectee lists and other U.S. government terrorist watch lists.[20] Historically, administration of the No Fly list was the responsibility of the FBI. It was transferred to the FAA in 2001 and then later to the TSA, which split the list into No Fly and Automatic Selectee lists. As the names suggest, passengers on the No Fly list are refused boarding, while those on the Automatic Selectee list are required to undergo additional security screening before boarding.

Homeland Security Presidential Directive 6, signed on September 16, 2003, called for the establishment of a new organization to integrate and maintain a dozen different U.S. watch lists being maintained by various federal agencies. As a result, the Terrorist Screening Center (TSC) was created to manage a consolidated watch list of known and suspected terrorists and to be a single point of contact for screeners.

The goal of the consolidated system was to eliminate unnecessary duplication and streamline the access process for users. The watch list database has grown to over 700,000 records and continues to grow by an average of 20,000 records per month.

## INTERNATIONAL PASSENGER PRESCREENING

At the time of this printing, responsibility for the passenger prescreening system is split between two government agencies, with Customs and Border Protection (CBP) responsible for passengers on inbound and outbound international flights and TSA for domestic flights under Secure Flight. DHS established a Screening Coordination Office in 2006 to integrate procedures for prescreening domestic and international passengers, in order to avoid redundant watch list matching efforts and to ease the burden on aircraft operators. According to a GAO report, "CBP and TSA officials stated that they are taking steps to coordinate their prescreening efforts, but they have not yet made all key policy decisions."[21] DHS is developing a single "portal,"

through which air carriers will transmit passenger data for both domestic and international flights.

For international flights, air carriers submit Passenger Name Record information based on reservation data to the CBP, generally approximately 72 hours prior to departure. Air carriers also transmit passenger manifest information to CBP for watch list matching through the Advance Passenger Information System (APIS), generally after flight departure, which explains why there have been many diversions of inbound international flights. Once en route, if it is discovered that there is a passenger on the watch list, the flight is diverted to an airport where law enforcement agents can take custody of the suspect passenger and/or sort out any name confusion.[22] Once passenger data are received by CBP, it conducts watch list matching. DHS recently announced the adoption of a final rule regarding APIS, under which air carriers would transmit passenger manifests in batch form no later than 30 minutes prior to departure, or individual passenger manifest information not later than the securing of the aircraft doors. CBP also interviews high-risk passengers at foreign airports under the Immigration Advisory Program.[23] DHS proposes to eventually transfer all watch list matching functions for international flights to the TSA, allowing CBP to concentrate on border enforcement operations.

## PASSENGER SCREENING

The process of preboarding passenger screening for explosives, weapons, or other dangerous items is carried out using a combination of X-ray machines, walk-through metal detectors, hand wands, explosive trace detection machines, and/or physical search of individuals and property. A major mandate issuing from the 2001 Aviation and Transportation Security Act was the establishment of a federal screener workforce to replace the underpaid and poorly trained screeners from the private companies hired by the airlines. The federal screeners are subject to Federal Aviation Administration (FAA) regulation and must meet specific training requirements. Since the TSA assumed responsibility for passenger screening at the more than 400 U.S. commercial airports, billions of dollars have been spent and ten of thousands of transportation security officers (TSOs) have been hired to strengthen passenger screening operations. As a GAO study reported in April 2006, there have been improvements, but "challenges remain," particularly in funding and staffing.[24] Performance checks released in October 2007 show that TSA screeners need to significantly improve their threat object detection performance, as many threat test objects still get through the airport security checkpoints, leaving them an attractive threat vector.[25]

Government pay and benefits have increased for TSOs, as compared to their private sector predecessors. In 2000, according to another GAO study,[26] private screeners were generally paid around the minimum wage of $5.15 an hour and received few benefits. In contrast, their European counterparts

were paid as much as three times more, and benefits, such as health care, were significantly better. One consequence of such low pay and poor benefits for U.S. screeners was a high annual rate of turnover averaging 126 percent, with one September 11 airport, Boston's Logan International, at over 200 percent and Lambert St. Louis International at a staggering annual rate of 416 percent.[27] This high turnover rate was a factor contributing to the overall low screener effectiveness in detecting weapons and explosives and preventing them from being taken aboard aircraft. Today, the starting salary for full-time TSA screeners is approximately $24,000 per year, with a number of federal employee benefits available, such as health, retirement, and insurance, but attrition remains high, although it is much lower than the pre–September 11 rate. ATSA mandated that screeners be U.S. citizens and high-school graduates, although the latter requirement can be satisfied by a general equivalency degree (GED) or one year's experience in security work, aviation screener work, or X-ray technician work. Even before September 11, 2001, the law required all screeners to speak English. Now they really do.

## PRIVATE SCREENING OPERATIONS

ATSA directed the federal government to assume passenger screening operations at U.S. commercial airports, but it also included a provision establishing a pilot program for the screening of passengers and property by qualified private screening companies at five airports. Under this program, participating companies were required to provide compensation and benefits to screeners at no less than the level of that provided to TSA screening personnel. These government-contracted companies were required to adhere to TSA standard operating procedures and were subject to federal supervision of their screening operations, similar to FAA supervision of private firms prior to September 11. The airports chosen for the program were selected from each of the five airport risk categories and reflected variations in size and typical passenger, among other things. The five participating airports were San Francisco International, CA (SFO); Kansas City International, MO (MCI); Greater Rochester International, NY (ROC); Jackson Hole, WY (JAC); and Tupelo Regional, MS (TUP).

An independent evaluator was hired to compare the performance of the privately contracted screener to that of TSA screeners in comparable airport operations. Among other things, screeners were evaluated on their ability to detect prohibited items, such as guns and knives. In general, contract screening operations were performed at the same level or better than federal screening operations, and costs were not significantly different.[28] It should be noted that the comparison was between TSA screeners and TSA-contracted screeners, not pre–September 11 private screeners, who were not subject to the compensation and training requirements included in ATSA.

Following the conclusion of the two-year pilot program in November 2004, the TSA established the Screening Partnership Program (SPP) to meet

ATSA's requirements for an "opt-out" program. The SPP was opened up to all U.S. airports that require screening services, which includes all airports with scheduled commercial passenger flights. A federal security director (FSD) remains responsible at airports operating under the SPP for overseeing contractor performance and adherence to TSA security standards. Originally, for airports wishing to have screening functions performed by private firms under the SPP, security companies were selected from a TSA-approved "qualified vendor list." The TSA now allows any interested company to respond to a "Request for Proposal" (RFP), a government document for contracting screening services at an airport.

The TSA's involvement in the private screener process is intended to remain comprehensive, with rather minimal involvement by the individual airport. The TSA is to select, hire, and manage the private security companies. The TSA grants contracted companies, who are to be bound by TSA regulations, "degrees of freedom" on a discretionary basis in areas such as personnel recruitment, scheduling, and day-to-day management of personnel and resources. Contractors make more decisions at the local level than their TSA counterparts. Private contractors are not bound by federal employment guidelines and it is thought that they can more expeditiously terminate screeners for unsatisfactory performance.

Given the ongoing uncertainties over liability issues regarding security breaches, the very limited leeway in the overall management of private screening companies, and the limited, if any, cost benefits, airports have generally been reluctant to opt out. All five of the original airports in the pilot program continue to participate in the SPP, but few additional airports have joined.[29]

## THE REGISTERED TRAVELER PROGRAM

In recognition of more extensive screening measures following the September 11 attacks and the longer airport security lines that followed the federalization of the security function and the introduction of new equipment and new procedures, the 2001 Aviation and Transportation Security Act authorized the TSA to "[e]stablish requirements to implement trusted passenger programs to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."[30] The aviation industry and business traveler groups generally supported such an approach. The underlying concept was for participating travelers to voluntarily provide personal information and submit to a background check. Participants would then receive an identification card, encoded with biometric information, and go through a faster, streamlined, and presumably less intrusive screening process.

Under the Registered Traveler (RT) program, applicants voluntarily provide biographic and biometric data in order for the TSA to conduct a security threat assessment (STA) and determine eligibility. In 2005, Orlando

International Airport became the first "sponsoring entity" (participating airport or air carrier) to implement the program, which featured special expedited security checkpoints for participants. At Orlando, more than 30,000 travelers joined the program and paid an annual fee of around $100, and renewal rates have been reported to be high. More than a dozen other sponsoring entities, including the international airports in Jacksonville and San Francisco, have since begun operating the RT program.

Cost increases and TSA and public skepticism of the program in general may prove to be insurmountable obstacles to the success of the RT program. The program fee consists of a TSA portion and a private sector portion. At the time of printing, the federal fee, which is mainly for background checks, is $28, but the TSA announced in 2006 that it needed additional fees of more than $100 to cover screener salaries and additional background checks. In the face of criticism from companies and the public due to a possible doubling of enrollment fees, the TSA backed off from raising its portion of the fee unless "RT screening modifications impact TSA duties, responsibilities, or costs." Private sector costs are certain to rise as well. Orlando had four security machines, costing $200,000 each, which read participants' biometric cards for identity verification and scanned shoes for explosives. After repeated testing, however, the TSA withdrew its authorization for the use of the machines at Orlando and other airports on the grounds of failure to meet explosives detection standards. But the TSA's main concern regarding the program is that a terrorist might be able to pass the background check and then be considered a low security risk. Obviously, such concerns, if justified, make an RT program not only useless but very dangerous and unlikely to be a long-term solution.

If the RT program can insure against terrorists or others intent on harm, such as physically dangerous or criminal elements, being admitted to the ranks of the "trusted travelers," and if it can become economically feasible to allow the adoption of the program at a large number of U.S. airports, RT could be expanded to encompass aviation employee personnel for expedited processing at security checkpoints. The maritime transportation system has recently begun a program, similar to RT, for workers requiring unescorted access to secure areas. The Transportation Worker Identification Credential (TWIC) Program, which was authorized by the Maritime Transportation Security Act of 2002, is administered jointly by TSA and the U.S. Coast Guard. Initial enrollment in the program has recently begun at the Port of Wilmington, Delaware, and the program is expected to eventually include more than 750,000 maritime workers, such as longshoremen, truckers, and port employees.

## AVIATION SECURITY AND CIVIL RIGHTS

September 11, 2001 should have forever changed our attitudes about security and privacy. But with each passing day without an attack on aviation, passengers and those responsible for their safety and security grow complacent, and many special interests assert their concerns about assorted rights, usually

based on illusory constitutional rights to fly. The Constitution, written in 1787, contains no such rights, since the first manned flight, by balloon, had occurred only a few years previously, in France.[31] The Constitution does, however, provide freedom for interstate travel, based on Article IV, Section 2. Contrary to widespread misinformation and misinterpretation, there is no constitutional provision, federal law, regulation, court decision, or treaty that provides for full and free expression of religious practices and speech in airports or on private aircraft owned by private carriers. In a landmark decision in 1992 that was applauded by hurried passengers and overburdened airport managers, the U.S. courts tossed out of airports the Hare Krishnas and others, who, under the pretext of expression of their religion, peddled posies in congested airport passages.[32]

What any government or government-sponsored entity must not do is "establish" any religion, meaning favor or support one religion over another, or deprive citizens (and others who, by various laws, have been granted rights similar to those of citizens), of constitutional due process, equal protection, and reasonable expectations of privacy. Contrary to public perception, free speech in a public airport or a commercial jetliner is not among the enumerated rights. Thus, while aviation security professionals must avoid violating air passengers' constitutional rights of due process, equal treatment, and reasonable expectations of privacy, neither Muslims nor Methodists have the right to kneel in the aircraft or cry out prayers and pleas to the Almighty. In an aircraft or in an airport, your rights to public free speech, public expression of religion, association, protection against unreasonable search and seizure, smoking and chewing, and even to a large degree liberty itself are voluntarily surrendered when you purchase a ticket or consent to go through security. Such acts are voluntary choices made in conjunction with a choice to fly. Such voluntary behavior is deemed by the law as consent to such constitutional intrusions, so long as they are reasonably related to the goals of security and safety.

As terrorist watch lists grow, as terrorists adopt more Western-sounding names, and as more U.S. citizens are among the terrorists and placed on watch lists, mismatches and other errors will increase.[33] Vigilant air travelers who report suspicions of terrorist activity to the authorities should be protected from retaliatory lawsuits.[34]

In spite of a provision of the 2001 Aviation and Transportation Security Act granting immunity for reporting suspicious activities relating to aircraft or passenger safety,[35] several lawsuits have been filed since September 11, 2001, in response to perceived racial, ethnic, or religious profiling. In one highly publicized incident that occurred in 2006, six imams were removed from a US Airways flight after they had gone through security screening, because other passengers had reported what they considered to be suspicious behavior, such as praying aloud in Arabic and allegedly making anti-American remarks. The six, who were questioned by airport security personnel and subsequently released, later filed suit against the airline, the Minneapolis–St. Paul Metropolitan

Airport, and several passengers, who had reported the behavior to the flight crew.[36] Following another incident in 2006, an U.S. citizen of Iranian descent was awarded $27.5 million in a lawsuit against Southwest Airlines alleging false imprisonment because flight attendants had had her arrested following a confrontation involving in-flight service. The flight attendants claimed that the passenger had interfered with the flight crew.[37]

With respect to the civil rights implications of evolving security screening technologies, some advances may actually make security searches less, rather than more, intrusive. Air passengers pulled from security lines for secondary screening to be inspected for potentially dangerous objects hidden on the body are usually given a pat-down or escorted to an inspection room for a strip search. New body-scan machines based on "millimeter wave" technology that create and transmit full-body images to screeners for viewing are being tested. The scanners create the images using electromagnetic waves from reflected body energy. Some privacy advocates remain skeptical.[38] They are concerned that the three-dimensional images are too graphic in that they show outlines of bodies and body parts, and that dishonest screening personnel might save screening images and leak them to the Internet or the media. When used properly, the black-and-white images show a blurred face, are instantly deleted, and are viewed at a location removed from the scanning area so that the actual person is not seen by the screeners viewing the images. In the test phase, body scans are performed only on passengers who request them as an alternative to a pat-down, but the machines could eventually replace metal detectors at airports.[39]

## CARGO SECURITY

The air cargo system is a vast and complex network that includes both all-cargo planes and passenger air carriers, manufacturers, shipping companies, freight forwarders, thousands of cargo facilities nationwide and internationally, and literally anyone who sends an air freight package. Domestic shipments, as represented by revenue ton miles (RTMs), are estimated to increase by 3.5 percent per year from FY 2003 to FY 2015, and international shipments by 5.3 percent per year during the same period.[40] Approximately 7,500 tons of cargo are carried on passenger aircraft daily.[41] About a quarter of the estimated 23 billion pounds of air cargo transported in the United states in 2004 was carried on passenger aircraft.[42]

Terrorist attacks even before September 11, 2001, included those involving explosives in aircraft cargo holds and left behind in luggage bins and under seats. The 9/11 Commission made a number of related recommendations, including the installation of in-line baggage screening equipment and the deployment of at least one hardened cargo bin on any aircraft carrying passengers. This recommendation was based on facts. In November 1979, the American "Unabomber," Theodore Kaczynski, concealed a bomb in a U.S. mail parcel carried on board American Airlines Flight 444 flying from

Chicago to Washington, DC, but it failed to detonate. A piece of checked baggage on Air India Flight 182 exploded over the Atlantic Ocean in June 1985, killing all 329 passengers and crew. And in December 1988, Pan Am Flight 103 was brought down over Lockerbie, Scotland, by plastic explosives concealed in an unaccompanied suitcase in the cargo hold, resulting in the death of all 259 passengers and crew.[43] The DHS's 2007 *National Strategy for Transportation Security* warned that "terrorists may infiltrate the cargo handling system to transport people, conventional or WMD, or weapons components."[44]

The Aviation and Transportation Safety Act of 2001 mandated the "screening of all passengers and property, including United States mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft" and called for a system for screening or inspecting cargo transported in all-cargo aircraft. ATSA did not, however, mandate that air cargo be physically screened. Advances in air cargo screening have not kept pace with screening for passengers, leaving all-cargo aircraft as an attractive target for hijacking, sabotage, or terrorism.

Air cargo security is maintained through technology, TSA oversight, and inspections of air carrier operations and risk assessment programs. Given the sheer volume of air cargo transported, however, the goal of 100 percent screening remains elusive and has met with skepticism from the TSA as costly and adding little benefit for security, diverting airport screeners from other activities. Even on passenger planes, only a small percentage of the cargo flying directly underneath the passengers is subjected to an actual physical inspection.

## IN-LINE BAGGAGE SYSTEMS

Well before September 11, 2001, thousands of stand-alone explosive detection system (EDS) machines were deployed in airport lobbies, along with tabletop explosives trace detection (ETD) units. However, an in-line baggage system integrates EDS machines with the airport baggage handling system. Typically, after luggage is checked in and loaded onto a conveyor belt, it moves into a secure area and through an EDS machine, where it is screened for explosives, before being loaded into departing aircraft. Currently, there are approximately 25 operational in-line systems and another 26 under construction. Of course, the TSA may also open and physically hand inspect checked luggage.

## TSA OVERSIGHT

TSA also oversees the screening operations of cargo aircraft operators, who use a variety of methods—including physical inspection, X-ray, EDS machines, and canine teams—to screen cargo prior to loading it on board aircraft. Oversight is exercised through the use of cargo transportation security

inspectors (TSIs), who conduct security regulation compliance reviews of air carriers. However, a July 2007 DHS inspector general's review of passenger cargo security found that the TSA "does not provide sufficient resources for air carrier inspection coverage."[45] The TSA plans to increase the number of air cargo TSIs from 300 to 450 by the end of FY 2008. In addition, the inspector general found that the TSA lacked a "comprehensive, consistent, and reliable program to provide proper coverage and oversight of air carrier cargo screening."

## THE KNOWN SHIPPER PROGRAM

The TSA also attempts to determine the legitimacy of shippers and assess risk through a system called the Known Shipper Program. Under this program, air carriers, who must comply with specific security requirements, provide information on their cargo shippers to the TSA. The TSA then determines the shippers' legitimacy as business entities and qualifies them as known shippers. Designation as a known shipper eliminates the need for air carriers to repeatedly validate shipper information once the existence and legitimacy of a shipper has been established.

## IMPLEMENTING THE RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007

The disparity between the inspection requirements for passenger checked baggage and air cargo, which both end up in the cargo hulls of passenger aircraft, led to the enactment of H.R. 1, the Implementing Recommendations of the 9/11 Commission Act of 2007, which was signed into law on August 3, 2007. This law requires that air cargo loaded onto passenger airplanes be subjected to security screening equivalent to that for checked baggage. A system for 100 percent inspection of cargo is to be phased in over a three-year period. Astonishingly, the bill was opposed by the airline industry as too costly—the same objection the airline industry made before September 11, 2001.[46]

The bill was also not originally supported by TSA officials, who argued that different screening requirements for air cargo are justified on the grounds that background checks of air cargo employees and systems such as the Known Shipper Program are sufficient to ensure security. In addition, the TSA argued that resources would be diverted unnecessarily and safety ultimately reduced.[47]

This new law, which requires the development of a full inspection program for air cargo, is being interpreted by the TSA in a way that does not require X-ray screening or physical inspection, as with checked baggage. Under the Known Shipper Program, companies whose identity has been verified are merely registered with the TSA. Now, the TSA is considering a "certified shipper" program, under which a shipper must be certified as safe. According

to a TSA spokesperson, cargo would be considered "inherently screened" if it is packed and sealed by a certified shipper at a government-certified facility. The law's main supporter, Congressman Edward J. Markey of Massachusetts, was "outraged that the Bush Administration and the airline industry would even think that they could get away with anything less than a full physical screening of all cargo that goes onto passenger planes."[48] Such incremental approaches to the urgent issue of improving cargo security illustrate not only the formidable task of bringing about fundamental reform in the face of industry opposition but the piecemeal approach that to date has left many threat vectors open to terrorists.

## CONCLUSION

In spite of bureaucratic inertia and a lack of fundamental change in aviation security structures overall since September 11, as well as the general erosion of the legal responsibility of those responsible for lax security or negligent in their duties, some modest progress has been made in efforts to protect the flying public and those on the ground over whom they fly. One needed and overdue reform was the establishment of a federalized screener program under the TSA, with better pay and benefits than the airlines had offered and employees who must be U.S. citizens or U.S. nationals and speak English. Although still underfunded and understaffed, and with TSA screeners turning in weak performances, the program is nonetheless a positive step toward ensuring passenger safety. In addition, the fact that a terrorist contemplating a future hijacking might encounter an armed and well-trained federal air marshal seated inconspicuously among aircraft passengers would add an element of uncertainty to the terrorist operation.[49] Flight decks with reinforced doors and armed volunteer flight deck officers also enhance the security of passenger aircraft operations. Nevertheless, security technologies and procedures must continue to improve and expand. Our air cargo system remains unacceptably vulnerable as the airline industry and its supporters in government resist efforts to implement programs for the full inspection of air cargo due to cost considerations. Formidable challenges in improving aviation security remain but will never be overcome without the full accountability of those responsible for our nation's aviation safety and security. Bold new laws and legislative requirements can be a force for safer skies, but provisions embedded in such laws to allow security failures to go unpunished and negligent performers to escape responsibility will render impotent the best of intentions.

Prohibiting judicial redress of the failure, whether negligent or intentional, of our nation's security laws means that the most powerful tool proven to enhance security performance is missing—accountability. Accountability for performance has time and time again been found by the Office of Inspector General and the Government Accountability Office to be the key to successful security systems and performance. The legal system has been and should continue to be a strong ally of accountability.

## NOTES

1. In 2001, airlines were subject to security directives and guidelines issued by the FAA under CFR Title 14, Section 108.5, revised January 1, 2001. Section 108.5 required that "[e]ach certificate holder shall adopt and carry out a security program that meets the requirements of Sec. 108.7," where a certificate holder was defined as "a person holding an FAA operating certificate when that person engages in scheduled passenger or public charter passenger operations or both."

2. See CFR Title 14, Section 108.7, revised January 1, 2001.

3. Under CFR Title 14, Section 107.3, revised January 1, 2001, "[n]o airport operator may operate an airport subject to this part unless it adopts and carries out a security program."

4. *Federal Register* 66, no. 137 (July 17, 2001): 37353.

5. U.S. Government Accountability Office, *Aviation Security: Vulnerabilities Still Exist in the Aviation Security System* (GAO-00–142, 2000), 3.

6. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W.W. Norton & Company, Inc., 2004), 339.

7. *Air Transportation Safety and System Stabilization Act of 2001*, Public Law 107–42, *U.S. Statutes at Large* 115 (2001): 230.

8. Leslie Wayne and Michael Moss, "A Nation Challenged: The Airlines; Bailout for Airlines Showed the Weight of a Mighty Lobby," *New York Times*, October 10, 2001, http://query.nytimes.com/gst/fullpage.html?res=9F07EEDC1F3CF933A25753C1A9679C8B63.

9. Securicor PLC, Preliminary Results Announcement for the Year Ended September 30, 2003.

10. See CFR Title 28, Part 104, September 11th Victim Compensation Fund of 2001, March 13, 2002.

11. *Aviation and Transportation Security Act*, Public Law 107–71, *U.S. Statutes at Large* 115 (2001): 597.

12. "Air Marshals Taught to Be Risk Averse," *CNN.com*, December 7, 2005, http://www.cnn.com/2005/US/12/07/air.marshal/index.html.

13. Congressional Research Service, *CRS Report for Congress: Air Cargo Security* (RL32022, updated July 30, 2007), i.

14. *Homeland Security Act of 2002*, Public Law 107–296, *U.S. Statutes at Large* 116 (2002): 2135.

15. Other than the defunct Argenbright Security.

16. The federal flight deck officer program, created by Section 1402 of the Homeland Security Act of 2002, was designed to "deputize volunteer pilots of air carriers providing passenger air transportation or intrastate passenger air transportation as Federal law enforcement officers to defend the flight decks of aircraft of such air carriers against acts of criminal violence or air piracy."

17. Section 865 defines the term "qualified anti-terrorism technology" to mean "any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary."

18. *Boyle v. United Technologies Corp.*, 487 U.S. 500 (1988).

19. *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108–458, *U.S. Statutes at Large* 118 (2004): 3638.

20. *9/11 Commission Report*, 393.

21. U.S. Government Accountability Office, *Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain* (GAO-07–346, May 2007), 5.

22. In one high-profile incident in September 2004, a United Airlines flight en route from London to Washington, DC, carrying Yusuf Islam, the pop singer formerly known as Cat Stevens, was diverted to Bangor, Maine. After departure, U.S. Customs agents discovered that Yusuf Islam was on government watch lists due to suspected terrorist connections. See Sara Kehaulani Goo, "Cat Stevens Leaves U.S. after Entry Denied," *Washington Post*, September 23, 2004, http://www.washingtonpost.com/wp-dyn/articles/A43282–2004Sep22.html.

23. The IAP is a pilot program begun in 2004 to identify and target high-risk passengers for behavioral assessment and enhanced security screening.

24. U.S. Government Accountability Office, *Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain* (GAO-06–371T, 2006).

25. Jeanne Meserve, "Airport Screeners Failed to Find Most Fake Bombs, TSA Says," *CNN.com*, October 18, 2007, http://www.cnn.com/2007/TRAVEL/10/18/airport.screeners/.

26. U.S. Government Accountability Office, *Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance* (GAO/RCED-00–75, 2000), 37.

27. Ibid., 24.

28. Transportation Security Administration press release, "TSA Releases Performance Report on Contract Screeners at Five U.S. Airports," April 22, 2004.

29. A TSA press release dated June 22, 2007, announced the selection of Trinity Technology Group, Inc., as the private screening company for the Charles M. Schulz-Sonoma County (CA) Airport. In addition to the original five airports, the only other SPP participants are Joe Foss Field in Sioux Falls (SD), Key West International Airport, Florida Keys Marathon Airport, and the East 34th Street Heliport in New York City.

30. *Aviation and Transportation Security Act*, Public Law 107–71, *U.S. Statutes at Large* 115 (2001): 597.

31. The Montgolfier brothers undertook the first manned balloon flight in 1783, and in 1784 manned flight was already being regulated by French police because of dangers to persons on the ground.

32. *Lee v. International Soc. for Krishna Consciousness, Inc.*, 505 U.S. 830 (1992).

33. A CBS *Sixty Minutes* segment in 2006 reported that among the names that had turned up on the U.S. government's No-Fly List were those of 14 of the 19 September 11 hijackers, the president of Ecuador, and an assortment of other dead and otherwise unlikely persons.

34. H.R. 1401, the Rail and Public Transportation Security Act of 2007, which passed the House on March 27, 2007, and is awaiting action in the U.S. Senate, contained language granting citizens who report suspicious activity relating to terrorism immunity from lawsuits.

35. *Aviation and Transportation Security Act*, Public Law 107–71, *U.S. Statutes at Large* 115 (2001): 597, §44941.

36. Libby Sander, "6 Imams Removed from Flight for Behavior Deemed Suspicious," *New York Times*, November 22, 2006, http://www.nytimes.com/2006/11/22/us/22muslim.html.

37. Alan Levin, "Woman Wins $27.5 Million in Suit against Southwest Airlines," *USATODAY.com*, April 12, 2006, http://www.usatoday.com/travel/flights/2006–04–11-swa-lawsuit_x.htm.

38. Austin Considine, "Will New Airport X-Rays Invade Privacy?" *New York Times*, October 9, 2005, http://travel.nytimes.com/2005/10/09/travel/09xray.html.

39. Carol Cratty, "TSA Trying New Airline Passenger Screening Machines," *CNN.com*, October 12, 2007, http://www.cnn.com/2007/TRAVEL/10/11/airport.screening/.

40. Federal Aviation Administration, *FAA Aerospace Forecasts Fiscal Years 2005–2016* (FAA-APO-04–1, 2004), I-28.

41. Office of the Inspector General, Department of Homeland Security, *Transportation Security Administration's Oversight of Passenger Aircraft Cargo Faces Significant Challenges* (OIG-07–57, 2007), 3.

42. U.S. Government Accountability Office, *Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security* (GAO-06–76, 2005), 1.

43. Roy Rowan, "Pan Am 103: Why Did They Die?" *Time*, April 27, 1992, http://www.time.com/time/magazine/article/0,9171,975399,00.html.

44. Department of Homeland Security, *National Strategy for Aviation Security*, March 26, 2006.

45. Office of the Inspector General, Department of Homeland Security, *Transportation Security Administration's Oversight of Passenger Aircraft Cargo Faces Significant Challenges* (OIG-07–57, 2007), 6.

46. *Federal Register* 66, no. 137 (July 17, 2001): 37341.

47. Eric Lipton, "U.S. Security Debate Centers on Inspections of Air Cargo," *International Herald Tribune*, February 8, 2007, http://www.iht.com/articles/2007/02/08/america/web.0208security.php.

48. Charlie Savage, "No Checks for Bombs in Certified Air Cargo," *Boston Globe*, August 24, 2007, http://www.boston.com/news/nation/articles/2007/08/24/no_checks_ for_bombs_in_certified_air_cargo/.

49. At Miami International Airport in 2005, an American Airlines passenger was fatally shot by federal air marshals when he suddenly bolted from an airplane while claiming to have a bomb. See Thomas Frank, Mimi Hall and Alan Levin, "Air Marshals Thrust into Spotlight," *USATODAY.com*, December 8, 2005, http://www.usatoday.com/news/nation/2005–12–07-air-marshals_x.htm.

# CHAPTER 10

# A Chronology of Attacks against Civil Aviation

*Mary F. Schiavo*

One of the frequent criticisms of our approach to aviation security is that we devote too much or even all of our attention to responding to the last attack rather than protecting ourselves against the next attack. We are reactive rather than proactive, and our institutional memory if any, is usually short term.

The September 11, 2001, attacks were both foreseeable and foreseen. There have been more hijackings in history than bombings or shoot-downs, and there were prior instances of multiple hijackings on the same or successive days. Nonetheless, on September 11, 2001, if the airlines were looking for anything, they were looking for a terrorist with a bomb in the checked luggage. The last major terrorist attack that people remembered was Pan Am Flight 103 in 1988, brought down over Lockerbie, Scotland, by a bomb in a checked bag.

Thus, this chapter is an effort to alleviate the problems of the lack of institutional memory and the lack of any publicly available printed historical chronology of the attacks against civil aviation. In a world in which holy wars span millennia, forgetting the history of the past century can prove deadly.

## 1930s

**May 1930**
**Hijacking:** Peruvian revolutionaries seized a Pan American mail plane.
Source: http://www.centennialofflight.gov/essay/Government_Role/security/POL18.htm.

**February 21, 1931**
**Hijacking:** Revolutionary soldiers hijacked a Ford Tri-Motor aircraft at Arequipa Airport, Peru.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

**October 17, 1933**
**Bombing:** A United Airlines flight exploded over Chesterton, Indiana, killing everyone on board, including the first flight attendant to die while in service.

## 1947

**July 19, 1947**
**Hijacking:** Three Romanians killed an air crew member.
Source: http://www.centennialofflight.gov/essay/Government_Role/security/POL18.htm.

## 1948

**April 6, 1948**
**Hijacking:** A group of 17 hijackers at Praha/Ruzyne International Airport, Czech Republic, demanded to be taken to the U.S. Zone in Germany.

**June 17, 1948**
**Hijacking:** A Transporturile Aeriene Romano-Sovietice (TARS) flight was hijacked. The target was Austria.

**June 30, 1948**
**Hijacking:** Anticommunists seized a TABSO Ju-52 aircraft after takeoff from Varna Airport, Bulgaria, in order to have it flown to Istanbul, Turkey.

**July 17, 1948**
**Hijacking:** A Cathay Pacific Airlines Catalina seaplane was hijacked en route from Macao to Hong Kong.

**September 12, 1948**
**Hijacking:** An Olympic Airways DC-3 aircraft was hijacked on a domestic flight between Athens and Thessaloniki International Airport, Greece.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1949

**January 4, 1949**
**Hijacking:** A Maszovlet DC-3 aircraft was hijacked on a domestic flight in Hungary.

**January 30, 1949**
**Hijacking:** Six hijackers seized a China National aircraft in Shanghai.

**April 29, 1949**
**Hijacking:** A hijacker, on a Romanian domestic flight, seized a TARS DC-3 in order to go to Greece.

**May 7, 1949**
**Bombing:** Two ex-convicts placed a time bomb on a Philippine Airlines flight en route between Daet and Manila. The bomb exploded.

**September 9, 1949**
**Bombing:** In order to marry another woman and profit from his wife's $10,000.00 life insurance policy, a man had a time bomb placed in his wife's suitcase. The bomb exploded on a Canadian Pacific Airlines aircraft en route between Montreal and Comeau Bay.

**September 16, 1949**
**Hijacking:** A Polskie Linie Lotnicze (LOT) aircraft in Gdansk, Poland, was hijacked. The target was Sweden.

**December 9, 1949**
**Hijacking:** Four hijackers seized a TARS DC-3 aircraft at Sibiu Airport, Romania.

**December 16, 1949**
**Hijacking:** A LOT aircraft was seized by 16 hijackers who demanded to be taken to Denmark.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1950

**March 24, 1950**
**Hijacking:** Two people hijacked a CSA DC-3 in Brno, Czech Republic.

**March 24, 1950**
**Hijacking:** A Ceskoslovenske Aerolinie (CSA) DC-3 was hijacked on a domestic flight in the Czech Republic. The two hijackers demanded to be taken to the U.S. Zone in Germany.

**March 24, 1950**
**Hijacking:** A CSA DC-3 was hijacked en route from Slovakia to the Czech Republic. The four hijackers demanded to be taken to the U.S. Zone in Germany.

**April 13, 1950**
**Bombing:** An explosion caused a hole in the fuselage in the rear of a British European Airways (BEA) aircraft on a flight between Northolt Airport, England, and Paris, France.

**August 11, 1950**
**Hijacking:** Two hijackers seized a CSA aircraft in order to be taken to Germany.
Source**:** Aviation Safety Network Database: http://aviation-safety.net/database.

## 1951

**October 17, 1951**
**Hijacking:** A Jugoslovenski Aerotransport (JAT) DC-3 aircraft was seized by two hijackers who demanded to be taken to Zurich, Switzerland.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1952

**March 23, 1952**
**Hijacking:** Four hijackers demanding to go to Germany seized a CSA Douglas C-47 aircraft on a Czech Republic domestic flight.

**April 18, 1952**
**Hijacking:** A JAT aircraft en route from Croatia to Slovenia was hijacked. The target was Austria.

**June 26, 1952**
**Hijacking:** A JAT aircraft was hijacked as it was departing from Serbia.

**August 12, 1952**
**Bombing:** An in-flight explosion caused a Transportes Aéreos Nacionales aircraft to crash while en route between Rio Verde and Goiânia Santa Genoveva airports in Brazil.

**September 24, 1952**
**Bombing:** A suitcase bomb with shrapnel exploded after a Mexicana aircraft departed from Mexico City. The intention was to cash in on the life insurance policies of eight people on board.

**December 30, 1952**
**Hijacking:** A lone gunman hijacked a Philippine Airlines Douglas DC-3 on a flight from Laoag, Philippines. He forced himself into the cockpit and shot the captain and a steward; then the crew set the plane in a steep dive to knock the hijacker off balance.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1953

**February 3, 1953**
**Bombing:** An Air-Outre Mer aircraft exploded near Lai Chau, Vietnam.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1954

**July 6, 1954**
**Hijacking:** A 15-year-old armed with an empty pistol charged the cockpit of an American Airlines Douglas DC-9 on a flight from Cleveland, Ohio, to St. Louis, Missouri.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1955

**April 11, 1955**
**Bombing:** A device placed in the wheel well of an Air India aircraft exploded en route between Hong Kong and Jakarta.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

**November 1, 1955**
**Bombing:** A bomb destroyed a United Airlines plane after it took off from Denver, Colorado. A son placed a bomb in his mother's luggage in order to cash in on her insurance policy.
Source: http://www.centennialofflight.gov/essay/Government_Role/security/POL18.htm; "FAA History Chronology, 1926–1996." Washington, DC: Government Printing Office, 1997.

## 1956

**July 3, 1956**
**Hijacking:** Seven hijackers attempted to seize a Malev Hungarian Airlines HA-LIG aircraft on a domestic flight departing from Budapest, Hungary.

**October 13, 1956**
**Hijacking:** Four armed gunman seized a Malev aircraft on a domestic route in Hungary.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1957

**July 25, 1957**
**Bombing:** Dynamite exploded in the lavatory of a Western Airlines aircraft flying at 7,500 feet over California, blowing the person who had detonated the charge through the side of the aircraft.
Source: "FAA History Chronology, 1926–1996."

**December 19, 1957**
**Bombing:** A bomb exploded in the lavatory of a SAGETA aircraft en route between Argentina and Paris.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1958

**February 16, 1958**
**Hijacking:** A Korean National Airlines Douglas DC-3 en route between Busan-Gimhae and Seoul-Gimpo international airports, South Korea, was hijacked. The hijackers demanded to be taken to North Korea.

**April 9, 1958**
**Hijacking:** A Cubana de Aviacion aircraft was hijacked en route from Havana, Cuba, to Santa Clara Airport, Cuba.

**April 13, 1958**
**Hijacking:** Three peopled hijacked a Cubana Douglas DC-3 aircraft on a domestic flight in Cuba and demanded to be taken to the United States.

**October 22, 1958**
**Hijacking:** A Cubana Douglas DC-3 aircraft hijacked en route from Cayo Mambi to Moa Bay, Cuba, disappeared with the three hijackers on board.

**November 6, 1958**
**Hijacking:** A Cubana Douglas DC-3 aircraft was hijacked after departing from Manzanillo, Cuba.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1959

**April 10, 1959**
**Hijacking:** Six rebels killed the pilot on board a COHATA Douglas DC-3 flying from Les Cayes Airport to Port-au-Prince, Haiti, in order to divert the plane to Cuba.

**April 16, 1959**
**Hijacking:** An Aerovias Cuba International Douglas DC-3 was hijacked to be flown to the United States.

**April 25, 1959**
**Hijacking:** A Cubana de Aviacion aircraft was hijacked en route from Varadero to Havana, Cuba.

**July 8, 1959**
**Hijacking:** A JAT aircraft was hijacked en route from Tivat Airport to Beograd Airport, Serbia.

**September 8, 1959**
**Bombing:** A bomb was detonated in the passenger cabin of a Mexicana aircraft after it departed from Mexico City. The passenger who is believed to have carried the bomb fell from the aircraft.

**October 2, 1959**
**Hijacking:** A Cubana Aviacion aircraft was hijacked en route from Havana, Cuba, to Santiago Airport, Chile.

**December 2, 1959**
**Hijacking:** Brazilian Air Force officers seized a Panair do Brasil L-049 aircraft after it departed from Rio de Janeiro, Brazil.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1960

**January 6, 1960**
**Bombing:** A National Airlines aircraft crashed near Bolivia, North Carolina. The accident investigation revealed that the plane had disintegrated in flight as a result of a dynamite explosion.
Source: "FAA History Chronology, 1926–1996."

**April 12, 1960**
**Hijacking:** A pilot and two crewmen were among the four hijackers of a Cubana de Aviacion aircraft.

**July 5, 1960**
**Hijacking:** A Cubana de Aviacion aircraft was hijacked en route from Madrid, Spain, to Havana.

**July 17, 1960**
**Hijacking:** A pilot hijacked a Cubana de Aviacion aircraft en route from Havana to Miami, Florida.

**July 19, 1960**
**Hijacking:** A lone hijacker demanded to be taken to Singapore on a Trans Australia Airlines L-188 flight en route from Sydney to Brisbane.

**July 28, 1960**
**Hijacking:** A Cubana de Aviacion DC-3 flight en route to Camaguey, Cuba, was diverted to Miami by the captain in order for him to gain political asylum.

**October 29, 1960**
**Hijacking:** The copilot of a Cubana de Aviacion DC-3, after takeoff from Havana, demanded to be taken to the United States along with eight other people on board.
Source for the 1960 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1961

**January 1, 1961**
**Hijacking:** Two hijackers seized a Cubana de Aviacion aircraft departing from Havana in order to go to New York.

**May-August 1961**
**Hijacking:** Five incidents originated in the United States.
Source: "FAA History Chronology, 1926–1996."

**May 1, 1961**
**Hijacking:** A flight between Marathon Flight Strip and Key West, Florida, was hijacked. The target was Cuba.

**May 10, 1961**
**Bombing:** An Air France aircraft en route from Chad to France broke up in flight over the Sahara Desert after what was thought to be an explosive device caused the empennage to fail.

**July 3, 1961**
**Hijacking:** A Cubana de Aviacion aircraft was hijacked en route from Havana to Varadero, Cuba.

**July 24, 1961**
**Hijacking:** An Eastern Airlines flight was hijacked en route from Miami to Tampa, Florida, to go to Cuba.

**July 31, 1961**
**Hijacking:** A Pacific Airlines flight was hijacked en route to San Francisco, California. The target was Cuba.

**August 3, 1961**
**Hijacking:** A Continental Airlines B-707 was hijacked en route to Houston, Texas, from Los Angeles, California. The hijackers demanded to be taken to Cuba.

**August 9, 1961**
**Hijacking:** A Pan American World Airways flight was hijacked en route from Mexico City to Guatemala City. The hijacker demanded to be taken to Cuba.

**August 9, 1961**
**Hijacking:** Five hijackers attempted to seize an Aerovias Cuba International flight after takeoff from Havana.

**November 10, 1961**
**Hijacking:** Six hijackers seized a TAP Air Portugal aircraft in order to drop leaflets over Lisbon, Portugal.

**November 27, 1961**
**Hijacking:** Five students seized an AVENSA aircraft in order to drop leaflets over Caracas, Venezuela.
Source for the 1961 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1962

**March 17, 1962**
**Hijacking:** An aircraft was hijacked en route between Paris and St. Martin de l'Ardoise.

**April 16, 1962**
**Hijacking:** A hijacker seized a KLM Royal Dutch Airlines aircraft en route between the Amsterdam, the Netherlands, and Lisbon airports in order to be taken to East Berlin.

**May 22, 1962**
**Bombing:** A Continental Air Lines 707 flying over southern Iowa exploded with the probable cause cited as a dynamite detonation in the rear lavatory.
Source: "FAA History Chronology, 1926–1996."
Source for the 1962 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1963

**November 28, 1963**
**Hijacking:** Six hijackers took over an AVENSA aircraft en route between Ciudad Bolívar and Caracas airports, Venezuela.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1964

**May 7, 1964**
**Hijacking:** The captain and first officer of a Pacific Air Lines Fokker F-27 were shot en route from Reno, Nevada, to San Francisco.
Source: "FAA History Chronology, 1926–1996."

**December 8, 1964**
**Bombing:** A dynamite charge exploded on board an Aerolineas Abaroa aircraft on a domestic flight headed to La Paz, Bolivia.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1965

**July 8, 1965**
**Bombing:** A bomb detonated in the left aft lavatory of a Canadian Pacific Air Lines aircraft on a domestic flight from Vancouver to White Horse.

**August 31, 1965**
**Hijacking: A** Hawaiian Airlines flight was hijacked as it was departing from Honolulu International Airport, Hawaii, en route to Kauai Island Airport.

**October 11, 1965**
**Hijacking:** Two hijackers seized an Aloha Airlines aircraft departing from Hoolehua-Molokai Airport en route to Honolulu International Airport.

**October 26, 1965**
**Hijacking:** A hijacker attempted to size a National Airlines aircraft en route from Miami to Key West.

**November 17, 1965**
**Hijacking:** A National Airlines MD DC-8 was hijacked en route from Houston, Texas, to Melbourne, Florida.

**December 31, 1965**
**Hijacking:** An Aeroflot aircraft was taken over by two hijackers.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1966

**March 27, 1966**
**Hijacking:** The flight engineer seized a Cubana de Aviacion aircraft en route between Santiago, Cuba, and Havana.

**July 7, 1966**
**Hijacking:** Nine hijackers, including the pilot, seized a Cubana de Aviacion aircraft en route to Havana from Santiago.

**August 1966**
**Hijacking:** Three hijackers stormed an Aeroflot aircraft in Batumi, Georgia.

**September 28, 1966**
**Hijacking:** In order to stage a symbolic invasion, 19 Argentineans seized an Aerolineas Argentinas aircraft en route from Buenos Aires, Argentina.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1967

**February 7, 1967**
**Hijacking:** A single hijacker seized a United Arab Airlines aircraft en route to Hurghada, Egypt, from Cairo, Egypt.

**April 23, 1967**
**Hijacking:** Five hijackers took over a Nigeria Airways aircraft en route from Benin City to Lagos, Nigeria.

**May 29, 1967**
**Bombing:** A time bomb detonated on board an Aerocondor de Colombia aircraft en route from Barranquilla to Bogotá, Colombia.

**June 5, 1967**
**Shooting:** An Alia Royal Jordanian Airlines DC-7 was destroyed on the ground at Damascus International Airport, Syria, during an Israeli air raid during the Six-Day War.

**June 30, 1967**
**Bombing:** A bomb exploded while an Aden Airways aircraft was being quarantined on the ground at the Aden International Airport in Yemen.

**August 6, 1967**
**Hijacking:** Five hijackers attempted to seize an Aerovias Condor aircraft after the flight departed from Barranquilla, Colombia.

**September 9, 1967**
**Hijacking:** Three hijackers seized an Avianca aircraft after the flight departed from Barranquilla, Colombia.

**October 12, 1967**
**Bombing:** A device detonated under a seat in the cabin area of a BEA aircraft en route to Nicosia Airport in Cyprus. The explosion caused a structural breakup in the aircraft and it crashed into the ocean.

**November 12, 1967**
**Bombing:** A bomb exploded in the rear baggage compartment on board an American Airlines B-727 en route from Chicago, Illinois, to San Diego, California.

**December 11, 1967**
**Bombing:** A homemade bomb detonated in the rear baggage compartment on board an American Airlines B-727 en route from Chicago to San Diego.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

## 1968

**Hijackings:** There were 35 hijackings in total. During 1968, 12 airliners and 6 general aviation aircraft belonging to U.S. carriers were hijacked. Out of the 35, 18 involved U.S. aircraft.
Source: "FAA History Chronology, 1926–1996."

**February 9, 1968**
**Hijacking:** A lone hijacker seized a Pan Am aircraft en route from Vietnam to Hong Kong.

**February 21, 1968**
**Hijacking:** A Delta Air Lines flight from Tampa en route to West Palm Beach, Florida, was hijacked.

**March 5, 1968**
**Hijacking:** Three hijackers seized an Avianca aircraft en route to Barranquilla, Colombia.

**March 12, 1968**
**Hijacking:** Three hijackers seized a National Airlines aircraft en route from Tampa to Miami.

**March 21, 1968**
**Hijacking:** Three hijackers attempted to seize an AVENSA aircraft after its departure from Caracas Airport.

**June 19, 1968**
**Hijacking:** A VIASA aircraft was hijacked after departing from Santo Domingo. The hijacker demanded to be taken to Cuba.

**June 29, 1968**
**Hijacking:** A Southeast Airlines aircraft was hijacked en route to Key West from Tampa. The hijacker demanded to be taken to Cuba.

**July 1, 1968**
**Hijacking:** A Northwest Airlines B-727 was hijacked en route to Miami from Chicago. The hijacker demanded to be taken to Cuba.

**July 4, 1968**
**Hijacking:** A TWA Airlines B-727 was hijacked en route from Kansas City to Las Vegas, Nevada.

**July 12, 1968**
**Hijacking:** A Delta Air Lines aircraft was hijacked en route to Houston from Baltimore, Maryland. The hijacker demanded to be taken to Cuba.

**July 17, 1968**
**Hijacking:** A National Airlines aircraft was hijacked en route to Miami, Florida, from Los Angeles, California. The hijacker demanded to be taken to Cuba.

**July 19, 1968**
**Bombing:** The ticket offices of both Air France and Japan Air Lines in Los Angeles, were damaged by explosions.
Source: Brian Jenkins and Janera Johnson, *International Terrorism: A Chronology, 1968–1974* (Santa Monica, CA: RAND Corporation, 1975).

**July 23, 1968**
**Hijacking:** An El Al B-707 flying from Rome, Italy, to Tel Aviv, Israel, was hijacked by three people and flown to Algeria.

**August 17, 1968**
**Bomb:** A Mexican Airlines office in Miami was damaged by a bomb.
Source: Jenkins and Johnson, *International Terrorism: A Chronology, 1968–1974.*

**August 22, 1968**
**Bombing:** Fire bombs destroyed two East Coast Leasing aircraft on the ground at Martinsburg Airport in West Virginia.

**September 11, 1968**
**Hijacking:** An Air Canada aircraft was hijacked en route from St. John Airport to Toronto, Canada. The hijacker demanded to be flown to Cuba.

**September 20, 1968**
**Hijacking:** An Eastern Airlines B-720 was hijacked en route from San Juan, Puerto Rico, to Miami. The hijacker demanded to be taken to Cuba.

**September 22, 1968**
**Hijacking:** An Avianca B-727 was hijacked after its departure from Barranquilla Airport, Colombia. The hijacker demanded to be taken to Cuba.

**September 22, 1968**
**Hijacking:** An Avianca Douglas DC-4 aircraft was hijacked after its departure from Barranquilla Airport, Colombia. The hijacker demanded to be taken to Cuba.

**October 6, 1968**
**Hijacking:** An AeroMaya aircraft was hijacked after its departure from Cozumel, Mexico. The three hijackers demanded to be taken to Cuba.

**October 30, 1968**
**Hijacking:** An SAESA aircraft was hijacked after its departure from Tampico, Mexico. The hijacker demanded to be taken to Brownsville, Texas.

**November 2, 1968**
**Hijacking:** An Eastern Airlines MD DC-9 was hijacked en route to Chicago from Mobile, Alabama. The hijacker demanded to be taken to South Vietnam.

**November 4, 1968**
**Hijacking:** A National Airlines B-727 was hijacked en route from New Orleans, Louisiana, to Miami. The hijacker demanded to be taken to Cuba.

**November 6, 1968**
**Hijacking:** Four hijackers demanding money seized a Philippine Air Lines aircraft en route from Abu to Manila, the Philippines.

**November 8, 1968**
**Hijacking:** Two hijackers seized an Olympic Airways B-707 en route from Paris, France, to Athens, Greece.

**November 18, 1968**
**Hijacking:** Two hijackers demanding to be taken to Cuba seized a Mexicana aircraft departing Mérida-Rejon Airport, Mexico.

**November 19, 1968**
**Bombing:** There was an explosion in the lavatory of a Continental Air Lines B-707 upon its descent into Denver International Airport. The flight originated in Los Angeles.

**November 23, 1968**
**Hijacking:** Nine hijackers seized an Eastern Air Lines B-727 en route to Miami from Chicago. They demanded to be flown to Cuba.

**November 24, 1968**
**Hijacking:** Three hijackers, demanding to be flown to Cuba, seized a Pam Am B-707 aircraft en route from New York to San Juan.

**November 30, 1968**
**Hijacking:** An Eastern Airlines B-720 was hijacked en route to Dallas, Texas, from Miami. The hijacker demanded to be flown to Cuba.

**December 3, 1968**
**Hijacking:** A hijacker seized a National Airlines B-727 en route from Tampa to Miami in order to go to Cuba.

**December 11, 1968**
**Hijacking:** Two hijackers demanded to go to Cuba on board a TWA B-727 en route to Nashville, Tennessee, from Miami.

**December 19, 1968**
**Hijacking:** An Eastern Airlines MD DC-8 was hijacked en route from Philadelphia, Pennsylvania, to Miami by two hijackers demanding to be flown to Cuba.

**December 26, 1968**
**Shooting:** Israeli commandos opened fire on an El Al (Israel Airlines) plane in Athens.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."
Source for the 1968 section (unless otherwise stated): Aviation Safety Network Databases, http://aviationsafety.net/database/.

## 1969

**Hijackings:** There were 87 hijackings in total. Out of these, 40 involved U.S. aircraft and 47 involved foreign aircraft.
Source: "FAA History Chronology, 1926–1996"

**January 1969**
**Hijacking:** A total of eight U.S. airliners were hijacked during January 1969.
Source: "FAA History Chronology, 1926–1996"

**January 2, 1969**
**Hijacking:** An Olympic Airways aircraft was taken over by one hijacker after departing Heraklion Airport en route to Athens.

**January 2, 1969**
**Hijacking:** Three hijackers demanded to be taken to Cuba on board an Eastern Air Lines flight en route from JFK Airport in New York to Miami.

**January 7, 1969**
**Hijacking:** An Avianca flight was hijacked while on a domestic flight in Colombia departing from Riohacha-Almirante Padilla Airport. The hijacker wanted to go to Cuba.

**January 9, 1969**
**Hijacking:** An Eastern Airlines B-727 was hijacked en route from Miami to Nassau, in the Bahamas. The hijacker demanded to be flown to Cuba.

**January 11, 1969**
**Hijacking:** A United Air Lines B-727 was hijacked en route from Jacksonville, Texas, to Miami. The hijacker demanded to be flown to Cuba.

**January 11, 1969**
**Hijacking:** An Aerovias Peruanas (APSA) flight was hijacked en route from Panama City to Miami. The hijacker demanded to be flown to Cuba.

**January 13, 1969**
**Hijacking:** A Delta Air Lines flight was hijacked en route from Detroit, Michigan, to Miami. The hijacker demanded to be flown to Cuba.

**January 19, 1969**
**Hijacking:** An Ecuatoriana airliner was hijacked en route from Guayaquil–Simon Bolivar Airport, Equador, to Quito, Equador. The 10 hijackers demanded to be flown to Cuba.

**January 19, 1969**
**Hijacking:** An Eastern Air Lines flight was hijacked en route to Miami from New York. The hijacker demanded to be flown to Cuba.

**January 24, 1969**
**Hijacking:** A National Airlines B-727 was hijacked en route from Key West to New York. The hijacker demanded to be flown to Cuba.

**January 28, 1969**
**Hijacking:** A National Airlines MD DC-8 aircraft was hijacked en route from New Orleans to Miami. The two hijackers demanded to be flown to Cuba.

**January 28, 1969**
**Hijacking:** An Eastern Airlines MD DC-8 was hijacked en route to Miami from Atlanta, Georgia. The three hijackers demanded to be flown to Cuba.

**January 31, 1969**
**Hijacking:** A National Airlines flight was hijacked en route between San Francisco and Tampa. The hijacker demanded to be flown to Cuba.

**February 3, 1969**
**Hijacking:** A National Airlines B-727 was seized en route from New York to Miami by two hijackers.

**February 3, 1969**
**Hijacking:** An Eastern Airlines B-727 was hijacked en route from Newark, New Jersey, to Miami. The four hijackers demanded to be flown to Cuba.

**February 5, 1969**
**Hijacking:** A SAM Colombia airliner was hijacked en route from Barranquilla to Medellín, Colombia. The hijacker demanded to be flown to Cuba.

**February 6, 1969**
**Hijacking:** A Venezuelan plane en route to Havana was hijacked by seven men.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**February 8, 1969**
**Hijacking:** A Douglas DC-6 aircraft was hijacked after departure from Mexico City. The hijacker demanded to be flown to Cuba.

**February 10, 1969**
**Hijacking:** An Eastern Air Lines airliner was hijacked en route from San Juan to Miami. The hijacker demanded to be flown to Cuba.

**February 11, 1969**
**Hijacking:** A Linea Aeropostal Venezolana (LAV) airliner was hijacked en route from San Juan to Miami. The three hijackers demanded to be flown to Cuba.

**February 25, 1969**
**Hijacking:** An Eastern Airlines MD DC-8 was hijacked en route to Miami from Atlanta. The hijacker demanded to be flown to Cuba.

**March 5, 1969**
**Hijacking:** A National Airlines B-727 was hijacked en route from New York to Miami. The hijacker demanded to be flown to Cuba.

**March 11, 1969**
**Bombing:** There were two explosions in the passenger compartment while an Ethiopian Airlines B-707 was on the ground at Frankfurt International Airport, Germany.

**March 11, 1969**
**Hijacking:** A SAM Colombia airliner was hijacked en route from Medellín to Cartagena. The hijacker demanded to be flown to Cuba.

**March 15, 1969**
**Hijacking:** An Aerovias Condor was hijacked en route to San Andrés Island, Colombia, from Barranquilla, Colombia. The hijacker demanded to be flown to Cuba.

**March 17, 1969**
**Hijacking:** A Delta Air Lines MD DC-9 was hijacked en route to Augusta, Georgia, from Atlanta. The hijacker demanded to be flown to Cuba.

**March 17, 1969**
**Hijacking:** A Faucett B-727 was hijacked en route from Lima to Arequipa-Rodriguez Ballon Airport, Peru. The four hijackers demanded to be flown to Cuba.

**March 19, 1969**
**Hijacking:** A Delta Air Lines airliner was hijacked en route from Dallas, Texas, to New Orleans, Louisiana. The hijacker demanded to be flown to Cuba.

**March 25, 1969**
**Hijacking:** A Delta Air Lines MD DC-8 was hijacked en route from Dallas to San Diego. The hijacker demanded to be flown to Cuba.

**April 11, 1969**
**Hijacking:** A Douglas DC-6 airliner was hijacked en route to Quito from Guayaquil-Simon Bolivar Airport, Ecuador. The three hijackers demanded to be flown to Cuba.

**April 13, 1969**
**Hijacking:** A Pan Am B-727 was hijacked during a flight from San Juan to Miami. The four hijackers demanded to be flown to Cuba.

**April 14, 1969**
**Hijacking:** A SAM Colombia airliner was hijacked en route from Medellín to Barranquilla, Colombia. The three hijackers demanded to be flown to Cuba.

**May 5, 1969**
**Hijacking:** A National Airlines B-727 was hijacked during a flight from New York to Miami. The two hijackers demanded to be flown to Cuba.

**May 20, 1969**
**Hijacking:** An Avianca B-737 was hijacked en route to Pereira from Bogotá, Colombia. The three hijackers demanded to be flown to Cuba.

**May 26, 1969**
**Hijacking:** A Northeast Airlines B-727 was hijacked en route from Miami to New York. The three hijackers demanded to be flown to Cuba.

**May 30, 1969**
**Hijacking:** A Texas International Airlines flight from New Orleans to Alexandria Airport, Egypt, was hijacked. The hijacker demanded to be flown to Cuba.

**June 4, 1969**
**Hijacking:** Three hijackers attempted to seize a Direcção de Exploração dos Transp. Aéreos (DTA) airliner en route from Ambrizete, Brazil, to Santo Antonio do Zaire, Brazil.

**June 8, 1969**
**Hijacking:** A Portuguese airliner was diverted to Pointe-Noire, Congo Brazauille, by two people in Portuguese army uniforms.

Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**June 17, 1969**
**Hijacking:** A TWA B-707 was hijacked en route to New York from Oakland, California. The hijacker demanded to be flown to Cuba.

**June 18, 1960**
**Hijacking:** An Ethiopian airliner was hijacked in Karachi by members of Eritrean Liberation Front (ELF).
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**June 20, 1969**
**Hijacking:** Four hijackers demanded to be flown to Cuba on board a Lineas Aéreas La Urraca flight from Villavicencio–La Vanguardia Airport to Monterrey Airport, Colombia.

**June 22, 1969**
**Hijacking:** An Eastern Air Lines MD DC-8 was hijacked en route from Newark to Miami. The three hijackers demanded to be flown to Cuba.

**June 25, 1969**
**Hijacking:** A United Air Lines MD DC-8 was hijacked en route to New York from Los Angeles. The hijacker demanded to be flown to Cuba.

**June 28, 1969**
**Hijacking:** An Eastern Air Lines B-727 was hijacked en route to Tampa from Baltimore. The hijacker demanded to be flown to Cuba.

**July 3, 1969**
**Hijacking:** A SAETA airliner was hijacked en route from Tulcán to Quito, Ecuador. The 13 hijackers demanded to be flown to Cuba.

**July 10, 1969**
**Hijacking:** An Avianca airliner was hijacked en route to Santa Marta from Barranquilla, Colombia. The hijacker demanded to be flown to Cuba.

**July 10, 1969**
**Hijacking:** A SAM Colombia aircraft was hijacked en route to Bogotá. The hijacker demanded to be flown to Cuba.

**July 26, 1969**
**Hijacking:** A Continental Air Lines airliner was seized en route from El Paso to Midland, Texas. The hijacker demanded to be flown to Cuba.

**July 26, 1969**
**Hijacking:** A Mexicana Douglas DC-6 was hijacked en route to Villa Hermosa, Mexico. The two hijackers demanded to be flown to Cuba.

**July 29, 1969**
**Hijacking:** An airliner after departing Managua Airport, Nicaragua, was hijacked in order to be flown to Cuba.

**July 31, 1969**
**Hijacking:** A TWA B-727 was hijacked en route to Los Angeles from Philadelphia. The hijacker demanded to be flown to Cuba.

**August 4, 1969**
**Hijacking:** An Avianca airliner was hijacked after departing from Santa Marta–Simon Bolívar Airport, Colombia. The three hijackers demanded to be flown to Cuba.

**August 5, 1969**
**Bombing:** A passenger on board a Philippine Air Lines flight exploded a bomb in the lavatory of the plane. The explosion pushed the passenger out of the plane, but the plane landed safely.

**August 5, 1969**
**Hijacking:** An Eastern Air Lines MD DC-9 was hijacked en route from Charlotte, North Carolina, to Tampa. The hijacker demanded to be flown to Cuba, to see if he had the nerve to simulate a hijacking.

**August 9, 1969**
**Bomb:** Two American tourists were injured when a bomb exploded at an Olympic Airways facility in Athens.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**August 11, 1969**
**Hijacking:** Seven hijackers seized an Ethiopian Airlines airliner en route to Addis Ababa–Bole Airport.

**August 14, 1969**
**Hijacking:** Two hijackers seized a Northeast Airlines B-727 en route to Miami from Boston, Massachusetts, in order to be flown to Cuba.

**August 16, 1969**
**Hijacking:** Four hijackers demanding to be taken to Albania seized an Olympic Airways airliner after its departure from Athens.

**August 18, 1969**
**Hijacking:** Six hijackers seized a Misrair airliner en route from Cairo to Luxor Airport, Egypt.

**August 23, 1969**
**Hijacking:** Two hijackers seized an Avianca airliner en route to Bogotá. The target was Cuba.

**August 29, 1969**
**Hijacking:** A U.S. aircraft outside the Western Hemisphere, a TWA 707 bound for Greece, was hijacked and diverted to Syria.
Source: "FAA History Chronology, 1926–1996"; Aviation Safety Network Database: http://aviation-safety.net/database/events/event.php?code=SE.

**August 29, 1969**
**Hijacking:** A National Airlines B-727 was hijacked en route to New Orleans from Miami. The hijacker demanded to be flown to Cuba.

**September 6, 1969**
**Hijacking:** Seven hijackers seized a TAME Ecuador airliner in order to be flown to Cuba.

**September 6, 1969**
**Hijacking:** Six hijackers seized a TAME Ecuador airliner in order to be flown to Cuba.

**September 7, 1969**
**Hijacking:** An Eastern Air Lines airliner en route from New York to San Juan. The hijacker demanded to be flown to Cuba.

**September 10, 1969**
**Hijacking:** An Eastern Air Lines MD DC-8 was hijacked en route to San Juan from New York. The hijacker demanded to be flown to Cuba.

**September 13, 1969**
**Hijacking:** A Servicio Aéreo de Honduras (SAHSA) airliner was hijacked en route to Tegucigalpa, Honduras.

**September 13, 1969**
**Hijacking:** Three hijackers seized an Ethiopian Airlines aircraft en route from Addis Ababa–Bole Airport, Ethiopia, to Djibouti.

**September 16, 1969**
**Hijacking:** A Türk Hava Yollari (THY) flight was hijacked en route to Ankara from Istanbul, Turkey.

**September 24, 1969**
**Hijacking:** A National Airlines B-727 was hijacked en route from Charleston, South Carolina, to Miami. The hijacker demanded to be flown to Cuba.

**October 8, 1969**
**Hijacking:** An Aerolineas Argentinas B-707 was hijacked en route from Buenos Aires to Miami. The hijacker demanded to be flown to Cuba.

**October 8, 1969**
**Hijacking:** A Cruzerio airliner was hijacked en route from Belém Airport to Manaus, Brazil. The four hijackers demanded to be flown to Cuba.

**October 9, 1969**
**Hijacking:** A National Airlines flight from Los Angeles to Miami, Florida was hijacked. The hijacker demanded to be flown to Cuba.

**October 19, 1969**
**Hijacking:** Two hijackers seized a LOT airliner en route to Germany from Poland.

**October 21, 1969**
**Hijacking:** A Pan Am B-720 was hijacked en route to Miami from Mexico City. The hijacker demanded to be flown to Cuba.

**October 28, 1969**
**Hijacking:** Two hijackers seized an airliner on a domestic flight to Bogotá.

**October 31, 1969**
**Hijacking:** A U.S. Marine who was absent without leave hijacked a TWA 707 plane bound for San Francisco and diverted the plane on a 17-hour journey that ended in Rome.
Source: "FAA History Chronology, 1926–1996."

**November 4, 1969**
**Hijacking:** A Varig airliner was hijacked en route to Santiago, Chile, from Buenos Aires, Argentina. The six hijackers demanded to be flown to Cuba.

**November 4, 1969**
**Hijacking:** A Nicaraguan flight was hijacked en route to Mexico from Miami.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**November 4, 1969**
**Hijacking:** A LANICA aircraft was hijacked en route from Managua Airport to San Salvador, El Salvador. The two hijackers demanded to be flown to Cuba.

**November 8, 1969**
**Hijacking:** An Austral Lineas Aéreas aircraft was hijacked en route to Buenos Aires. The hijacker demanded to be taken to Cuba.

**November 10, 1969**
**Hijacking:** A hijacker demanding to be taken to Sweden/Mexico seized a Delta Air Lines airliner en route to Chicago from Cincinnati, Ohio.

**November 12, 1969**
**Hijacking:** A Cruzerio airliner was hijacked en route from Manaus, Brazil, to Belém Airport. The hijacker demanded to be taken to Cuba.

**November 12, 1969**
**Hijacking:** Two hijackers demanding to be flown to Cuba seized a LAN Chile airliner after its departure from Santiago, Chile. The two hijackers were taken down.

**November 13, 1969**
**Hijacking:** Six hijackers demanded an Avianca airliner en route to Bogotá be flown to Cuba.

**November 20, 1969**
**Hijacking:** Two hijackers demanded an LOT airliner en route from Poland to Slovakia to be flown to Vienna, Austria.

**November 27, 1969**
**Bombing:** An El Al (Israel Airlines) office was a target of hand grenades in Athens.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**November 29, 1969**
**Hijacking:** A hijacker demanded a Varig flight from Paris to Rio de Janeiro to be flown to Cuba.

**December 2, 1969**
**Hijacking:** A TWA B-707 flight from San Francisco to Philadelphia was hijacked. The hijacker demanded to be flown to Cuba.

**December 11, 1969**
**Hijacking:** A Korean Air Lines (KAL) aircraft en route to Seoul-Gimpo from Kangnung Airport, South Korea, was hijacked and diverted to North Korea.

**December 12, 1969**
**Hijacking:** Two hijackers seized an Ethiopian Airlines B-707 en route from Madrid to Addis Ababa-Bole Airport, Ethiopia.

**December 19, 1969**
**Hijacking:** A LAN Chile B-727 was hijacked en route to Arica Airport, Colombia, from Santiago, Chile. The hijacker demanded to be flown to Cuba.

**December 23, 1969**
**Hijacking:** A Lineas Aéreas Costarricenses (LACSA) airliner was hijacked en route from Puerto Limon, Costa Rica, to San José, Costa Rica. The hijacker demanded to be flown to Cuba.

**December 24, 1969**
**Attempted bombing:** Three members of the PFLP were arrested as they were boarding a TWA flight to Rome and New York. They were found to be carrying explosives and were armed.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**December 26, 1969**
**Hijacking:** A hijacker seized a United Air Lines B-727 en route from New York to Chicago in order to be flown to Cuba.
Source for the 1969 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1970

**January 1, 1970**
**Hijacking:** A Cruzeiro airliner was hijacked en route from Montevideo, Uruguay, to Rio de Janeiro, Brazil. The four hijackers demanded to be flown to Cuba.

**January 6, 1970**
**Hijacking:** A hijacker seized a Delta Air Lines flight en route to Atlanta, Georgia, from Orlando, Florida, in order to be taken to Switzerland.

**January 7, 1970**
**Hijacking:** An Iberia flight was hijacked en route to Zaragoza from Madrid. The hijacker demanded to be taken to Albania.

**January 8, 1970**
**Hijacking:** A TWA 707 airliner en route from Paris to Rome was hijacked to Beirut, Lebanon.

**January 9, 1970**
**Hijacking:** A hijacker demanded that a Panamá Rutas Aéreas Panameñas SA (RAPSA) airliner flight be flown to Cuba.

**January 24, 1970**
**Hijacking:** Four hijackers seized an Antillean Airlines (ALM) airliner en route from Santo Domingo to the Netherlands Antilles in order to be flown to Cuba.

**February 6, 1970**
**Hijacking:** A LAN Chile airliner was hijacked en route to Santiago. The two hijackers demanded to be flown to Cuba.

**February 10, 1970**
**Airport Attack:** El Al passengers on a bus at Munich Airport, Germany, were attacked by three terrorists with guns and grenades.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State," www.globalspecialoperations.com/techran2.html.

**February 16, 1970**
**Hijacking:** An Eastern Airlines B-727 was hijacked en route to Miami from Newark. The four hijackers demanded to be flown to Cuba.

**February 21, 1970**
**Bombing:** An explosion on board an Austrian Airlines in the forward freight hold blew a hole in the fuselage during a flight from Germany to Austria.

**February 21, 1970**
**Bombing:** A bomb exploded after takeoff in the rear of a Swissair aircraft en route to Tel Aviv.

**March 1, 1970**
**Attempted bombing:** Members of ELF placed explosives in luggage on an Ethiopian airliner on the ground in Rome.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**March 10, 1970**
**Hijacking:** The hijackers reportedly committed suicide after an ill-fated attempt to hijack an Interflug airliner en route to Leipzig Airport, German Democratic Republic.

**March 11, 1970**
**Hijacking:** Four hijackers demanding to be taken to Cuba seized an Avianca B-727 en route to Barranquilla Airport, Colombia.

**March 11, 1970**
**Hijacking:** Six hijackers demanding to be flown to Cuba seized a United Air Lines B-727 en route to West Palm Beach, Florida, from Cleveland.

**March 12, 1970**
**Hijacking:** A hijacker demanded to be taken to Cuba after seizing a Varig B-707 en route to London from Chile.

**March 14, 1970**
**Bombing:** A United Arab Airlines (UAA) flight suffered an explosion in the engine nacelle after departing from Alexandria Airport, Egypt.

**March 17, 1970**
**Hijacking:** The copilot was murdered and the pilot was wounded on an Eastern Airlines shuttle from Newark to Boston.
Source: "FAA History Chronology, 1926–1996."

**March 24, 1970**
**Hijacking:** An Aerolineas Argentinas flight was hijacked en route to Tucuman Airport, Argentina. The two hijackers demanded to be flown to Cuba.

**March 31, 1970**
**Hijacking:** A Japan Air Lines (JAL) B-727 was seized en route from Tokyo to Fukuoka. The nine hijackers demanded to be flown to North Korea.

**April 23, 1970**
**Hijacking:** A North Central Airlines flight was hijacked en route to Sault Ste. Marie Airport, Ontario, from Pellston-Emmet County Airport, Michigan. The hijacker demanded to be taken to Detroit.

**April 25, 1970**
**Hijacking:** A VASP B-737 was hijacked en route to Manaus, Brazil. The hijacker demanded to be flown to Cuba.

**April 25, 1970**
**Bombing:** An El Al Israel Airlines office in Istanbul was bombed.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**May 1, 1970**
**Hijacking:** Two hijackers demanding to be taken to Cuba seized a British West Indian Airways (BWIA) B-727 en route to the Cayman Islands from Jamaica.

**May 12, 1970**
**Hijacking:** Seven hijackers demanded to be taken to Cuba after seizing a ALM airliner en route to the Netherlands Antilles from Santo Domingo.

**May 14, 1970**
**Hijacking:** A hijacker demanded to be flown to Cuba after seizing a VASP B-737 en route to Manaus, Brazil.

**May 14, 1970**
**Hijacking:** A flight between Sydney and Brisbane, Australia, was hijacked.

**May 21, 1970**
**Hijacking:** Four hijackers demanded to be flown to Cuba after seizing an Avianca flight after its departure from El Yopal Airport, Colombia.

**May 24, 1970**
**Hijacking:** A Mexicana B-727 was hijacked en route to Mexico City. The hijacker demanded to be flown to Cuba.

**May 25, 1970**
**Hijacking:** A hijacker seized an American Airlines Chicago to New York flight in order to be flown to Cuba.

**May 25, 1970**
**Hijacking:** Two hijackers demanded to be flown to Cuba after seizing a Delta Air Lines flight en route to Miami from Chicago.

**May 30, 1970**
**Hijacking:** An Avianca flight was hijacked after departing from Bogotá. The seven hijackers demanded to be flown to Cuba.

**June 2, 1970**
**Bombing:** A Philippine Air Lines flight from Manila to Bacolod Airport had a hand grenade detonate inside the passenger cabin.

**June 4, 1970**
**Hijacking:** A TWA 727 jet on a Phoenix–Washington, DC, flight was hijacked for money.

**June 5, 1970**
**Hijacking:** A hijacker seized a LOT flight en route to Gdansk, Poland, in order to gain political asylum.

**June 8, 1970**
**Hijacking:** Nine hijackers seized a CSA flight after its departure from Karlovy Vary Airport in the Czech Republic in order to be taken to Germany.

**June 9, 1970**
**Hijacking:** Two hijackers were taken down on an LOT flight after its departure from Katowice, Poland.

**June 21, 1970**
**Hijacking:** An Iran Air B-727 was hijacked en route to Abadan Airport, Iran, from Tehran.

**June 22, 1970**
**Hijacking:** A Pan Am B-707 was hijacked en route to Rome from Beirut. The hijacker demanded to be flown to Egypt.

**June 22, 1970**
**Hijacking:** A U.S. citizen with an Albanian passport hijacked a Pan American World Airways jet bound from Beirut to New York.
Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**June 26, 1970**
**Hijacking:** Two hijackers demanding to be flown to Cuba seized an Avianca B-727 en route to Bogotá from Cucuta, Colombia.

**July 1, 1970**
**Hijacking:** A National Airlines flight from New Orleans to Miami was hijacked. The hijacker demanded to be flown to Cuba.

**July 1, 1970**
**Hijacking:** Four hijackers demanding to be flown to Cuba and demanding the release of prisoners seized a Cruzeiro flight en route to São Paulo from Rio de Janeiro, Brazil.

**July 4, 1970**
**Hijacking:** A Cruzeiro flight was hijacked en route to Macapá International Airport, Brazil.

**July 12, 1970**
**Hijacking:** A Saudi Arabian Airlines B-707 was hijacked en route to Beirut from Riyadh, Saudi Arabia.

**July 22, 1970**
**Hijacking:** An Air Vietnam flight was hijacked en route from Pleiku Airport, Vietnam, to Saigon Airport.

**July 22, 1970**
**Hijacking:** Six hijackers demanding the release of prisoners in Cairo, Egypt, seized an Olympic Airways B-727 en route to Athens from Beirut.

**July 25, 1970**
**Hijacking:** Four hijackers demanding to be flown to Cuba seized an Aeronaves de Mexico aircraft en route to Mexico City from Acapulco.

**July 28, 1970**
**Hijacking:** An Aerolineas Argentinas flight was hijacked en route to Buenos Aires from Salta Airport. The hijacker demanded to be flown to Cuba.

**August 2, 1970**
**Hijacking:** A Pan American 747 from New York was hijacked. This was the first hijacking of a wide-bodied airliner.
Source: "FAA History Chronology, 1926–1996."

**August 3, 1970**
**Hijacking:** A Pan Am B-727 was hijacked en route to West Berlin from München-Riem Airport, Germany. The hijacker demanded to be flown to Hungary.

**August 7, 1970**
**Hijacking:** A hijacker demanding to be flown to Germany seized a LOT flight en route to Katowice Airport, Poland.

**August 8, 1970**
**Hijacking:** Three hijackers seized a CSA flight after departing from Praha-Ruzyne International Airport in the Czech Republic and demanded to be flown to Austria.

**August 19, 1970**
**Hijacking:** An All Nippon Airways flight between Nagoya-Komaki Airport, Japan, and Sapporo was hijacked.

**August 19, 1970**
**Hijacking:** Three hijackers demanding to be flown to Cuba seized a Trans Caribbean Airways flight between Newark, New Jersey, and San Juan.

**August 19, 1970**
**Hijacking:** Five hijackers seized a LOT flight after its departure from Gdansk, Poland. They demanded to be flown to Denmark.

**August 20, 1970**
**Hijacking:** A hijacker seized a Delta Air Lines flight between Atlanta and Savannah, Georgia, in order to be flown to Cuba.

**August 24, 1970**
**Hijacking:** A TWA flight from Chicago to Philadelphia was hijacked. The hijacker demanded to be flown to Cuba.

**August 26, 1970**
**Hijacking:** Three hijackers seized a LOT flight after departing from Katowice, Poland. They demanded to be flown to Austria.

**August 31, 1970**
**Hijacking:** An Air Algerie flight was hijacked en route to Algiers Airport. The three hijackers demanded to be flown to Albania.

**September 6–9, 1970**
**Hijacking:** A hijacking occurred involving four airplanes and five governments (the United States, Germany, Switzerland, Israel, and Britain). It was carried out by the Palestinian Liberation Front.
Source: "FAA History Chronology, 1926–1996."

**September 6, 1970**
**Hijacking:** A Pan Am B-747 was hijacked en route from Amsterdam to New York. Seven others boarded the flight after the two original hijackers diverted the plane to Beirut.

**September 6, 1970**
**Hijacking:** An El Al Israel Airlines B-707 was hijacked en route to Amsterdam from New York. The pilot threw the plane into a steep nosedive and was able to knock the two hijackers off their feet.

**September 10, 1970**
**Hijacking:** Three hijackers seized a flight en route from Beirut to Cairo.

**September 12, 1970**
**Hijacking:** A BOAC flight from Bahrain to Lebanon was hijacked by the PFLP.

**September 12, 1970**
**Hijacking:** An Egyptian plane en route from Tripoli, Libya, to Cairo.

**September 13, 1970**
**Hijacking:** The PFLP hijacked a TWA B-707 en route to New York from Frankfurt International Airport.

**September 13, 1970**
**Hijacking:** A Swiss Air flight from Zurich to New York was seized. The flight was hijacked on September 6, but the plane was blown up by the PFLP on September 13.

**September 14, 1970**
**Hijacking:** A Tarom flight from Bucharest, Romania, to the Czech Republic was hijacked. The six hijackers demanded to be flown to Germany.

**September 15, 1970**
**Hijacking:** A passenger on board TWA flight from Los Angeles to San Francisco pulled a handgun and demanded to be flown to North Korea.

**September 16, 1970**
**Hijacking:** A hijacker was taken down on board a UAA flight from Luxor to Cairo, Egypt.

**September 19, 1970**
**Hijacking:** A hijacker demanded to be taken to Cuba after seizing an Allegheny Airlines flight from Pittsburgh to Philadelphia, in Pennsylvania.

**September 22, 1970**
**Hijacking:** An Eastern Air Lines flight from Boston to San Juan was seized. The hijacker demanded to be flown to Cuba.

**October 10, 1970**
**Hijacking:** Three hijackers demanding to be flown to Iraq seized an Iran Air B-727 en route to Abadan Airport from Tehran.

**October 15, 1970**
**Hijacking:** Two hijackers seized an Aeroflot flight after its departure from Batumi-Chorokh Airport, Georgia, and demanded to be flown to Turkey.

**October 21, 1970**
**Hijacking:** Seven hijackers demanding to be flown to Cuba seized a LACSA flight from Costa Rica to San José.

**October 27, 1970**
**Hijacking:** An Aeroflot flight was hijacked en route to Sevastopol Airport, Ukraine. The two hijackers demanded to be flown to Turkey.

**October 30, 1970**
**Hijacking:** A National Airlines flight was hijacked en route from Miami to Tampa. The seven hijackers demanded to be flown to Cuba.

**November 1, 1970**
**Hijacking:** A United Air Lines flight from San Diego to Los Angeles was hijacked. The three hijackers demanded to be flown to Cuba.

**November 1, 1970**
Hijacking: A National Airlines jet from Miami to San Francisco was hijacked.
Source: *New York Times*, November 1, 1970.

**November 4, 1970**
**Hijacking:** An Eastern Airlines jet on a Richmond to Dallas flight was hijacked.
Source: *New York Times*, November 4, 1970.

**November 9, 1970**
**Hijacking:** Two hijackers seized an Aeroflot flight after its departure from Vilna en route to Palanga Airport, Lithuania.

**November 9, 1970**
**Hijacking:** Nine hijackers demanding to be taken to Iraq seized a flight from Dubai Airport en route to Bandar Abbas Airport, Iran.

**November 10, 1970**
**Hijacking:** A Saudi Arabian Airlines flight from Amman, Jordan, to Riyadh was hijacked.

**November 13, 1970**
**Hijacking:** An Eastern Airlines flight from Raleigh, North Carolina, to Atlanta was hijacked. The hijacker demanded to be flown to Cuba.

**December 10, 1970**
**Hijacking:** A CSA flight from Slovakia to the Czech Republic was hijacked.

**December 19, 1970**
**Hijacking:** A Continental Air Lines flight from Wichita, Kansas, to Tulsa, Oklahoma, was hijacked. The hijacker handed a note to the stewardess that stated he had a gun and he demanded to be taken to Cuba.

**December 21, 1970**
**Hijacking:** A Prinair flight from San Juan to Ponce-Mercedita Airport, Puerto Rico, was hijacked. The hijacker demanded to be flown to Mexico.
Source for the 1970 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1971

**January 3, 1971**
**Hijacking:** Seven hijackers seized a National Airlines fight from Los Angeles to Tampa.

**January 22, 1971**
**Hijacking:** A Northwest Airlines flight from Milwaukee, Wisconsin, to Detroit was seized. The hijacker demanded to be flown to Cuba.

**January 22, 1971**
**Hijacking:** An Ethiopian Airlines was seized en route to Gondar Airport from Bahar Dar Airport, Ethiopia.

**January 23, 1971**
**Hijacking:** A KAL flight from Kangnung Airport to Seoul-Gimpo Airport, South Korea, was seized. The hijacker was carrying grenades.

**January 26, 1971**
**Hijacking:** A hijacker demanded to be taken to Cuba on board an Aerovias Quisqueyana flight after its departure from Cabo Rojo Airport, Dominican Republic.

**February 2, 1971**
**Hijacking:** An Indian Airlines flight from Srinagar Airport to Jammu-Satwari Airport, India, was hijacked on January 20. The two hijackers set the plane on fire on February 2.

**February 4, 1971**
**Hijacking:** A Delta Air Lines flight from Chicago to Nashville, Tennessee, was hijacked. The hijacker demanded to be flown to Cuba.

**February 25, 1971**
**Hijacking:** A hijacker demanded to be taken to Cuba after seizing a Western Airlines B-737 en route to Seattle, Washington, from San Francisco.

**March 8, 1971**
**Hijacking:** A National Airlines flight from Mobile, Alabama, to New Orleans was seized. The hijacker demanded to be flown to Canada.

**March 19, 1971**
**Hijacking:** A KLM flight from Suriname to the Netherlands was hijacked. The hijacker demanded to be flown to Sweden.

**March 30, 1971**
**Hijacking:** Six hijackers seized a Philippine Air Lines flight from Manila to Davao-Mati Airport.

**March 31, 1971**
**Hijacking:** A hijacker demanding to be flown to Cuba seized an Eastern Airlines flight from New York to San Juan.

**April 21, 1971**
**Hijacking:** A hijacker demanding to be flown to Italy seized an Eastern Airlines flight from Newark to Miami.

**April 25, 1971**
**Hijacking:** An Avianca flight was hijacked en route to Medellín from Barranquilla, Colombia.

**April 29, 1971**
**Hijacking:** An Avianca flight was hijacked en route to Bogotá from Los Angeles.

**May 8, 1971**
**Hijacking:** An Avianca flight from Monteria to Cartagena Airport, Colombia, was hijacked.

**May 13, 1971**
**Hijacking:** A hijacker was arrested on board an All Nippon Airways flight from Tokyo to Sendai, Japan.

**May 17, 1971**
**Hijacking:** A Scandinavian Airline System (SAS) flight to Stockholm was hijacked.

**May 27, 1971**
**Hijacking:** Six hijackers demanding to be flown to Austria seized a Tarom flight from Oradea Airport to Bucharest.

**May 28, 1971**
**Hijacking:** A hijacker demanding to be flown to New York; Nassau, Bahamas; and Ireland seized an Eastern Air Lines flight from Miami to New York.

**May 29, 1971**
**Hijacking:** A Pan Am flight from Caracas Airport to Miami was seized. The hijacker demanded to be taken to Cuba.

**June 4, 1971**
**Hijacking:** A hijacker demanding to be taken to Israel seized a United Air Lines flight from Charleston to Newark.

**June 11, 1971**
**Hijacking:** A TWA flight from Chicago to New York was seized. The hijacker demanded to be flown to North Vietnam.

**June 12, 1971**
**Hijacking:** A passenger trying to help the stewardess was killed by the hijacker, who seized the stewardess on a TWA aircraft bound from Albuquerque, New Mexico, to New York.
Source: "FAA History Chronology, 1926–1996."

**June 18, 1971**
**Hijacking:** A Piedmont Airlines flight was hijacked at Winston-Salem Airport, North Carolina. The hijacker demanded to be flown to Cuba.

**June 21, 1971**
**Hijacking:** An Avianca flight from Monteria to Medellín, Colombia, was hijacked.

**June 29, 1971**
**Hijacking:** A Finnair flight departing from Helsinki, Finland, was hijacked.

**July 2, 1971**
**Hijacking:** Two hijackers seized a Braniff Airways flight from Mexico City to San Antonio, Texas. They demanded money and to be flown to Algeria.

**July 11, 1971**
**Hijacking:** Two hijackers seized a Cubana de Aviacion flight after its departure from Havana.

**July 23, 1971**
**Hijacking:** A hijacker demanding to be flown to Italy seized a TWA flight from New York to Chicago. He was shot and killed as he attempted to change aircraft.

**July 24, 1971**
**Hijacking:** A National Airlines flight from Miami to Jacksonville, Florida, was seized. The hijacker demanded to be flown to Cuba.

**August 22, 1971**
**Hijacking:** A hijacker demanding to be taken to Israel seized a UAA flight from Cairo to Amman.

**August 24, 1971**
**Bombing:** An Alia Royal Jordanian Airlines aircraft suffered an explosion in the aft lavatory while parked at Madrid-Barajas Airport, Spain.

**September 3, 1971**
**Hijacking:** An Eastern Air Lines flight from Chicago to Miami was seized. The hijacker demanded to be flown to Cuba.

**September 8, 1971**
**Hijacking:** A hijacker on board an Alia Royal Jordanian Airlines flight from Beirut to Amman. used a hand grenade that she hid under her wig in an attempt to seize the plane.

**September 16, 1971**
**Hijacking:** A hijacker demanding to be flown to Iraq seized an Alia Royal Jordanian Airlines flight from Beirut to Amman.

**September 24, 1971**
**Hijacking:** An American Airlines flight from Detroit to New York was hijacked. The hijacker demanded to be taken to Algeria and demanded the release of prisoners.

**October 4, 1971**
**Hijacking:** Two hijackers demanding to be flown to Iraq seized an Alia Royal Jordanian Airlines flight from Beirut to Amman.

**October 6, 1971**
**Hijacking:** A hijacker on an Olympic Airways flight en route to Greece demanded to be flown to Lebanon.

**October 9, 1971**
**Hijacking:** An Eastern Air Lines flight from Detroit to Miami. The hijacker demanded to be flown to Cuba.

**October 12, 1971**
**Hijacking:** Two hijackers seized an AVENSA aircraft en route to Caracas from Barcelona, Spain.

**October 18, 1971**
**Hijacking:** A hijacker demanding to be flown to Cuba seized a Wien Consolidated Airlines flight from Anchorage to Bethel Airport, Alaska.

**October 20, 1971**
**Hijacking:** Six hijackers seized a SAETA flight from Quito to Cuenca Airport, Ecuador.

**October 25, 1971**
**Hijacking:** An American Airlines flight from New York to San Juan. The target was Cuba.

**October 26, 1971**
**Hijacking:** A hijacker demanded to be taken to Italy after seizing an Olympic Airways flight from Athens to Crete.

**November 12, 1971**
**Hijacking:** An Air Canada flight from Calgary to Toronto was hijacked. The target was Ireland.

**November 17, 1971**
**Hijacking:** An Arawak Airlines flight from Trinidad to Tobago was hijacked. The target was Cuba.

**November 21, 1971**
**Bombing:** A China Airlines flight crashed into the sea en route from Taipei (Taiwan) to Hong Kong.

**November 24, 1971**
**Hijacking:** D. B. Cooper, on a Northwest Airlines flight from Portland, Oregon, to Seattle, successfully demanded $200,000 and four parachutes, and then parachuted from the rear stairway of the B-727.
Source: "FAA History Chronology, 1926–1996"; Aviation Safety Network Database: http://aviation-safety.net/database.

**November 27, 1971**
**Hijacking:** Three hijackers seized a TWA flight from Albuquerque to Chicago. The target was Cuba.

**December 2, 1971**
**Hijacking:** In order to get supplies for Bangladesh, a hijacker seized a Pakistan International Airlines (PIA) flight from Paris to Karachi International Airport in Pakistan.

**December 12, 1971**
**Hijacking:** Three hijackers seized a LANICA flight from San Salvador to Managua. The target was Cuba.

**December 16, 1971**
**Hijacking:** A Lloyd Aéreo Boliviano (LAB) flight was hijacked en route to La Paz from Sucre Airport, Bolivia. The target was Chile.

**December 24, 1971**
**Hijacking involving extortion:** A Northwest Airlines flight from Minneapolis, Minnesota, to Chicago was hijacked. There was a demand for ransom money and parachutes.
Source: "FAA History Chronology, 1926–1996"; Aviation Safety Network Database: http://aviation-safety.net/database.

**December 26, 1971**
**Hijacking:** An Air Canada en route to Thunder Bay Airport, Ontario, from Toronto was hijacked.

**December 26, 1971**
**Hijacking:** An American Airlines flight from Chicago to San Francisco was hijacked.
Source for the 1971 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1972

**January 7, 1972**
**Hijacking:** A Pacific Southwest Airlines (PSA) flight from San Francisco to Los Angeles was hijacked. The three hijackers demanded to be flown to Africa and Cuba.

**January 12, 1972**
**Hijacking:** A Braniff Airways flight from Houston to Dallas was hijacked. Money was demanded.

**January 20, 1972**
**Hijacking:** A hijacker parachuted from a Hughes Airwest flight into the vicinity of Denver.

**January 26, 1972**
**Hijacking:** A Mohawk Airlines flight from Albany, NY to New York was hijacked. Money was demanded.

**January 26, 1972**
**Bombing:** A homemade bomb placed by Croatian extremists exploded in the forward cargo hold of a JAT flight en route to Serbia from Denmark.

**January 29, 1972**
**Hijacking:** A TWA flight from Los Angeles to New York was hijacked. Demands were made for the release of prisoners and money.

**February 19, 1972**
**Hijacking:** An Alia Royal Jordanian Airlines flight from Cairo to Amman was hijacked. The target was Libya.

**February 22, 1972**
**Hijacking:** A Lufthansa flight from New Delhi to Athens was hijacked. Five hijackers demanded money.

**March 6, 1972**
**Bombing/hijacking:** TWA was warned that four of its planes would be blown up at six-hour intervals unless $2 million in ransom was paid. One bomb exploded in a plane on the ground in Las Vegas and another was sniffed out by a dog at JFK airport in New York.
Source: "FAA History Chronology, 1926–1996."

**March 7, 1972**
**Bombings:** A bomb was discovered as part of an extortion plot and defused aboard a TWA plane at New York's JFK Airport.
Source: "FAA History Chronology, 1926–1996."

**March 7, 1972**
**Hijacking:** A National Airlines flight from Tampa to Melbourne, Florida, was hijacked. The target was Sweden.

**March 9, 1972**
**Bombings:** A bomb damaged a TWA airliner parked at Las Vegas. Another bomb was found aboard a United Air Lines jet at Seattle.
Source: "FAA History Chronology, 1926–1996."

**March 11, 1972**
**Hijacking:** An Alitalia flight from Rome to Milan was hijacked.

**April 5, 1972**
**Hijacking:** A Merpati Nusantara Airlines flight from Surabaya to Jakarta, Indonesia, was hijacked. Money was demanded.

**April 7, 1972**
**Hijacking:** A hijacker parachuted near Provo, Utah, from a United Air Lines flight from Denver to Los Angeles.

**April 8, 1972**
**Hijacking:** A Faucett flight from Piura Airport to Chiclayo, Peru, was hijacked.

**April 9, 1972**
**Hijacking:** A PSA flight from Oakland to San Diego was hijacked. Money was demanded.

**April 13, 1972**
**Hijacking:** A Frontier Airlines flight from Albuquerque to Phoenix was hijacked. The hijacker had a history of psychological problems and after giving a speech in Spanish over radio and TV he surrendered.

**April 16, 1972**
**Hijacking:** A Prinair flight from Ponce-Mercedita Airport to San Juan was hijacked.

**April 17, 1972**
**Hijacking:** A Delta Air Lines flight from West Palm Beach to Chicago was hijacked. Money was demanded.

**April 17, 1972**
**Hijacking:** An Alaska Airlines flight en route to Annette Island from Seattle was hijacked. The target was Egypt.

**April 17, 1972**
**Hijacking:** A Swissair flight en route to Rome was hijacked.

**April 18, 1972**
**Hijacking:** A Slovair flight was hijacked after departing from Praha-Ruzyne International Airport, Caechoslovakia. The two hijackers demanded to be flown to Germany.

**May 3, 1972**
**Hijacking:** Four hijackers seized a THY flight from Ankara to Istanbul. There was a demand for the release of prisoners.

**May 5, 1972**
**Hijacking:** A Western Air Lines flight from Salt Lake City, Utah, to Los Angeles was hijacked. The target was North Vietnam.

**May 5, 1972**
**Hijacking:** An Eastern Air Lines flight from Allentown International Airport, Pennsylvania, to Washington, DC. There was a demand for money.

**May 8, 1972**
**Hijacking:** A Sabena flight from Austria to Israel was seized by four hijackers. There was a demand for the release of prisoners.

**May 23, 1972**
**Hijacking:** A flight from Quito to Guayaquil, Ecuador, was hijacked. Money was demanded.

**May 24, 1972**
**Hijacking:** Two hijackers seized a South African Airways (SAA) flight from Zimbabwe to Johannesburg, South Africa.

**May 25, 1972**
**Bombing:** A homemade pipe bomb exploded in the fountain service compartment on board a LAN Chile flight en route to Miami from Panama City, Panama.

**May 28, 1972**
**Hijacking:** An Olympic Airways flight en route to Athens was hijacked. Demands were made for a ticket to London and medical treatment.

**May 30, 1972**
**Hijacking:** A Varig flight was hijacked after departing from São Paulo, Brazil. Money was demanded.

**May 31, 1972**
**Rifles and grenades in airport terminal:** Three armed Japanese men flew to Tel Aviv's Lod Airport on a flight from Paris and waited for an incoming El Al flight. They opened fire and threw hand grenades at the passengers.

Source: Jenkins and Johnson, "International Terrorism: A Chronology, 1968–1974."

**June 2, 1972**
**Hijacking:** A Western Air Lines flight from Los Angeles to Seattle was hijacked. There were demands for money and to be taken to Algiers.

**June 2, 1972**
**Hijacking:** A United Air Lines flight from Reno, Nevada, to San Francisco. There was a demand for money. The hijacker parachuted from the plane.

**June 8, 1972**
**Hijacking:** Eleven hijackers seized a Slovair en route to Praha-Ruzyne International Airport, Caechoslovakia. The target was West Germany.

**June 15, 1972**
**Bombing:** A Cathay Pacific flight from Bangkok to Hong Kong crashed after an explosion in the passenger cabin.

**June 23, 1972**
**Hijacking:** An American Airlines flight from St. Louis to Tulsa was hijacked. A demand was made for $502,000 then the hijacker parachuted from the plane near Peru, Indiana.

**June 30, 1972**
**Hijacking:** A Hughes Airwest flight from Seattle to Portland was hijacked. A demand for money was made.

**July 2, 1972**
**Hijacking:** A Pan Am flight from Manila to Saigon, Vietnam, was hijacked. The target was North Vietnam.

**July 5, 1972**
**Hijacking:** A PSA flight from Sacramento, California, to San Francisco was hijacked. Demands were made for money and to be flown to the Soviet Union.

**July 5, 1972**
**Hijacking:** A hijacker demanded to be flown out of the area in an empty American Airlines B-707 on the ground in Buffalo, New York.

**July 6, 1972**
**Hijacking:** A PSA flight from Oakland to Sacramento, was hijacked. Money was demanded.

**July 10, 1972**
**Hijacking:** A Lufthansa flight en route to Munich was hijacked. Money was demanded.

**July 12, 1972**
**Hijacking:** An American Airlines B-727 en route to Dallas from Oklahoma City was hijacked.

**July 12, 1972**
**Hijacking:** A UTA flight en route to Paris was hijacked.

**July 12, 1972**
**Hijacking:** Two hijackers seized a National Airlines B-727 flight from Philadelphia to New York. Money was demanded.

**July 31, 1972**
**Hijacking:** Eight hijackers seized a Delta Air Lines flight from Detroit to Miami in order to divert it to Algiers. Money was demanded.

**August 15, 1972**
**Hijacking:** Ten hijackers seized an Austral Lineas Aéreas flight en route to Buenos Aires from Trelew Airport, Argentina. A demand for political asylum was made.

**August 16, 1972**
**Bombing:** A bomb stored in a portable record player detonated in the aft baggage compartment after the departure of El Al Israel Airlines flight from Rome.

**August 18, 1972**
**Hijacking:** A United Airlines B-727 flight from Reno to San Francisco was hijacked and money was demanded.

**August 22, 1972**
**Hijacking:** Three hijackers seized an Alyemda flight in Benghazi, Libya.

**August 25, 1972**
**Hijacking:** Four hijackers seized an Aerolineas TAP aircraft en route to Bogotá.

**September 15, 1972**
**Hijacking:** Three members of the Croatian Ustasja Movement seized a Scandinavian Airlines System (SAS) aircraft en route to Stockholm, Sweden. Demands were made for money and the release of prisoners.

**September 16, 1972**
**Bombing:** A hand grenade exploded in the cargo compartment of an Air Manila International flight en route to Iligan, in the Philippines.

**October 6, 1972**
**Hijacking:** An Aero Transporti Italiani (ATI) was hijacked after departing from Trieste-Ronchi dei Legionari Airport, Italy. Money was demanded.

**October 11, 1972**
**Hijacking:** A Lufthansa flight from Lisbon to Frankfurt was hijacked. Money was demanded.

**October 22, 1972**
**Hijacking:** Four hijackers seized a THY flight from Istanbul to Ankara, Turkey. A demand was made for the release of prisoners.

**October 29, 1972**
**Hijacking:** Two hijackers seized a Lufthansa flight from Beirut to Ankara. A demand was made for the release of prisoners.

**October 29, 1972**
**Hijacking:** Four fugitives killed a ticket agent and hijacked an Eastern Air Lines B-727 at Houston, Texas.
Source: "FAA History Chronology, 1926–1996."

**November 6, 1972**
**Hijacking:** A JAL flight from Tokyo to Fukuoka was hijacked. Demands were made for money and to be flown to Cuba.

**November 8, 1972**
**Hijacking:** Four hijackers seized a Mexicana flight from Monterrey to Mexico City. Demands were made for money and the release of prisoners.

**November 10, 1972**
**Hijacking:** Three wanted criminals hijacked a Southern Airways DC-9 flying out of Birmingham, Alabama.
Source: "FAA History Chronology, 1926–1996."

**November 15, 1972**
**Hijacking:** An Ansett Airlines of Australia flight was hijacked on its approach to Alice Springs Airport.

**November 24, 1972**
**Hijacking:** An Air Canada flight was hijacked en route to Montreal, Quebec, from Frankfurt. A demand was made for the release of prisoners.

**December 8, 1972**
**Hijacking:** Seven hijackers attempted to seize an Ethiopian Airlines flight from Ethiopia to Eritrea.

**December 14, 1972**
**Hijacking:** A Quebecair flight from Wabush Airport to Montreal was hijacked.
Source for the 1972 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1973

**January 2, 1973**
**Hijacking:** A Piedmont Airlines flight from Washington, DC, to Baltimore was hijacked. The target was Canada.

**January 4, 1973**
**Hijacking:** A Pacific Western Airlines flight was hijacked after departing from Vancouver, Canada. Demands were made for money and to be flown to North Vietnam.

**April 24, 1973**
**Hijacking:** An Aeroflot flight from Leningrad to Moscow, USSR, was hijacked with an explosive device. The device killed both the hijacker and the flight engineer.

**May 18, 1973**
**Hijacking:** An Aeroflot flight from Irkutsk to Chita, USSR, was hijacked. The plane crashed when the hijacker's weapon exploded at a certain altitude.

**May 18, 1973**
**Hijacking:** Four hijackers seized an AVENSA flight en route to Barquisimeto Airport, Colombia. A demand was made for the release of prisoners.

**May 25, 1973**
**Hijacking:** An Aeroflot flight from Moscow to Chita, USSR, was hijacked.

**May 30, 1973**
**Hijacking:** Two hijackers seized a SAM Colombia aircraft en route to Bogotá. Demands were made for money and the release of prisoners.

**June 10, 1973**
**Hijacking:** Three hijackers seized a Royal Nepal Airlines after departing from Biratnagar Airport, Nepal. A demand was made for money.

**July 4, 1973**
**Hijacking:** An Aerolineas Argentinas flight was hijacked after departing from Buenos Aires. The hijacker demanded government grants to medical agencies.

**July 23, 1973**
**Hijacking:** Five hijackers seized a JAL flight en route to Anchorage, Alaska, from Amsterdam.

**August 16, 1973**
**Hijacking:** An armed hijacker entered the cockpit of a Middle East Airlines (MEA) B-720 en route from Libya to Lebanon.

**August 25, 1973**
**Hijacking:** A Yemen Airlines flight was hijacked en route to Eritrea from Yemen. The target was Kuwait.

**September 5, 1973**
**Bombing:** There was an explosion in the galley of an Air Vietnam B-727 en route to Saigon from Bangkok, Thailand.

**October 2, 1973**
**Hijacking:** A KLM flight was hijacked en route to Amsterdam from Germany.

**October 10, 1973**
**Hijacking:** A Mexican flight from Mexico City to Monterrey Airport, Colombia, was hijacked.

**October 11, 1973**
**Hijacking:** Three hijackers seized a Philippine Air Lines flight after departing from Davao-Mati Airport, in the Philippines.

**October 18, 1973**
**Hijacking:** An Air France flight en route from Paris to Nice, France, by a female hijacker. She demanded a cessation of all air traffic in France for 24 hours.

**October 20, 1973**
**Hijacking:** Four hijackers seized an Aerolineas Argentinas flight from Buenos Aires to Salta Airport. The target was Cuba.

**October 20, 1973**
**Hijacking:** Four hijackers seized an Aerolineas Argentinas flight and diverted it to Bolivia.

**October 31, 1973**
**Hijacking:** An AVENSA flight was hijacked en route to Caracas Airport. The hijacker shot himself and sustained serious injuries.

**November 2, 1973**
**Hijacking:** Four hijackers seized an Aeroflot flight from Briansk to Moscow. Demands were made for money and to be flown to Sweden.

**November 25, 1973**
**Hijacking:** Three hijackers surrendered after seizing a KLM flight in Addis Ababa, Ethiopia.

**December 1, 1973**
**Hijacking:** A Swiss Air flight was hijacked after departing from Genève-Cointrin Airport. The hijacker demanded money for those starving in Africa and a plane ticket to New York.

**December 17, 1973**
**Bombing and hijacking:** Arab terrorists used incendiaries to kill 30 passengers aboard a Pan American airliner at Rome's Leonardo da Vinci Airport. After leaving the plane, the assailants killed a guard, hijacked a Lufthansa jet, and killed a passenger while in Greece.
Source: "FAA History Chronology, 1926–1996."
Source for the 1973 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1974

**January 3, 1974**
**Hijacking:** An Air Jamaica flight from Kingston to Detroit was hijacked. The target was Miami.

**January 21, 1974**
**Hijacking:** An Aeropesca Colombia flight was hijacked en route to Popayan, Colombia.

**February 17, 1974**
**Hijacking:** A soldier flew a stolen Army helicopter to the White House, where guards opened fire with shotguns.
Source: "FAA History Chronology, 1926–1996."

**February 20, 1974**
**Hijacking:** A hijacker detonated explosives on board an Air Vietnam flight from Qui Nhon to Da Nang, Vietnam, once he realized the pilot had tricked him into believing the crew were following his demands.

**February 22, 1974**
**Hijacking:** A Delta Air Lines flight en route to Atlanta from Baltimore was hijacked.

**February 22, 1974**
**Hijacking:** At Baltimore-Washington International Airport, a former mental patient killed two persons and wounded another in an attempt to hijack a DC-9 and crash it into the White House.
Source: "FAA History Chronology, 1926–1996."

**March 3, 1974**
**Hijacking:** A BOAC flight from Beirut to London was hijacked. The two hijackers diverted the plane to Amsterdam and then set the plane on fire after releasing the passengers and crew.

**March 12, 1974**
**Hijacking:** A JAL flight en route to Okinawa from Tokyo was hijacked. There was a demand for money.

**March 20, 1974**
**Hijacking:** Two hijackers seized an East African Airways flight after it departed from Nairobi. The target was Libya.

**March 22, 1974**
**Bombing:** A bomb exploded in the forward landing gear of an Air Inter aircraft while on the ground in Bastia, France.

**March 30, 1974**
**Hijacking:** A National Airlines B-727 was hijacked while on the ground in Sarasota, Florida. A maintenance man was able to disarm the hijacker.

**May 10, 1974**
**Hijacking:** Four hijackers seized an Avianca flight en route to Bogotá. Demands were made for money and to be flown to Cuba.

**July 15, 1974**
**Hijacking:** A JAL flight en route to Tokyo from Osaka was hijacked.

**July 24, 1974**
**Hijacking:** An Avianca flight from Piera to Medellin, Colombia, was hijacked.

**August 5, 1974**
**Bombing:** A bomb exploded on an Air Inter aircraft near Quimper, France.

**September 4, 1974**
**Hijacking:** An Eastern Air Lines flight was hijacked en route to Boston from New York. A demand was made for money.

**September 8, 1974**
**Bombing:** A bomb in exploded in the aft cargo compartment of a Trans World Airlines Boeing 707 bound for Rome and then New York.
Source: "FAA History Chronology, 1926–1996."

**September 10, 1974**
**Hijacking:** TWA Flight 355 from Chicago to New York was hijacked.
Source: Peter St. John, Air Piracy, *Airport Security, and International Terrorism: Winning the War against Hijackers* (Westport, CT: Quorum Books, 1991).

**September 15, 1974**
**Hijacking:** A hijacker with two hand grenades seized an Air Vietnam flight en route to Saigon.

**October 7, 1974**
**Hijacking:** A Far Eastern Air Transport (FEAT) aircraft was hijacked en route to Taipei. The target was China.

**November 6, 1974**
**Hijacking:** Three hijackers seized an Alia Royal Jordanian Airlines flight after it departed from Amman. A demand for political asylum was made.

**November 20, 1974**
**Hijacking:** A Canadian Pacific Air Lines (CPAL) flight was hijacked after departing from Winnipeg Airport, Canada. A demand was made to be flown to Cyprus.

**November 22, 1974**
**Hijacking:** Four hijackers seized a British Airways flight en route to Calcutta, India. A demand was made for the release of prisoners.

**November 23, 1974**
**Hijacking:** An All Nippon Airways flight from Tokyo to Sapporo was hijacked.

**December 1, 1974**
**Hijacking:** A Swissair flight from Bombay (Mumbai), India, to Karachi, Pakistan. The target was the Middle East.

**December 17, 1974**
**Hijacking:** A Lufthansa flight was hijacked after departing from Rome.

**December 25, 1974**
**Hijacking:** An Air India flight from Bombay to Rome was hijacked.
Source for the 1974 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1975

**January 3, 1975**
**Hijacking:** A National Airlines B-727 was hijacked while parked at Pensacola International Airport, Florida.

**January 7, 1965**
**Hijacking:** A British Airways flight was hijacked en route to London from Manchester, England. Money was demanded.

**January 13, 1965**
**Hijacking:** An Eastern Air Lines flight from Atlanta to Philadelphia was hijacked. The target was San Juan, Puerto Rico.

**January 22, 1975**
**Hijacking:** A VASP flight was hijacked en route to Brasilia International Airport. Demands were made for money and release of prisoners.

**February 3, 1975**
**Bombing:** With petrol from a whiskey bottle and a butane refill cartridge, a passenger started several fires in restrooms on board a Pan Am flight en route to India from Bangkok.

**February 22, 1975**
**Hijacking:** A VASP flight was hijacked en route to Brasilia International Airport. A demand was made for money.

**February 23, 1975**
**Hijacking:** A Yemen Airlines flight was hijacked after departing from Hodeida, Yemen.

**February 25, 1975**
**Hijacking:** Two hijackers seized a Philippine Air Lines flight en route to Zamboanga Airport, Philippines.

**March 1, 1975**
**Hijacking:** Three hijackers seized an Iraqi Airways flight from Mosul Airport to Baghdad, Iraq.

**March 2, 1975**
**Hijacking:** An Air New England aircraft was hijacked while on the ground at Hyannis Airport, Massachusetts.

**April 8, 1975**
**Hijacking:** A JAL flight was hijacked en route to Tokyo from Sapporo. A demand was made for money.

**April 25, 1975**
**Hijacking:** A United Air Lines flight from Raleigh, North Carolina, to Newark was hijacked. The target was Cuba.

**May 15, 1975**
**Hijacking:** A United Air Lines flight from Eugene, Oregon, to San Francisco was hijacked.

**June 3, 1975**
**Bombing:** A bomb exploded in the aft lavatory on a Philippines Air Lines flight on its descent into Manila.

**June 28, 1975**
**Hijacking:** A Balkan Bulgarian Airlines flight was hijacked en route to Sofia. The target was Greece.

**July 5, 1975**
**Bombing:** While on the ground in Rawalpindi, Pakistan, a bomb planted under a passenger seat cushion on a PIA B-707 exploded.

**July 28, 1975**
**Hijacking:** An All Nippon flight was hijacked by a 17-year-old male en route to Sapporo from Tokyo. He demanded to be flown to Hawaii.

**August 28, 1975**
**Bombing:** A Fuerza Aérea Argentina flight crashed after takeoff in San Miguel de Tucumán, Argentina, due to the explosion of a bomb.

**September 9, 1975**
**Hijacking:** Three hijackers seized a Haiti Air Inter aircraft after its departure from Port-au-Prince. The target was Cuba.

**September 15, 1975**
**Hijacking:** A hijacker seized a Continental Airlines B-727 while it was parked in San Juan by taking four hostages.

**September 27, 1975**
**Hijacking:** An Olympic Airways flight was hijacked en route to Mikonos, Greece, from Athens.

**October 5, 1975**
**Hijacking:** Leftist guerillas seized an Aerolineas Argentinas flight after its departure from Buenos Aires.

**October 7, 1975**
**Hijacking:** A Philippine Air Lines flight was hijacked en route to Manila. The target was Libya.

**December 29, 1975**
**Bombing:** A high intensity bomb exploded in a coin-operated locker at New York's La Guardia Airport.
Source: "FAA History Chronology, 1926–1996."

Source for the 1975 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 1976

**January 1, 1976**
**Bombing:** An MEA flight, en route to Dubai from Beirut, crashed into the desert after an explosion in the forward baggage compartment.

**January 5, 1976**
**Hijacking:** Two hijackers seized a JAL flight en route to Tokyo from Manila.

**February 29, 1976**
**Hijacking:** An Aerolineas Centrales de Colombia (ACES) flight from Medellín was hijacked . Money was demanded.

**April 7, 1976**
**Hijacking:** Three hijackers seized a Philippine Air Lines flight for seven days after it departed from Cagayan de Oro-Lumbia Airport in the Philippines. Demands were made for money and the release of prisoners.

**April 24, 1976**
**Hijacking:** An Avianca flight was hijacked en route to Bogotá from Pereira, Colombia.

**April 30, 1976**
**Hijacking:** A THY flight was hijacked en route to Istanbul from Paris. The target was Marseille or Lyon.

**May 23, 1976**
**Hijacking:** Six Muslim rebels seized a Philippine Air Lines flight en route to Manila. Demands were made for money and to be flown to Libya.

**June 27, 1976**
**Hijacking:** Members of two political groups, the Baader-Meinhof Group and the PFLP, seized an Air France flight and forced the plane to go to Uganda.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State."

**July 6, 1976**
**Hijacking:** A Libyan Arab Airlines flight was hijacked after departing from Tripoli, Libya.

**August 23, 1976**
**Hijacking:** Three hijackers seized an Egypt-Air plane en route to Luxor from Cairo.

**August 28, 1976**
**Hijacking:** An Air France plane was hijacked while on the ground at Ho Chi Minh City Airport, Vietnam. When authorities came to arrest the

hijacker, he detonated two hand grenades. He was killed during the explosion.

**September 4, 1976**
**Hijacking:** Three hijackers seized a KLM flight destined for Amsterdam. A demand was made for the release of prisoners.

**September 10, 1976**
**Hijacking:** A TWA jetliner en route from New York to Chicago was hijacked by five Croatian nationalists.
Source: "FAA History Chronology, 1926–1996."

**September 10, 1976**
**Hijacking:** Six hijackers seized an Indian Airlines flight from New Delhi en route to Bombay.

**October 6, 1976**
**Bombing:** An explosion in the rear cabin caused a Cubana de Aviacion plane to crash upon takeoff from Barbados.

**October 28, 1976**
**Hijacking:** A CSA flight from the Czech Republic to Slovakia was hijacked. The target was West Germany.

**November 4, 1976**
**Hijacking:** A LOT flight from Denmark to Poland was hijacked. The target was Austria.

**December 21, 1976**
**Hijacking:** A United Air Lines flight was hijacked in San Francisco. The hijacker demanded to be flown to the East Coast.
Source for the 1976 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

### 1977

**January 11, 1977**
**Hijacking: A** TWA B-747 was hijacked en route from New York to London. The target was Uganda.

**February 13, 1977**
**Hijacking:** A THY DC-9 was hijacked en route from Istanbul to Izmir, Turkey. The target was Yugoslavia.

**March 14, 1977**
**Hijacking:** An Iberia flight was hijacked en route from Barcelona to Palma de Mallorca, Spain.

**March 17, 1977**
**Hijacking:** An All Nippon Airways B-727 was hijacked en route to Sendai, Japan, from Chitose.

**March 17, 1977**
**Hijacking:** All Nippon Airways B-727 was hijacked en route from Tokyo to Sendai, Japan.

**March 19, 1977**
**Hijacking:** A THY B-727 was hijacked en route from Diyarbakir to Ankara, Turkey. The target was Beirut.

**April 24, 1977**
**Hijacking:** A LOT (Poland) TU-134 was hijacked en route from Krakow, Poland, to Nuremburg, Federal Republic of Germany (FRG).

**April 25, 1977**
**Hijacking:** An Ethiopian Airlines flight from Mekele to Gondar, Ethiopia, was hijacked.

**May 2, 1977**
**Hijacking:** An Iberia flight was hijacked en route to Rome from Madrid.

**May 8, 1977**
**Hijacking:** A Northwest Airlines B-747 was hijacked en route from Tokyo to Honolulu.

**May 26, 1977**
**Hijacking:** An Aeroflot AN-24 was hijacked en route from Donetsk to Riga, USSR. The target was Sweden.

**June 5, 1977**
**Hijacking:** An MEA (Lebanon) B-707 was hijacked en route from Beirut to Baghdad. The target was Kuwait.

**June 18, 1977**
**Hijacking:** A Balkan Airlines AN-24 was hijacked en route from Vidin to Sofia, Bulgaria. The target was Argentina.

**June 21, 1977**
**Hijacking:** A LAN (Chile) B-727 was hijacked en route from Antofagasta to Santiago, Chile.

**June 28, 1977**
**Hijacking:** A Lufthansa B-727 was hijacked en route from Frankfurt to Istanbul. The target was Munich.

**June 29, 1977**
**Hijacking:** A Gulfair VC-10 was hijacked en route from London to Dubai to Muscat, Oman.

**July 5, 1977**
**Hijacking:** A Ladeco flight from Arica to Santiago, Chile was hijacked. A demand was made for political asylum in Cuba.

**July 8, 1977**
**Hijacking:** A Kuwait Airways B-707 was hijacked en route from Beirut to Kuwait. The target was Syria.

**July 10, 1977**
**Hijacking:** An Aeroflot TU-134 was hijacked en route from Petrozavodsk to Leningrad, USSR. The target was Finland.

**August 12, 1977**
**Hijacking:** An Air France A-300 from Nice, France, to Cairo was hijacked. The target was Libya.

**August 20, 1977**
**Hijacking:** A Western B-707 was hijacked en route from San Diego to Denver.

**September 5, 1977**
**Hijacking:** A Garuda flight from Jogjakarta to Surabaja to East Java, Indonesia, was hijacked.

**September 28, 1977**
**Hijacking:** A Japan Airlines DC-8 was hijacked en route to Tokyo from Bombay.

**September 30, 1977**
**Hijacking:** An Air International flight from Paris to Lyon, France, was hijacked to make a political statement.

**October 11, 1977**
**Hijacking:** A Czechoslovak Airlines YAK-40 was hijacked en route from Karlovy Vary, German Democratic Republic (GDR), to Prague to obtain political asylum in the Federal Republic of Germany (FRG).

**October 13, 1977**
**Hijacking:** A Lufthansa B-737 was hijacked en route from Palma de Mallorca, Spain, to Frankfurt.

**October 18, 1977**
**Hijacking:** A LOT AN-24 was hijacked en route from Katowice to Warsaw. The target was Vienna.

**October 19, 1977**
**Hijacking:** A Lufthansa aircraft was hijacked and its pilot murdered.
Source: "FAA History Chronology, 1926–1996."

**October 20, 1977**
**Hijacking:** A Frontier Airlines B-737 was seized en route from Grand Island, Nebraska, to Lincoln, Nebraska. A demand was made for prisoner release.

**October 28, 1977**
**Hijacking:** An Air Vietnam DC-3 was hijacked en route from Ho Chi Minh City, Vietnam, to Phy Quoc Island, Thailand.

**December 4, 1977**
**Hijacking:** A Malaysian Airlines Boeing 737 en route to Kuala Lumpur from Penang, Malaysia, crashed after being hijacked.
Source: "FAA History Chronology, 1926–1996"; *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

**December 25, 1977**
**Hijacking:** An Eastern Airlines DC-9 was hijacked en route to Indianapolis from Miami. The target was Cuba.
Source for the 1977 section (unless otherwise stated)*: Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1978

**Hijacking Attempts:** There were eight attempts involving U.S.-registered aircraft.
Source: "FAA History Chronology, 1926–1996."

**January 18, 1978**
**Hijacking:** A SAETA flight was hijacked en route from Quito to Guayaquil, Ecuador. The target was Cuba.

**January 20, 1978**
**Hijacking:** A PIA Fok-27 was hijacked en route from Sukkur to Karachi, Pakistan. The target was India.

**January 28, 1978**
**Hijacking:** A Piedmont YS-11 was hijacked en route from Washington, DC, to Wilmington, North Carolina.

**February 6, 1978**
**Hijacking:** A Czechoslovak Airlines TU-134 was hijacked en route from East Berlin to Prague.

**March 2, 1978**
**Hijacking:** A PIA flight from Islamabad to Karachi, Pakistan, was hijacked.

**March 9, 1978**
**Hijacking:** A China Air B-737 was hijacked en route from Kaohsiung, Taiwan, to Hong Kong.

**March 13, 1978**
**Hijacking:** A United Airlines B-727 flight from San Francisco to Seattle was hijacked. The target was Cuba.

**April 1, 1978**
**Hijacking:** A Piedmont flight from Richmond to Norfolk, Virginia was hijacked. The target was New York.

**May 6, 1978**
**Hijacking:** An Aeroflot flight from Ashkhabad to Mineralnyye Vody, USSR.

**May 10, 1978**
**Hijacking:** A Czechoslovak Airlines IL-18 was hijacked en route from Prague to Brno, Czechoslovakia.

**May 11, 1978**
**Hijacking:** An Avianca B-727 was hijacked en route from Santa Marta to Bogota. The target was Aruba.

**May 16, 1978**
**Hijacking:** An Aero Mexico flight to Mexico City was hijacked to make a public statement.

**May 17, 1978**
**Hijacking:** A Czechoslovak Airlines YAK-40 was hijacked en route from Brno to Prague.

**May 29, 1978**
**Hijacking:** A Czechoslovak Airlines YAK-40 was hijacked en route from Brno to Karlovy Vary, Czechoslovakia.

**August 6, 1978**
**Hijacking:** A KLM flight from Amsterdam to Madrid was hijacked. The target was Algiers.

**August 18, 1978**
**Bombing:** There was an explosion in the rear lavatory on board a Philippine Airlines flight en route to Manila from Cebu.

**August 25, 1978**
**Hijacking:** A TWA flight from New York to Geneva, Switzerland, was hijacked. A demand was made for prisoner release in Switzerland.

**August 27, 1978**
**Hijacking:** A United Airlines DC-8 was hijacked en route from Denver to Seattle.

**August 30, 1978**
**Hijacking:** A LOT TU-134 was hijacked en route from Gdansk, Poland, to East Berlin, GDR, for the purpose of gaining political asylum.

**September 7, 1978**
**Bombing:** There was an explosion in the cabin area in an Air Ceylon HS-748 on the ground at Colombo, Sri Lanka.

**September 30, 1978**
**Hijacking:** A FINNAIR flight from Oulu to Helsinki was hijacked.

**October 22, 1978**
**Hijacking:** A TAP B-727 was hijacked en route from Lisbon to Madiera Island, Portugal, to divert the plane to Morocco.

**November, 1978**
**Hijacking:** An Aeroflot flight from Krasnodar, USSR, was hijacked.

**November 23, 1978**
**Hijacking:** A North Central flight was hijacked en route from Madison, Wisconsin, to Milwaukee.

**December 14, 1978**
**Hijacking:** A National Airlines B-727 flight was hijacked en route from New York to Miami. The target was Cuba.

**December 20, 1978**
**Hijacking:** An Indian Airlines B-737 was hijacked en route from Patna to New Delhi, India, to make a political statement.

**December 21, 1978**
**Hijacking:** A TWA DC-9 flight from St. Louis to Kansas City was hijacked. A demand was made for prisoner release.

Source for the 1978 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1979

**January 12, 1979**
**Hijacking:** A Tunis Air B-727 was hijacked en route from Tunis to Diurba Island, Tunisia, for the purpose of obtaining a prisoner release and to gain political asylum.

**January 16, 1979**
**Hijacking:** An MEA flight from Beirut to Amman was hijacked to obtain the return from prison in Jordan of Muslim leader Musa Sadr.

**January 27, 1979**
**Hijacking:** A United Airlines flight from Los Angeles to New York was hijacked to make a political statement.

**February 27, 1979**
**Hijacking:** An Aeroflot TU-154 was hijacked en route from Oslo, Norway, to Stockholm, Sweden, to Moscow, USSR.

**March 16, 1979**
**Hijacking:** A Continental Airlines flight from Los Angeles to Tucson was hijacked. The target was Cuba.

**April 4, 1979**
**Hijacking:** A Pan Am B-747 was hijacked en route from Sydney, Australia, to Auckland, New Zealand. A demand was made for political asylum.

**April 26, 1979**
**Bombing:** There was an explosion in the forward lavatory of an Indian Airlines B-737 flying between Trivandrum and Madras, India.

**June 8, 1979**
**Hijacking:** A Trans Australia flight was hijacked en route to Brisbane from Coolangatta.

**June 11, 1979**
**Hijacking: A** Delta L-1011 flight was hijacked en route from New York to Fort Lauderdale, Florida.

**June 20, 1979**
**Hijacking:** An American Airlines flight from New York to Chicago was hijacked. The target was South America.

**June 30, 1979**
**Hijacking:** An Eastern Air Lines L-1011 aircraft was hijacked en route from San Juan to Miami. The target was Cuba.

**July 9, 1979**
**Hijacking:** A Condo Aerovias Nacional flight from Tulcan to Quito, Ecuador, was hijacked. The target was Costa Rica.

**July 20, 1979**
**Hijacking:** A United Airlines B-727 was hijacked en route from Denver to Omaha, Nebraska. The target was Cuba.

**July 25, 1979**
**Hijacking:** A Biman Bangladesh flight was hijacked en route from Jessore to Dacca, Bangladesh.

**August 5, 1979**
**Hijacking:** An Iberia DC-9 was hijacked while on the ground in the Canary Islands. The plane was seized for the purpose of gaining political asylum in Geneva.

**August 16, 1979**
**Hijacking:** An Eastern Air Lines B-727 was hijacked en route from Guatemala City to Miami. The target was Cuba.

**August 22, 1979**
**Hijacking:** A United Airlines B-727 was hijacked en route from Portland to Los Angeles with an alleged explosive.

**August 24, 1979**
**Hijacking:** A Libyan Arab Airlines B-727 was hijacked en route from Benghazi to Tripoli, Libya, The hijacker wanted to be taken to Cyprus for political asylum.

**September 9, 1979**
**Hijacking:** An Alitalia DC-8 was hijacked en route from Beirut to Rome to obtain the return of Muslim leader Musa Sadr.

**September 12, 1979**
**Hijacking:** A Lufthansa B-727 was hijacked en route from Frankfurt to Cologne, FRG, to make a public statement.

**October 16, 1979**
**Hijacking:** A Libyan Arab Airlines Fok-27 was hijacked en route to Tripoli from Hon, Libya, to be taken to Switzerland for a public statement.

**October 30, 1979**
**Hijacking:** A PSA flight was hijacked en route from Los Angeles to San Diego. The hijacker was fleeing from a death threat.

**November 13, 1979**
**Hijacking:** A Japan Airlines DC-10 was hijacked en route from Osaka to Tokyo. The target was the USSR.

**November 15, 1979**
**Bombing:** A mail bag in the cargo hold exploded on an American Airlines B-727 flight between Chicago and Washington, DC.

**November 24, 1979**
**Hijacking:** An American Airlines B-727 was hijacked en route from San Antonio to El Paso, Texas. The target was Iran.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

### 1980

**January 14, 1980**
**Hijacking:** An Alitalia flight was hijacked en route to Tunis, Tunisia, from Rome for the purpose of obtaining a prisoner release and political asylum. The target was Libya.

**January 18, 1980**
**Hijacking:** An MEA flight from Beirut to Larnaca, Cyprus, was hijacked to obtain the return of Muslim leader Musa Sadr.

**January 25, 1980**
**Hijacking:** A hijacker armed with a pistol and pretending to have a bomb took over a Delta Airlines L-1011 flight to Cuba, and demanded to be flown to Iran.
Source: "FAA History Chronology, 1926–1996."

**January 28, 1980**
**Hijacking:** An MEA flight was hijacked en route to Beirut from Baghdad to obtain the return of Musa Sadr.

**January 30, 1980**
**Hijacking:** An Interflug flight was hijacked en route from Erfurt to Berlin, GDR.

**February 29, 1980**
**Hijacking:** An Empresa Ecuatoriana B-707 was hijacked en route from Guayaquil, Ecuador, to Mexico City.

**March 10, 1980**
**Hijacking:** An MEA flight from Amman to Beirut was hijacked to obtain the return of Musa Sadr.

**March 20, 1980**
**Hijacking:** An Aeroflot TU-134 en route to Yerevan to Baku, USSR, was hijacked. The target was Turkey.

**April 9, 1980**
**Hijacking:** An American Airlines B-727 flight from Ontario, Canada, to Chicago was hijacked. The target was Cuba.

**April 14, 1980**
**Hijacking:** A Continental Airlines B-727 was hijacked en route to Ontario, Canada, from Denver.

**May 1, 1980**
**Hijacking:** A PSA B-727 flight from Stockton to Los Angeles was hijacked. The target was Iran, to make a political statement.

**May 6, 1980**
**Hijacking:** A TAP B-727 was hijacked en route from Lisbon to Faro, Portugal. The target was Madrid, for the purpose of extortion.

**June 30, 1980**
**Hijacking:** An Aerolinas B-737 was hijacked en route to Buenos Aires. The target was Mexico.

**July 11, 1980**
**Hijacking:** A Northwest Airlines B-727 flight from Seattle to Portland was hijacked.

**July 12, 1980**
**Hijacking:** A Philippine Airlines B-727 was hijacked en route to Cebu from Manila. The target was Libya.

**July 22, 1980**
**Hijacking:** A man diverted a Delta Air Lines L-1011 by holding a flight attendant at gunpoint.
Source: "FAA History Chronology, 1926–1996."

**July 24, 1980**
**Hijacking:** A Kuwait Airways B-737 was hijacked en route from Beirut to Kuwait. The target was Dubai.

**August 10, 1980**
**Hijacking:** An Air Florida B-737 was hijacked en route from Miami to Key West with a fake bomb. The target was Cuba.

**August 13, 1980**
**Hijacking:** An Air Florida B-737 was hijacked en route from Key West to Miami with an incendiary device.

**August 14, 1980**
**Hijacking:** A National Airlines DC-10 was hijacked en route from Miami to San Juan. The target was Cuba.

**August 16, 1980**
**Hijacking:** An Eastern Airlines B-727 was hijacked en route from Miami to Orlando. The target was Cuba.

**August 16, 1980**
**Hijacking:** A Republic Airlines DC-9 was hijacked en route from Miami to Orlando. The target was Cuba.

**August 16, 1980**
**Hijacking:** A Delta Airlines flight was hijacked en route from San Juan to Miami. The target was Cuba.

**August 18, 1980**
**Hijacking:** An Eastern Airlines flight was hijacked en route from Melbourne, Florida, to Atlanta. A demand for prisoner release was made. The target was Cuba.

**August 26, 1980**
**Hijacking:** An Eastern Airlines L-1011 bound for Miami from New York was hijacked. The target was Cuba.

**August 29, 1980**
**Hijacking:** A Braniff Airways flight from Lima, Peru, to Los Angeles was hijacked for the purpose of immigration to the United States.

**September 8, 1980**
**Hijacking:** An Eastern Airlines flight was hijacked en route to Tampa from New York. The target was Cuba.

**September 9, 1980**
**Bombing:** There was an explosion in the cargo hold of a United Airlines B-727 while on the ground in Portland, Oregon.

**September 12, 1980**
**Hijacking:** An Eastern Airlines B-727 was hijacked en route from Newark to Miami. The target was Cuba.

**September 13, 1980**
**Hijacking:** A Delta B-727 was hijacked in New Orleans. The target was Cuba.

**September 14, 1980**
**Hijacking:** An Eastern Airlines B-727 was hijacked en route to Miami from Tampa. The target was Cuba.

**September 17, 1980**
**Hijacking:** A Delta Airlines B-727 was hijacked en route from Atlanta to Columbia, South Carolina. The target was Cuba.

**October 13, 1980**
**Hijacking:** A THY B-727 was hijacked en route from Istanbul to Ankara. The objective was Tehran.

**October 25, 1980**
**Hijacking:** A Continental Airlines B-727 was hijacked en route from Miami to Houston. The target was Cuba.

**November 6, 1960**
**Hijacking:** An AVENSA flight from Caracas to Puerto Ordaz, Venezuela, was hijacked. The target was Cuba.

**November 12, 1980**
**Hijacking:** An ARCO flight from Colonia, Uruguay, to Buenos Aires was hijacked. The target was Cuba.

**December 4, 1980**
**Hijacking:** A LOT AN-24 was hijacked en route to Warsaw, Poland, from Zielena Gora, Germany. The target was West Berlin for the purpose of political asylum.

**December 5, 1980**
**Hijacking:** An Aeropostal DC-9 was hijacked en route from Porlamar to Caracas. The target was Higuerote, Venezuela.

**December 15, 1980**
**Hijacking:** An Avianca B-727 was hijacked en route to Pereira from Bogotá, Colombia. The target was Cuba.

Source for the 1980 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1981

**January 10, 1981**
**Hijacking:** A LOT AN-24 was hijacked en route from Katowice to Warsaw. A demand was made for political asylum.

**February 5, 1981**
**Hijacking:** An Eastern Airlines flight from New York to San Juan was hijacked. The target was Cuba.

**February 6, 1981**
**Hijacking:** An Avianca B-727 was hijacked en route from Bucaramanga to Cucuta, Colombia.

**March 2, 1981**
**Hijacking:** A PIA B-720 was hijacked en route to Peshawar, Pakistan, from Karachi for the purpose of obtaining a prisoner release.

**March 5, 1981**
**Hijacking:** A Continental Airlines flight to Phoenix, Arizona from Los Angeles was hijacked.

**March 27, 1981**
**Hijacking:** A SAHSA flight from Tegucigalpa to San Pedro Sula, Honduras, was hijacked. The target was Managua for the purpose of a prisoner release.

**March 28, 1981**
**Hijacking:** A Garuda flight from Palembang to Medan, Indonesia, was hijacked. The target was Malaysia.

**April 10, 1981**
**Hijacking:** An Eastern Airlines A-300 was hijacked en route from New York to Miami. The target was Cuba.

**May 2, 1981**
**Hijacking:** An Aer Lingus B-737 was hijacked en route from Dublin, Ireland, to London. The target was Tehran, for religious objectives.

**May 24, 1981**
**Hijacking:** A THY DC-9 was hijacked en route from Istanbul to Ankara. The target was Burgas, Bulgaria, in order to gain the release of a prisoner.

**July 10, 1981**
**Hijacking:** An Eastern Airlines flight from Chicago to Miami was hijacked. The target was Cuba.

**July 11, 1981**
**Hijacking:** A U.S. jet was hijacked by two men who lit firebombs made of baby bottles aboard the plane.
Source: Not confirmed, but believed to be true.

**July 21, 1981**
**Hijacking:** A LOT AN-24 was hijacked en route from Katowice to Gdansk, Poland. The target was West Berlin, for political reasons.

**August 5, 1981**
**Hijacking:** A LOT T-prop aircraft was hijacked en route from Katowice to Gdansk.

**August 11, 1981**
**Hijacking:** A LOT flight to Gdansk from Katowice was hijacked. The target was West Berlin, for political reasons.

**August 22, 1981**
**Hijacking:** A LOT AN-24 was hijacked en route to Warsaw from Wroclaw, Poland. The objective was West Berlin, for political reasons.

**August 31, 1981**
**Bombing:** There was an explosion on a Middle East Airlines B-720 on the ground in Beirut.

**September 18, 1981**
**Hijacking:** A LOT AN-24 en route to Warsaw from Katowice was hijacked. The target was West Berlin, for political reasons.

**September 22, 1981**
**Hijacking:** A LOT flight to Koszalin, Poland, from Warsaw, Poland, was hijacked. A demand was made for political asylum in West Berlin.

**September 26, 1981**
**Hijacking:** A JAT flight from Titograde with a final destination of Belgrade, Yugoslavia, was hijacked. The target was Israel.

**September 29, 1981**
**Hijacking:** An Indian Airlines B-737 was hijacked en route to Amritsar from New Delhi, India. Demands were made for the release of prisoners in Lahore and for a separate Sikh state.

**September 29, 1981**
**Hijacking:** A LOT AN-24 was hijacked en route from Warsaw to Szczecin, Poland. The target was West Berlin.

**October 5, 1981**
**Hijacking:** A USAirways BAC-111 was hijacked en route from Albany to Buffalo, NY. The target was the USSR.

**October 13, 1981**
**Bombing:** The baggage compartment exploded on an Air Malta B-737 while it was on the ground in Cairo, Egypt.

**October 23, 1981**
**Hijacking:** An American Airlines DC-10 was hijacked en route from San Juan to New York. The target was Quebec.

**October 29, 1981**
**Hijacking:** A SANSA flight was hijacked en route to San José from Quepos, Costa Rica. Demands were made for a prisoner release and a public statement. The target was San Miguel, El Salvador.

**November 26, 1981**
**Hijacking:** An Air India B-707 was hijacked en route to Bombay from Mahe Island, in the Seychelles, in order to escape fighting at Seychelles Airport. The target was Durban, South Africa.

**December 5, 1981**
**Hijacking:** A TWA B-707 was hijacked en route from Cleveland to New York.

**December 7, 1981**
**Hijacking:** An Aeropostal DC-9 was hijacked en route from Caracas to Puerto Ordaz, Venezuela. The target was Cuba.

**December 7, 1981**
**Hijacking:** An Aeropostal DC-9 was hijacked en route from Caracas to Barcelona, Venezuela. The target was Cuba.

**December 7, 1981**
**Hijacking:** An AVENSA B-727 was hijacked after departing from Caracas. The target was Cuba.

**December 7, 1981**
**Hijacking:** A Libyan Arab Airlines flight from Zurich to Tripoli was hijacked. A demand was made for the return of Musa Sadr. The target was Beirut.

**December 12, 1981**
**Bombing:** There was an explosion in the rear cabin area of an Aeronica B-727 while it was on the ground in Mexico City.
Source for the 1981 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1982

**January 7, 1982**
**Hijacking:** An Aerotal B-727 was hijacked en route from Santa Marta to Barranquilla, Colombia. A demand was made for a prisoner release. The target was Aruba.

**January 27, 1982**
**Hijacking:** An Aerotal B-727 was hijacked en route to Pereira from Bogota, Colombia, in order to make a political statement.

**February 2, 1982**
**Hijacking:** An Air Florida B-737 was hijacked en route from Miami to Key West. The target was Cuba.

**February 13, 1982**
**Hijacking:** A Braniff Airways B-727 was hijacked in Amarillo, Texas.

**February 24, 1982**
**Hijacking:** A Kuwait Airways B-707 was hijacked en route from Beirut to Kuwait. A demand was made for the return of Musa Sadr.

**February 26, 1982**
**Hijacking:** A Air Tanzania B-737 was hijacked en route to Kilimanjaro from Mwanza, Tanzania. A demand was made for the resignation of the Tanzanian president.

**March 1, 1982**
**Hijacking:** A United Airlines B-727 was hijacked en route from Chicago to Miami. The target was Cuba.

**April 5, 1982**
**Hijacking:** A Delta Airlines B-727 was hijacked en route from Chicago to Miami. The objective was Cuba.

**April 28, 1982**
**Hijacking:** An ANHSA flight was hijacked en route from La Ceiba to San Pedro Sula, Honduras. A prisoner release was demanded. The target was Cuba.

**April 30, 1982**
**Hijacking:** A LOT AN-24 was hijacked en route to Warsaw from Wroclaw, Poland. A demand was made for political asylum. The target was West Berlin.

**May 10, 1982**
**Hijacking:** An Aeronica flight was hijacked en route to the Corn Islands, Nicaragua. A demand was made for political asylum. The objective was Limon, Costa Rica.

**May 19, 1982**
**Hijacking:** An Aero Del Guaviare aircraft was hijacked. The target was Cuba.

**May 21, 1982**
**Hijacking:** A Philippine Airlines flight from Bacolod to Cebu, in the Philippines, was hijacked. A demand was made for government reform.

**May 27, 1982**
**Hijacking:** A Royal Air Maroc flight departing from Damascus with a final destination of Casablanca, Morocco, was hijacked. A demand was made for government reform. The target was Tunis.

**June 9, 1982**
**Hijacking:** A LOT aircraft was hijacked en route to Warsaw from Katowice. The target was West Berlin.

**June 23, 1982**
**Hijacking:** A Henson DHC-7 in Staunton, Virginia, was hijacked with an alleged gun.

**June 30, 1982**
**Hijacking:** An Alitalia flight from New Delhi, India, to Bangkok, Thailand, was hijacked. The objective was for the hijacker to reunite with his wife and child.

**July 22, 1982**
**Hijacking:** A Marco Island M-404 was hijacked en route from Miami to Key West. The objective was Cuba.

**July 25, 1982**
**Hijacking:** A CAAC IL-18 was hijacked en route to Shanghai from Xian, China. The target was Taiwan.

**August 4, 1982**
**Hijacking:** An Indian Airlines flight from New Delhi to Amritsar, India, was hijacked. A demand was made to speak with Sikh leaders. The target was Lahore.

**August 11, 1982**
**Bombing:** A bomb exploded on board a Pan American 747 traveling from Japan to Hawaii. A similar incident was seen in the April 2, 1986, bomb enclosed in a seat cushion on board a TWA 727.
Source: "FAA History Chronology, 1926–1996."

**August 16, 1982**
**Hijacking:** A Dolphin EMB-110 was hijacked en route from Tampa to West Palm Beach. The objective was Cuba.

**August 20, 1982**
**Hijacking:** An Indian Airlines B-737 was hijacked en route from Jodhpur to New Delhi. A demand was made for political reform. The target was Lahore.

**August 25, 1982**
**Hijacking:** A LOT IL-18 was hijacked en route to Warsaw from Budapest. A demand was made for political asylum. The target was Munich.

**September 25, 1982**
**Hijacking:** An Alitalia B-747 was hijacked en route from Algiers to Rome. The objective was Libya.

**October 14, 1982**
**Hijacking:** A Balkan Airlines TU-134 was hijacked en route to Warsaw from Burgas, Bulgaria.

**October 27, 1982**
**Hijacking:** A TWA flight from Los Angeles to St. Louis, Missouri, was hijacked.

**November 7, 1982**
**Hijacking:** An Aeroflot AN-24 was hijacked en route from Novorossiysk to Odessa, USSR. A demand was made for political asylum. The objective was Turkey.

**November 22, 1982**
**Hijacking:** A LOT AN-24 was hijacked en route from Wroclaw to Warsaw. A demand was made for political asylum. The target was West Berlin.

**November 27, 1982**
**Hijacking:** A MALEV TU-154 was hijacked en route to Budapest from Warsaw. The target was West Berlin.

**December 30, 1982**
**Hijacking:** A United Airlines B-727 was hijacked en route from Chicago to Pittsburgh. The target was Washington, DC.
Source for the 1982 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1983

**January 7, 1983**
**Hijacking:** A Delta Airlines B-727 was hijacked en route from Portland, Maine, to Boston. The target was Las Vegas.

**January 18, 1983**
**Hijacking:** A Thai Airlines flight from Phitsanulok to Chiang Mai, Thailand, was hijacked. Chiang Mai was the target.

**January 20, 1983**
**Hijacking:** A Northwest Airlines flight from Seattle to Portland was hijacked. The target was Afghanistan.

**January 20, 1983**
**Hijacking:** An Alyemda B-707 was hijacked en route to Kuwait from Aden, Yemen. Djibouti was the target.

**February 13, 1983**
**Hijacking:** A Trans-Australia A-300 was hijacked en route from Perth to Melbourne, Australia. The target was Adelaide.

**February 15, 1983**
**Hijacking:** A Rio Airways DHC-7 was hijacked en route from Killeen, Texas, to Dallas by unscreened passengers. The target was Cuba.

**February 18, 1983**
**Hijacking:** A Czechoslovak Airlines TU-134 was hijacked en route to Prague from Poprad, Czechoslovakia.

**February 20, 1983**
**Hijacking:** A Libyan Arab Airlines B-727 was hijacked en route from Sabha to Benghazi. Morocco was the objective.

**March 7, 1983**
**Hijacking:** A Balkan Airlines plane en route to Varna from Sofia, Bulgaria, was hijacked. The target was Turkey.

**April 15, 1983**
**Hijacking:** A THY B-727 was hijacked en route from Istanbul to Izmir, Turkey. Australia was the objective.

**May 5, 1983**
**Hijacking:** A CAAC flight from Shenyang to Shanghai, China, was hijacked. The objective was South Korea.

**May 12, 1983**
**Hijacking:** A Capitol flight from San Juan to Miami was hijacked. The objective was Cuba.

**May 19, 1983**
**Hijacking:** An Eastern Airlines flight was hijacked en route to New York from Miami. The target was Cuba.

**June 14, 1983**
**Hijacking:** An Eastern Airlines A-300 was hijacked en route from Miami to New York. The objective was Cuba.

**June 22, 1983**
**Hijacking:** A Libyan Arab Airlines flight from Athens to Tripoli was hijacked. The target was Iran.

**June 24, 1983**
**Hijacking:** An Aeromexico flight from Mexico City to Miami was hijacked. The target was Cuba.

**July 2, 1983**
**Hijacking:** A Pan Am flight from Miami to Orlando was hijacked. The target was Cuba.

**July 5, 1983**
**Hijacking:** An Aeroflot flight from Moscow to Tallinn, USSR, was hijacked. The target was the United Kingdom or Norway.

**July 6, 1983**
**Hijacking:** An Iran Air flight to Tehran from Shiraz, Iran, was hijacked. A demand was made for a political statement. The target was Iraq.

**July 7, 1983**
**Hijacking:** An Air Florida B-737 was hijacked en route from Fort Lauderdale to Tampa. The objective was Cuba.

**July 17, 1983**
**Hijacking:** Three hijackers seized a Delta Air Lines flight from Miami. The target was Cuba.

**July 19, 1983**
**Hijacking:** An Eastern Airlines L-1011 was hijacked en route from New York to Miami. The objective was Cuba.

**July 21, 1983**
**Hijacking:** A Northwest Airlines B-727 was hijacked en route from Tampa to Miami. The target was Cuba.

**August 2, 1983**
**Hijacking:** A Pam Am flight from Miami to Houston was hijacked. The objective was Cuba.

**August 4, 1983**
**Hijacking:** A Capitol flight from San Juan to Miami was hijacked. The target was Cuba.

**August 18, 1983**
**Hijacking:** A Delta Air Lines flight en route to Tampa from Miami was hijacked. The target was Cuba.

**August 19, 1983**
**Bombing:** There was an explosion under a cabin area seat on a Syrian Arab Airlines B-727 on the ground in Rome.

**August 27, 1983**
**Hijacking:** An Air France flight from Vienna to Paris was hijacked. A prisoner release was demanded. The target was Tehran.

**September 1, 1983**
**Hostile territory:** A Soviet interceptor shot down Korean Airlines flight 007, which unknowingly flew into restricted airspace.
Source: "FAA History Chronology, 1926–1996."

**September 1, 1983**
**Hijacking:** A Mexicana flight from Mexico City to Miami was hijacked. The target was Tel Aviv.

**September 22, 1983**
**Hijacking:** An American Airlines B-727 was hijacked en route from New York to St. Thomas. The objective was Cuba.

**September 23, 1983**
**Bombing:** A Gulf Air B-737 crashed between Karachi and Abu Dhabi due to an explosion in the baggage compartment.

**October 15, 1983**
**Hijacking:** A People's Ex. flight from Buffalo, NY, to Newark was hijacked. The objective was Atlantic City.

**November 18, 1983**
**Hijacking:** An Aeroflot TU-134 was hijacked en route from Tbilisi to Batumi, USSR. Turkey was the objective.

**November 21, 1983**
**Hijacking:** A Republic flight from Detroit to Kalamazoo was hijacked. The target was Chicago.

Source for the 1983 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1984

**January 18, 1984**
**Bombing:** There was an explosion in the cargo hold of an Air France flight between Karachi and Dharan, Saudi Arabia.

**February 3, 1984**
**Hijacking:** A Varig-Cruzeiro flight from San Luis to Belam, Brazil, was hijacked. The target was Cuba.

**February 11, 1984**
**Hijacking:** An American Airlines B-727 was hijacked en route from Port-au-Prince to New York. A demand was made for political asylum. The target was the United States.

**March 7, 1984**
**Hijacking:** An Air France B-737 was hijacked en route from Frankfurt to Paris. Libya was the objective.

**March 10, 1984**
**Bombing:** A Union Des Transport DC-8 was destroyed by an explosion in the baggage compartment while on the ground in Chad.

**March 22, 1984**
**Hijacking:** A British Airways flight from Hong Kong to Beijing, China, was hijacked. The target was Taiwan.

**March 27, 1984**
**Hijacking:** A Piedmont Airlines B-737 from Charlotte, North Carolina, to Charleston was hijacked. Cuba was the target. A prisoner release demand was made.

**March 28, 1984**
**Hijacking:** A Delta Air Lines B-727 from New Orleans to Dallas was hijacked. The objective was Cuba.

**April 5, 1984**
**Hijacking:** A Saudi Arabian Airlines flight from Jiddah, Saudi Arabia, to Damascus was hijacked. The target was Stockholm.

**Summer 1984**
**Hijacking Plot:** During the Summer Olympic Games in Los Angeles, the FBI uncovered a plot to fly a crop-dusting plane into a filled Olympic stadium.
Source: Lt. General Mike Canavan, Retired, Testimony before the National Commission on Terrorist Attacks upon the United States, May 23, 2003.

**June 25, 1984**
**Hijacking:** A CAAC flight from Nanchang to Fuzhou, China, was hijacked. Taiwan was the objective.

**June 26, 1984**
**Hijacking:** An Iran Air B-727 was hijacked en route from Tehran to Bushehr, Iran. A demand was made for political asylum. The target was Baghdad.

**July 5, 1984**
**Hijacking:** An Indian Airlines flight was hijacked en route to New Delhi from Srinagar, India. Demands were made for a prisoner release and money to repair the Sikh temple in Lahore. The target was Lahore.

**July 21, 1984**
**Hijacking:** A MEA B-707 on a flight between Abu Dhabi and Beirut was hijacked.

**July 29, 1984**
**Hijacking:** An Aeropostal DC-9 flight between Caracas and Curaçao, Venezuela, was hijacked.

**July 31, 1984**
**Hijacking:** An Air France B-737 en route to Paris from Frankfurt was hijacked. A prisoner release demand was made. The target was Tehran.

**August 7, 1984**
**Hijacking:** An Iran Air flight originating in Tehran with a final destination of Jiddah, Saudi Arabia, was hijacked. A demand was made for political asylum. The target was Paris.

**August 10, 1984**
**Hijacking:** An Indian Airlines aircraft en route from Mangalore to Bangalore, India, was hijacked.

**August 24, 1984**
**Hijacking:** An Indian Airlines flight between New Delhi and Srinagar, India, was hijacked. A prisoner release demand was made. The target was Dubai.

**August 28, 1984**
**Hijacking:** An Iran Air flight was hijacked en route to Shiraz from Tehran, Iran. A demand was made for political asylum. The target was Kuwait.

**September 8, 1984**
**Hijacking:** An Iran Air flight between Bandar Abbas and Tehran, Iran, was hijacked. A demand was made for political asylum. The target was Abu Dhabi.

**September 12, 1984**
**Hijacking:** an Iran Air A-300 was hijacked en route from Tehran to Shiraz, Iran.

**September 16, 1984**
**Hijacking:** An Iraqi Airways B-737 was hijacked en route from Larnaca, Cyprus, to Baghdad.

**October 2, 1984**
**Hijacking:** An LAC DC-8 on a flight to Bogota from Cartagena, Colombia, was hijacked. The target was Cuba.

**November 5, 1984**
**Hijacking:** A Saudi Arabian Airlines flight from London with a final destination of Riyadh was hijacked. A demand was made for government reform and political asylum. The target was Tehran.

**November 24, 1984**
**Hijacking:** A Somali Airlines B-707 was hijacked en route from Mogadishu, Somalia, to Jiddah, Saudi Arabia. Demand for prisoner release and political asylum. The objective was Addis Ababa.

**November 29, 1984**
**Hijacking:** An Eastern flight from Augusta to Atlanta was hijacked. The demand was to speak with friends.

**December 4, 1984**
**Hijacking:** A Kuwait Air A-310 was hijacked en route to Karachi from Dubai. A prisoner release was demanded. The target was Tehran.

**December 31, 1984**
**Hijacking:** An American Airlines flight from St. Croix to New York was hijacked. The target was Cuba.
Source for the 1984 section (unless otherwise stated)*: Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1985

**January 4, 1985**
**Hijacking:** A Pan Am B-727 was hijacked en route from Cleveland to New York. The target was Brazil.

**January 18, 1985**
**Hijacking:** An Eastern Airlines A-300 was hijacked en route from Newark to Miami. The target was Cuba.

**January 23, 1985**
**Bombing:** There was an explosion in the forward lavatory of a Lloyd Aereo Boliviano B-727 while in flight from La Paz to Santa Cruz, Bolivia.

**February 7, 1985**
**Hijacking:** A Cyprus Air flight to Larnaca, Cyprus, from Beirut was hijacked. A prisoner release was demanded.

**February 23, 1985**
**Hijacking:** An MEA B-707 was hijacked en route from Beirut to Paris. A demand was made for government reform. The target was France.

**February 27, 1985**
**Hijacking:** A Lufthansa B-727 flight from Frankfurt to Damascus was hijacked. A demand was made for political asylum. The target was Vienna.

**March 9, 1985**
**Bombing:** There was an explosion in the baggage compartment of a Royal Jordanian Airlines L-1011 aircraft while it was on the ground in Dubai.

**March 17, 1985**
**Hijacking:** A Saudi Arabian Airlines B-737 flight from Jiddah to Riyadh was hijacked.

**March 27, 1985**
**Hijacking:** A Lufthansa B-727 flight from Munich to Athens was hijacked. The target was Libya.

**March 29, 1985**
**Hijacking:** A Lufthansa B-737 flight between Hamburg and London was hijacked. The target was Hawaii.

**April 1, 1985**
**Hijacking:** An MEA B-707 flight to Jiddah from Beirut was hijacked.

**April 26, 1985**
**Hijacking:** A China Airlines flight was hijacked after departing from Taiwan. The target was Hong Kong.

**May 18, 1985**
**Hijacking:** A Korean Airlines flight from Seoul to Cheju, South Korea, was hijacked. The target was North Korea.

**June 11, 1985**
**Hijacking:** An Alia B-727 on a flight between Beirut and Amman was hijacked. A demand was made for the departure of Palestine guerillas from Beirut. The target was Tunis.

**June 12, 1985**
**Hijacking:** An MEA flight from Beirut to Larnaca was hijacked in retaliation for the June 11 Alia hijacking.

**June 14, 1985**
**Hijacking:** A TWA B-727 flight was hijacked en route from Athens to Rome. The passengers and crew were held for 17 days.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State"; *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

**June 21, 1985**
**Hijacking:** A Braathens S.A.F.E. B-737 en route to Oslo from Trondheim, Norway, was hijacked. A demand was made for government reform.

**June 23, 1985**
**2 Bombings:** An Air India Boeing 747 from Montreal to London crashed in mid-flight over the north Atlantic due to a bomb in the forward cargo hold contained in a suitcase. This at almost the same time as a bombing at the Tokyo Airport involving to luggage handlers.
Source: "FAA History Chronology, 1926–1996"; *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

**June 28, 1985**
**Hijacking:** A THY B-727 was hijacked en route from Frankfurt to Istanbul.

**July 4, 1985**
**Hijacking:** An Air Niuguini flight from Port Moresby, New Guinea, to Brisbane was hijacked. The target was Sydney, Australia.

**August 5, 1985**
**Hijacking:** An Iran Air B-727 flight between Tehran and Bandar Abbas, Iran, was hijacked.

**October 30, 1985**
**Bombing:** An American Airlines B-727's baggage compartment exploded while the aircraft was on the ground in Dallas.

**November 2, 1985**
**Hijacking:** An Iran Air B-707 was hijacked en route to Tehran from Bandar Abbas, Iran.

**November 10, 1985**
**Hijacking:** A Ugandan Airways flight from Kampala to Arwa, Uganda, was hijacked. The target was Kasese.

**November 19, 1985**
**Hijacking:** An America West B-737 was hijacked en route from Phoenix to Ontario, California.

**November 23, 1985**
**Hijacking:** Three men seized control of an Egypt-Air B-737 after takeoff from Athens en route to Cairo. A gunfight on board killed one of the hijackers and many other people.
Source: "FAA History Chronology, 1926–1996."

**November 25, 1985**
**Hijacking:** An Iran Asseman flight en route to Bandar Abbas, Iran, was hijacked. The target was Dubai.

**December 19, 1985**
**Hijacking:** An Aeroflot AN-24 was hijacked en route from Nerchinskiy Zavod to Irkutsk, USSR.

**December 23, 1985**
**Hijacking:** An Iran Air flight from Sirri Island to Shiraz, Iran, was hijacked.

**December 27, 1985**
**Airport Hijacking:** Nearly simultaneous attacks on the airport check-in counters of El Al Airlines in Rome and Vienna resulted in 20 dead, including four hijackers, and 120 injured.
Source: "FAA History Chronology, 1926–1996."

**December 27, 1985**
**Hijacking:** A Saudi Arabian Airlines flight from Karachi to Riyadh was hijacked.
Source for the 1985 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1986

**January 16, 1986**
**Bombing:** A timed device exploded outside an Alyemda Democratic Yemen Airlines office in Abu Dhabi.

**January 23, 1986**
**Bombing:** There was an explosion at a Pakistan International Airlines ticketing office in Peshawar, Pakistan.

**February 2, 1986**
**Shooting:** While a TACA International Airlines aircraft was on the ground in Guatemala, a bullet was fired through the fuselage. A passenger was critically wounded.

**February 5, 1986**
**Hijacking:** A Delta Airlines L-1011 was hijacked in Dallas. The hijacker grabbed a male flight attendant and put a three-inch knife to his throat.

**February 14, 1986**
**Potential Bombing:** A bomb was placed in the mailbox of an Aeroflot office in Brussels, Belgium.

**February 27, 1986**
**Hijacking:** A Trans World Airlines flight from Miami to New York three inch.
Source: Aviation Safety Network Database, http://aviation-safety.net/database.

**March 4, 1986**
**Hijacking:** An Olympic Airways B-737 en route from Athens to Santorini, Italy, was hijacked and the hijackersdemanded to be taken to Libya.
Source: Aviation Safety Network Database, http://aviation-safety.net/database.

**March 11, 1986**
**Hijacking:** Members of the National Liberation Army seized a Compania Aeroexpreso of Bogota helicopter while it was on the ground near Arauca, Colombia.

**March 14, 1986**
**Hijacking:** A Delta Airlines aircraft in Dallas three inch. The hijacker committed suicide.

**March 30, 1986**
**Bombing:** A Palestinian terrorist seized TWA Flight 840 approaching Athens airport.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State"

**April 2, 1986**
**Bombing:** A bomb planted under Seat 10F in a TWA 727 flying from Rome to Athens.
Source: "FAA History Chronology, 1926–1996."

**April 7, 1986**
**Bombing:** A bomb in a backpack exploded in front of a Northwest Airlines office in Stockholm.

**April 9, 1986**
**Bombing:** A car bomb exploded in front of a Sabena Airlines office in Beirut.

**April 10, 1986**
**Bombing:** A bomb exploded at an Air France office in Lisbon.

**April 17, 1986**
**Attempted bombing:** El Al security officials at a checkpoint at Heathrow Airport, London, discovered a suitcase bomb, timed to explode in midflight, carried by an unsuspecting girlfriend of an Arab who was not traveling with her.

**April 24, 1986**
**Bombing:** A bomb, hidden in garbage bags outside the office, exploded near the British Airways Office in London.

**April 25, 1986**
**Attempted bombing:** An explosive device known as an artillery simulator was found on board a Pan Am B-727 on the ground at Istanbul. A U.S. solider had carried the device on to the plane.

**April 25, 1986**
**Attack:** The offices of Saudi Arabian Airlines and Kuwait Airways in Athens were attacked with hand grenades. One of the grenades was taped to the door of the Kuwait Airways office.

**April 28, 1986**
**Hijacking:** A Reno Flying Service Cessna-210 was hijacked after completing a chartered flight to Dunsmuir, California.

**May 1, 1986**
**Attempted bombing:** A Japanese national's luggage was found to contain explosive device components at Schiphol Airport in Amsterdam.

**May 2, 1986**
**Hijacking:** A Horizon Airlines flight from Eugene to Portland, Oregon, was hijacked. The hijacker, who boarded without a ticket, placed a hard object on the back of the pilot's neck to gain control of the plane.

**May 3, 1986**
**Hijacking:** A China Airlines B-747, en route from Bangkok to Hong Kong, was hijacked by the pilot. He demanded political asylum. His target was the People's Republic of China.

**May 3, 1986**
**Bombing:** There was an explosion in the cargo hold of an Air Lanka L-1011 while it was on the ground at Colombo, Sri Lanka.

**May 8, 1986**
**Bombing:** While the plane was boarding, a bomb exploded in the cargo hold of an Air Lanka L-1011 Tri-Star aircraft at Colombo's International Airport, Sri Lanka.

**May 8, 1986**
**Bombing:** A Santorini Airport, Italy, customs inspection revealed that a suitcase, from an Olympic 737 charted by a West German travel agency, contained flares and explosive devices.

**May 13, 1986**
**Bombing:** A British Airways office in Bogota sustained heavy damage during several attacks.

**May 20, 1986**
**Hijacking:** A Finn Air DC-9 was hijacked en route from Oulu to Helsinki, Finland, to make a public statement.

**May 22, 1986**
**Bombing:** A grenade exploded at the entrance of Bangkok's Don Maung International Airport.

**May 23, 1986**
**Hijacking:** A Swiss Air DC-10 on the ground at Chicago's O'Hare Airport was hijacked with the target of Zurich, for the purpose of producing a movie. The hijacker, who was not a ticketed passenger, ran past the gate attendant and used a pocket knife to take a female passenger hostage.

**May 27, 1986**
**Bombing:** Bombs left in bags outside three offices of the official airline of Saudi Arabia. The bombs detonated within 20 minutes of each other.

**May 27, 1986**
**Bombing:** A bomb in front of the Pan Am office in Karachi detonated within the same 20-minute time frame as the bombs at the three Saudi offices mentioned above. There was a Saudi office near the Pan Am office, and it is speculated that the Pan Am office was not the intended target.

**May 30, 1986**
**Attempted bombing:** A conspiracy among members of a Sikh fundamentalist group to blow up a specific aircraft leaving JFK International Airport was revealed due to collaborative efforts involving Canadian authorities and an undercover FBI agent.

**June 7, 1986**
**Hijacking:** An Aeronica B-727 was hijacked en route from Managua to San Salvador.

**June 26, 1986**
**Bombing:** A bomb, timed to explode two hours after takeoff, was discovered as it began to smoke during inspection at the El Al check-in counter in Madrid. The person transporting the suitcase had been told that he was transporting illegal drugs.

**July 4, 1986**
**Bombing:** One of five bombs in downtown Lima exploded at an Aeroperu office.

**July 5, 1986**
**Hijacking:** A Sudan Airways flight from Baghdad to Khartoum, Sudan, was hijacked. The hijacker passed a note to a flight attendant demanding that the plane should go to Israel or he would blow up the plane.

**July 18, 1986**
**Bombing:** An Eastern Air Lines office in downtown Santiago, Chile, sustained structural damage due to a blast.

**July 22, 1986**
**Bombing:** Experts defused a bomb before it exploded at the Aeroflot office in Lima.

**July 22, 1986**
**Bombing:** Dynamite was thrown into an Eastern Air Lines office in Lima during a night attack.

**August 6, 1986**
**Bombing:** There was an explosion in a restroom in the domestic flight wing at Lima International Airport.

**August 6, 1986**
**Bombing:** A bomb, placed under a staircase, exploded between Saudi Arabian Airways and Kuwait Airways offices in New Delhi.

**August 16, 1986**
**Shooting:** A Sudan Airways flight from Malakal to Khartoum, Sudan, was shot down by rebels believed to be part of the Sudanese People's Liberation Army (SPLA).

**August 28, 1986**
**Hijacking:** A LOT Airlines TU-134 was hijacked en route from Wroclaw to Warsaw.

**August 31, 1986**
**Hijacking:** A general aviation aircraft was seized by two men with a history of drug trafficking, in Uchiza, Peru.

**September 3, 1986**
**Attempted hijacking:** Preboarding screening of a male passenger, for an American Airlines flight from Miami to San Juan, revealed two Clorox bottles filled with gasoline.

**September 5, 1986**
**Hijacking:** Four men dressed as security guards hijacked a Pan Am 747 in Karachi.
Source: "FAA History Chronology, 1926–1996."

**September 8, 1986**
**Seizure:** Twelve protestors demonstrating against Iraqi army operations in Kurdistan held 10 people hostage in an Iraqi Airways office in Paris.

**September 14, 1986**
**Bombing:** A bomb was detonated by North Korean agents at Seoul's Kimpo airport.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State."

**September 20, 1986**
**Hijacking:** Two men seized an Aeroflot flight departing from Kiev, USSR, in order to escape police custody.

**September 22, 1986**
**Bombing:** An unclaimed package from Austria, sent to Esenboga Airport in Ankara, contained three hand grenades.

**September 25, 1986**
**Hijacking:** Rebels seized a general aviation aircraft of Gonini Airways in Suriname.

**October 3, 1986**
**Hijacking:** Two Compania Aeroexpreso helicopters were seized and stripped by guerrillas of the National Liberation Army in Arauca, Colombia. The hijackers forced the first helicopter to radio to the second for assistance and then seized and stripped that one too.

**October 18, 1986**
**Hijacking:** In Suriname, a chartered aircraft for tourists was hijacked after landing in Raleigh Falls, a remote vacation site.

**October 26, 1986**
**Bombing:** While an attempt was being made to repackage a smuggled grenade in the lavatory, it accidentally exploded on board a Thai Airways A-300 en route to Osaka.

**October 28, 1986**
**Bombing:** A Lufthansa Airline office was bombed in Cologne, FRG.

**November 1, 1986**
**Bombing:** Action Directe exploded a device in the offices of the Minerve Air Charter Company in Paris. This was in retaliation for the expulsion of Malians and the placement of a number of Algerian opposition figures under house arrest.

**November 5, 1986**
**Hijacking:** A prison escapee hired a pilot and a commercial helicopter to land near the prison in Pleasanton, California. He then seized the helicopter with a pistol, put it down it inside the prison long enough to pick up another inmate, and then flew to a secluded area to abandon the helicopter.

**November 10, 1986**
**Hijacking:** An Iran Air A-300 was hijacked en route from Tehran to Tabriz, Iran.

**November 23, 1986**
**Hijacking:** Two men seized a Red Cross helicopter and picked up two inmates in a prison courtyard near Rome. The pilot then flew to a nearby football field and the hijackers and prisoners escaped.

**December 25, 1986**
**Hijacking:** An Iraqi Airways flight between Baghdad and Amman was hijacked.

**December 26, 1986**
**Attempted bombing:** A suitcase bomb was deactivated after being discovered in the parking lot of Beirut Airport.

**December 31, 1986**
**Shooting:** A man fired his hunting rifle at a United Airlines flight landing in Raleigh, North Carolina.

**December 31, 1986**
**Attempted bombing:** A false-bottomed case containing a highly explosive device was carried by an individual attempting to board a Middle East Airlines flight to West Germany.

Source for the 1986 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1986.

## 1987

**January 5, 1987**
**Hijacking:** A Delta Air Lines aircraft in Dallas was hijacked. The target was Egypt.

**January 10, 1987**
**Hijacking:** A New York Air DC-9 was hijacked en route to Washington, DC. A demand was made to speak with officials.

**March 7, 1987**
**Hijacking:** An Alaska Airlines flight to Anchorage from Seattle was hijacked. The target was Cuba.

**March 10, 1987**
**Hijacking:** A Cubana Airlines flight from Havana to Nueva Gerona, Cuba, was hijacked. The target was the United States.

**May 5, 1987**
**Hijacking:** An Iran Air aircraft was hijacked on a flight from Shiraz to Tehran.

**May 15, 1987**
**Hijacking:** A plane was hijacked in Warsaw. A demand was made for political asylum. The target was West Berlin.

**May 19, 1987**
**Hijacking:** An Air New Zealand B-747 was hijacked at Nadi, Fiji. The target was Libya.

**June 5, 1987**
**Hijacking:** A Virgin Islands seaplane fight from St. Croix to San Juan was hijacked. The target was Cuba.

**July 24, 1987**
**Hijacking:** A Air Afrique DC-10 from Brazzaville, Congo, to Paris was hijacked. A demand was made for a prisoner release. The target was Beirut.

**September 8, 1987**
**Hijacking:** A LOT plane was hijacked en route from Warsaw to Athens.

**November 6, 1987**
**Hijacking:** An Air Canada B-767 was hijacked en route from San Francisco to Toronto. The targets were London and Ireland.

**November 29, 1987**
**Bombing:** North Korean agents planted a bomb on Korean Airlines Flight 858. The plane crashed into the Indian Ocean.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State."

**December 7, 1987**
**Shooting of pilots:** Pacific Southwest Airlines Flight 1771 was deliberately crashed at Paso Robles, California, after a disgruntled former employee shot the pilot and copilot in flight.
Source: "FAA History Chronology, 1926–1996."

**December 23, 1987**
**Hijacking:** A KLM B-737 was hijacked en route from Amsterdam to Milan, Italy. The target was the United States.
Source for the 1987 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1990.

## 1988

**January 4, 1988**
**Hijacking:** An Aeromexico flight co-pilot en route to Mexico City. The target was Brownsville, Texas.

**January 5, 1988**
**Hijacking:** An Iran Air plane was hijacked en route from Tehran to Mashad, Iran.

**February 13, 1988**
**Hijacking:** An Air Tanzania B-737 was hijacked en route from Dar es Salaam to Kilimanjaro, Tanzania. A demand was made for the release from prison of a political figure. The target was London.

**February 22, 1988**
**Hijacking:** A China Airlines B-737 was hijacked en route from Taipei to Kaohsiung, Taiwan.

**March 1, 1988**
**Bombing:** A BOP Air flight suffered an explosion in the cabin area en route between Phalaborwa and Johannesburg, South Africa.

**March 8, 1988**
**Hijacking:** An Aeroflot TU-154 was hijacked en route from Irkutsk to Leningrad, USSR. The target was London.

**March 12, 1988**
**Hijacking:** A Pakistan International Airlines A-300 was hijacked en route from Karachi to Quetta, Pakistan.

**April 5, 1988**
**Hijacking:** A Kuwait Airlines B-747 was hijacked en route from Bangkok to Kuwait. A demand for a prisoner release was made. The intended destination was Mashad, Iran.

**May 12, 1988**
**Hijacking:** A CAAC flight from Xiamen to Guangzhou, China, was hijacked. A demand was made for political asylum. The target was Taiwan.

**May 23, 1988**
**Hijacking:** An Avianca B-727 was hijacked en route from Medellin to Bogotá. The target was Cuba.

**August 1, 1988**
**Hijacking:** An ACES aircraft was robbed on a remote airstrip between El Bagre and Medellin, Colombia.

**September 29, 1988**
**Hijacking:** A flight was hijacked en route to Rio de Janeiro from Belo Horizonte, Brazil.

**October 1, 1988**
**Hijacking:** Three men seized an American Airlines flight from Port-au-Prince, Haiti, to New York. A demand was made for political asylum. The target was the United States.

**October 22, 1988**
**Hijacking:** An Iran Air B-747 flight was hijacked en route from Tehran to Frankfurt.

**November 18, 1988**
**Potential plot:** The FAA issued an information circular concerning the discovery by the West German officials that a cassette recorder contained a barometric device that could detonate at a certain altitude
Source: "FAA History Chronology, 1926–1996."

**December 2, 1988**
**Hijacking:** An Aeroflot flight was hijacked in Mineralnyye Vody, USSR. The target was Israel.

**December 5, 1988**
**Potential plot:** An anonymous phone call warned the U.S. Embassy in Helsinki that a bomb was going to be put on board a Pan Am plane in Frankfurt.
Source: "FAA History Chronology, 1926–1996."

**December 11, 1988**
**Hijacking:** A TWA flight from San Juan to Miami was hijacked. The target was Cuba.

**December 21, 1988**
**Bombing:** Pan Am Flight 103 bound for New York from London Heathrow Airport was blown up over Lockerbie, Scotland, by Libyan terrorists by a bomb contained in a radio-cassette player.
Source: "FAA History Chronology, 1926–1996,"
Source for the 1988 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1990.

## 1989

**January 20, 1989**
**Hijacking:** An Aeroflot flight from Arkhangelsk to Odessa, USSR, was hijacked. The targets were Israel and Bucharest.

**January 21, 1989**
**Hijacking:** An Aeroflot AN-24 from Ivano-Frankovsk to Kiev, USSR.

**January 31, 1989**
**Hijacking:** An ACES flight to Medellin from San Andreas, Colombia, was hijacked. The target was Miami.

**March 29, 1989**
**Hijacking:** A Malev flight from Prague to Frankfurt was hijacked. The target was the United States.

**March 31, 1989**
**Hijacking:** An Aeroflot flight from Astrakhan to Baku, USSR, was hijacked. The target was Pakistan.

**April 10, 1989**
**Hijacking:** Two men seized a Mission Aviation flight from Cap-Haitian, Haiti, to Fort Lauderdale, Florida. A demand was made to speak with the president of Haiti. The target was Miami.

**April 24, 1989**
**Hijacking:** A CAAC flight from Ningbo to Xiamen, China, was hijacked. The target was Taiwan.

**May 18, 1989**
**Hijacking:** An Aeroflot flight from Angola to Tanzania was hijacked.

**May 26, 1989**
**Hijacking:** A CSA YAK-40 aircraft was hijacked en route from Prague to Carlsbad, Czechoslovakia.

**May 27, 1989**
**Hijacking:** An American Airlines flight from Dallas to Miami was hijacked. The target was Cuba.

**May 31, 1989**
**Hijacking:** An ALM Antilles flight from Miami to Haiti was hijacked to Curaçao. The target was Israel.

**August 23, 1989**
**Hijacking:** Air France flight from Paris to Algiers. The target was Tunisia.

**September 19, 1989**
**Bombing:** UTA Flight 772 exploded in midair. The flight was from Brazzaville, Congo, to Paris.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State."

**September 19, 1989**
**Hijacking:** A Royal Air Maroc ATR-42 flight from Casablanca to El Aaiun was hijacked to Asmara, Western Sahara. The mentally unstable hijacker wanted to go to Las Palmas, in the Canary Islands.

**September 19, 1989**
**Bombing:** A Union Des Transport DC-10 was destroyed while flying between Brazzaville, Congo, and N'Djamena, Chad, due to an explosion in the cargo hold.

**October 6, 1989**
**Hijacking:** A Myanmar Airways flight from Mergui to Rangoon, Burma, was hijacked. The target was Bangkok, with the aim of making political demands.

**November 27, 1989**
**Bombing:** An Avianca B-727 aircraft was destroyed in flight due to an explosion in the cabin area. The aircraft was en route from Bogotá to Cali, Columbia.

**December 11, 1989**
**Hijacking:** A Trans World Airlines flight from San Juan to Miami was hijacked.
Source: Aviation Safety Network Database, http://aviation-safety.net/database.

**December 16, 1989**
**Hijacking:** A CAAC B-747 flight from Beijing, Shanghai, and San Francisco to New York was hijacked. A demand was made for political asylum. The target was Fukuoka, Japan.

**December 31, 1989**
**Hijacking:** A Saudi Arabian Airlines B-747 flight from Jeddah to Riyadh was hijacked. The mentally unstable hijacker wanted the plane diverted to Cyprus.
Source for the 1989 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1990.

## 1990

**January 3, 1990**
**Hijacking:** Five men and one woman seized an LATN Cessna-402 flight from Asuncion, Paraguay to Montevideo, Uruguay.

**January 16, 1990**
**Hijacking:** An America West Airlines flight en route to Las Vegas was hijacked. The hijacker claimed to have an explosive device, which was only a flashlight with a toothpaste container attached. The target was Cuba.

**January 18, 1990**
**Hijacking:** A United Airlines flight from San Francisco to Seattle was hijacked. The target was Vancouver, Canada. The hijacker claimed his cell phone was an explosive device.

**January 18, 1990**
**Bombing:** Car bombs, located in parking lots in both Peshawar and Islamabad international airports, detonated several hours apart.

**January 26, 1990**
**Hijacking:** Four armed passengers seized an Iran Air B-727 flight from Shiraz to Bandar Abbas, Iran.

**March 22, 1990**
**Assassination:** A machine gun attack at El Dorado Airport in Bogotá took the life of Colombian presidential candidate Bernardo Jaramillo.

**April 2, 1990**
**Hijacking:** An American Airlines flight from Port-au-Prince, Haiti, to New York was taken over on the ground in Haiti. A demand was made for political asylum. The target was the United States.

**April 18, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Moscow to Leningrad, USSR, was hijacked. The hijacker claimed to have biological weapons wrapped in cellophane.

**April 26, 1990**
**Assassination:** On an Avianca flight en route to Barranquilla from Bogotá, a lone gunman killed Colombian presidential candidate Carlos Pizarro Leongomez.

**April 29, 1990**
**Explosives seized:** A teenager wore a maternity smock to hide explosive devices and a detonator strapped to her waist. She was on a bus headed toward Belfast International Airport.

**May 5, 1990**
**Hijacking:** En route from Baardheere to Mogadishu, Somalia, a Rockwell Turbo-Commander aircraft was seized by a man with a pistol. The plane landed in Dolo, Ethiopia.

**May 21, 1990**
**Bombing:** The El Al ticket office in Istanbul sustained minor damage from an improvised explosive device (IED) that detonated on the sidewalk near the building.

**May 29, 1990**
**Hijacking:** The pilot and flight engineer of a military AN-26 flight from Mogadishu to Hargessa, Somalia, sought political asylum.

**June 7, 1990**
**Bombing:** Within a span of 45 minutes, three IEDs detonated in Gdansk, Poland. One of the targets was the Polish Airlines ticket office.

**June 8, 1990**
**Hijacking:** An Aeroflot TU-154 flight was hijacked en route from Minsk to Murmansk, USSR, by a 17-year-old who claimed to have a hand grenade. His destination objective was Sweden.

**June 19, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Riga to Murmansk, USSR, was hijacked. The hijacker demanded to be taken to Helsinki to obtain political asylum.

**June 24, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Tallinn to Lvov, USSR, was hijacked. The target was Finland.

**June 28, 1990**
**Hijacking:** An Aeroflot TU-154 flight from Krasnodar to Krasnoyarsk, USSR, was hijacked by a male hijacker with a plan to divert the plane to Turkey to claim political asylum. He claimed to have chemicals to poison everyone on board.

**June 30, 1990**
**Hijacking:** An Aeroflot TU-154 flight from Lvov to Leningrad, USSR, was hijacked. The objective was Sweden.

**June 30, 1990**
**Bombing:** An Iberia Airlines office in Amsterdam sustained considerable damage after an IED detonated in front of the building.

**July 3, 1990**
**Hijacking:** Two armed men took the pilot of a turboprop aircraft hostage in a mining area in Brazil's Para State.

**July 4, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Sochi to Rostov, USSR, was hijacked by a female hijacker with a plan to divert the plane to Turkey. Her 2-year-old daughter was also on the flight.

**July 5, 1990**
**Hijacking:** An Aeroflot TU-154 flight from Leningrad to Lvov, USSR, was hijacked. The objective was Sweden.

**July 5, 1990**
**Hijacking:** Five passengers seized an Aeroperlas flight from Colon to Panama City. The target was Colombia.

**July 10, 1990**
**Hijacking:** An Aeroflot flight from Leningrad to Murmansk, USSR, was hijacked. The target was France.

**July 12, 1990**
**Hijacking:** Two teenagers attempted to seize an Aeroflot flight from Leningrad to Murmansk, USSR. The target was Sweden.

**July 15, 1990**
**Bombing:** A dynamite charge detonated underneath a car in the long-term parking area at Jorge Chavez International Airport in Lima.

**July 18, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Odessa to Sukhumi, USSR, was hijacked. The objective was Turkey.

**July 23, 1990**
**Hijacking:** Two hijackers seized an Aeroflot TU-134 aircraft en route from Riga to Murmansk, USSR. The target was Sweden.

**July 28, 1990**
**Bombing:** A landing beacon was destroyed by masked men several kilometers from the Jorge Chavez International Airport in Lima.

**August 14, 1990**
**Shooting at airport:** A former Ogden Allied Services employee seized a fuel truck and then opened fire on another fuel truck at National Airport in Washington, DC. He then attempted to commander an airport shuttle bus.

**August 16, 1990**
**Hijacking:** A privately owned Beechcraft-200 was seized by several heavily armed men. The aircraft was on the ground at France Field in Colon, Panama.

**August 16, 1990**
**Hijacking:** An Ethiopian Airlines flight was hijacked during a domestic flight. The target was Yemen.

**August 19, 1990**
**Hijacking:** An Aeroflot TU-154 was seized by a group of prisoners aboard a flight from Neryungri to Yakutsk, USSR.

**August 20, 1990**
**Hijacking:** An American Airlines flight on the ground at Charleston, South Carolina, was hijacked by a man who stole a knife from the food area and ran into the sterile area via the passenger exit lane. He held the pilot at the counter at knife point and forced him to the jet way door before being apprehended.

**August 30, 1990**
**Hijacking:** A man entered the cockpit of an Aeroflot AN-2 flight from Voronezh, USSR, with a knife. The target was Afghanistan.

**August 30, 1990**
**Hijacking:** An Aeroflot YAK-42 flight en route from Moscow to Voronezh, USSR, was hijacked.

**September 2, 1990**
**Hijacking:** An Aeroflot flight from Przhevalsk to Frunze, USSR, was hijacked. The target was South Africa.

**September 13, 1990**
**Hijacking:** An India Airlines flight from Coimbatore to Madras, India, was hijacked. The hijacker forced himself into the cockpit, claiming to have a hand grenade.

**September 25, 1990**
**Hijacking:** An Aeroflot flight from Leningrad to Archangelsk, USSR, was hijacked. The target was Sweden.

**October 2, 1990**
**Hijacking:** A Xiamen Airlines B-737 flight en route to Guangzhou, China, was hijacked. During the landing, the pilot lost control and struck a B-757 aircraft waiting for departure.

**October 3, 1990**
**Attempted bombing:** A known gangster, apprehended at the Okinawa Airport on unrelated charges, was found to have an IED intended for an All Nippon Airways flight from Naha, Okinawa, to Tokyo.

**October 5, 1990**
**Hijacking:** An Aeroflot flight from Novgorod to Petroskoi, USSR, was hijacked. The target was Finland.

**October 5, 1990**
**Hijacking:** Two Aerotaxi Airlines on domestic flights en route to Puerto Ayacucho, Venezuela, were hijacked.

**October 7, 1990**
**Hijacking:** An Aeroflot AN-24 flight from Perm to Archangelsk, USSR, was hijacked. The target was Sweden.

**November 10, 1990**
**Hijacking:** Two Burmese students seized a Thai International Airways A-320 flight from Rangoon, Burma, to Bangkok.

**November 12, 1990**
**Hijacking:** An Aeroflot TU-154 flight from Leningrad to Lvov, USSR, was hijacked. The objective was Sweden.

**November 15, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Leningrad to Moscow was hijacked. The target was Finland.

**November 16, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Tallinn to Moscow was hijacked. The objective was Sweden.

**November 29, 1990**
**Hijacking:** An Aeroflot TU-134 flight from Moscow to Syktyvkar, USSR, was hijacked. The target was Iraq.

**November 29, 1990**
**Attempted bombing:** An IED was found on the roof above the preboarding lounge at the Warsaw airport.

**December 2, 1990**
**Hijacking:** An Aeroflot TU-154 flight from Murmansk to Leningrad was hijacked.

**December 6, 1990**
**Hijacking:** A CAAC flight from Guangzhou to Quingdao, China, was hijacked.

**December 11, 1990**
**Hijacking:** An Aeroflot YAK-40 flight from Baku to Tbilisi, USSR, was hijacked. The target was Turkey.

**December 15, 1990**
**Airport attack:** An Aires Airline 19-seat airliner was set on fire after landing during an attack on the Villagarzon Airport in Mocoa, Colombia.

**December 21, 1990**
**Hijacking:** A female stowaway hijacked an Aeroflot TU-154 flight from Rostov to Nizhnevartovsk, USSR.

**December 24, 1990**
**Hijacking:** An Aeroflot IL-86 flight from Moscow to Sochi, USSR, was hijacked. The target was England.

**December 28, 1990**
**Hijacking:** Two hijackers seized an Air Algerie B-737 flight from Ghardaia to Algiers.

Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1990.

## 1991

**January 7, 1991**
**Hijacking:** A Faucett flight en route to Lima from Trujillo, Peru, was hijacked.

**January 21, 1991**
**Hijacking:** An Aeroflot TU-154 flight from Tashkent, Uzbekistan, to Odessa, Ukraine, was hijacked. The target was Turkey.

**February 10, 1991**
**Hijacking:** A Southwest Airlines flight from Oakland, California, to Austin, Texas, was hijacked . The target was Cuba.

**February 13, 1991**
**Hijacking:** An Aeroflot flight from Tbilisi to Moscow was hijacked. The objective was Turkey.

**March 4, 1991**
**Hijacking:** An Aeroflot Anotnov-24 was hijacked en route to Leningrad from Arkhangelsk, Russia. The target was Sweden.

**March 6, 1991**
**Hijacking:** A TABA flight en route to Manaus, Brazil, was hijacked.

**March 14, 1991**
**Hijacking:** An Aeroflot Yakovlev-42 flight from Moscow to Naberezhnye, Russia, was hijacked.

**March 26, 1991**
**Hijacking:** A Singapore Airlines flight from Kuala Lumpur, Malaysia, to Singapore was hijacked. The objective was Australia.

**March 28, 1991**
**Hijacking:** An Aeroflot flight from Arkhangelsk to Kaliningrad, USSR, was hijacked. The target was Sweden.

**March 31, 1991**
**Hijacking:** An Air Algerie B-737 was hijacked en route from Bechar to Algiers for political reasons.

**April 29, 1991**
**Hijacking:** An Aeroflot TU-154 was hijacked en route from Barnaul, Russia, to Moscow. The target was the United States.

**June 13, 1991**
**Hijacking:** An Aeroflot TU-154 was hijacked en route from Rostov, USSR, to Moscow. The target was the Persian Gulf.

**June 17, 1991**
**Hijacking:** An Aeroflot TU-154 flight from Krasnodar to Krasnoyarsk, Russia, was hijacked. The target was Turkey.

**June 30, 1991**
**Hijacking:** A Somali Airlines flight from Djibouti to Mogadishu was hijacked.

**August 20, 1991**
**Hijacking:** A San Martin Airlines aircraft was hijacked en route from Caquetá to Meta, Colombia.

**September 7, 1991**
**Hijacking:** A Cessna Caravan 208 of the Colombian SATENA (National Territory Air Service) was hijacked en route from Bogota to San José de Guaviare.

**September 19, 1991**
**Hijacking:** An Alitalia DC-9 was hijacked en route from Rome to Tunis. The objective was Algeria.

**October 11, 1991**
**Hijacking:** A Bolivian Air Force flight from Rurrenabaque, Bolivia, to Trinidad was hijacked.

**October 16, 1991**
**Hijacking:** An Ethiopian Airlines flight from Debre Markos to Bahir Dar, Ethiopia, was hijacked.

**October 21, 1991**
**Hijacking:** A Czechoslovak Airlines flight from Bratislava to Prague was hijacked. The target was Libya.

**October 27, 1991**
**Hijacking:** A Beechcraft aircraft was hijacked en route from Trujillo to Tocache, Peru.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1991.

**October 27, 1991**
**Hijacking:** An Aero Commander 6–90 twin turboprop was hijacked en route from Guayaquil to Lago Agrio, Equador.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1991.

**November 1991**
**Hijacking plot foiled:** An Islamic fundamentalist group planned to hijack two airplanes outside Spain and fly them into Madrid, where Middle East peace talks were being held. One aircraft was to crash into the Spanish royal palace, killing President Bush, Mikhail Gorbachev, and other world leaders. The second plane was intended to crash into a hotel where the Soviet delegation to the conference was staying.
Source: *Times Online*, September 14, 2001, www.timesonline.co.uk.

**November 9, 1991**
**Hijacking:** An Aeroflot TU-154 on a flight from Mineralnyye Vody to Ekaterinburg, USSR, was hijacked. The target was Turkey.

**November 13, 1991**
**Hijacking:** An Aeroflot TU-154 was hijacked en route from Irkutsk to St. Petersburg, Russia. The objective was Great Britain.

**November 23, 1991**
**Hijacking:** A Girasol Company twin-engine aircraft was hijacked as it was departing from Tefe, Brazil.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1991.

**November 25, 1991**
**Hijacking:** An Ethiopian Airlines B-737 was hijacked en route from Addis Ababa to Dire Dawa, Ethiopia.

**November 25, 1991**
**Hijacking:** A flight in Papua New Guinea in order to steal cargo.

## 1992

**January 3, 1992**
**Theft:** A helicopter in Cuba was stolen. The target was the United States.

**January 17, 1992**
**Commandeering:** An Aeronica aircraft was taken over while the plane was on the ground in Nicaragua.

**January 24, 1992**
**Attack:** An Air Algerie office in Germany was attacked.

**January 28, 1992**
**Shooting:** An aircraft was shot in Azerbaijan.

**January 31, 1992**
**Hijacking:** An Aerotaxi Cessna Grand Caravan was hijacked en route from Panama City to El Porvenir, Panama.

**February 5, 1992**
**Hijacking:** An Ethiopian Airlines DHC-6 aircraft was hijacked between Addis Ababa and Bahir Dar, Ethiopia.

**March 12, 1992**
**Hijacking:** An Aerotaxi flight from El Porvenir to Panama City, Panama, was hijacked.

**April 1, 1992**
**Hijacking:** An Ethiopian Airlines 727 was hijacked en route from Dire Dawa to Addis Ababa, Ethiopia.

**April 9, 1992**
**Hijacking:** A Cessna 172 aircraft was hijacked during a charter flight from Pine Bluff to Little Rock, Arkansas.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1992.

**April 12, 1992**
**Hijacking:** An Ethiopian Airlines 727 from Addis Ababa was hijacked. The objective was Kenya.

**May 16, 1992**
**Hijacking:** An Aerotaca flight to Bucaramanga, Colombia, from Bogota was hijacked.

**May 29, 1992**
**Hijacking:** An Aeroexpreso helicopter was hijacked between Bogota and Yopal, Colombia.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1992.

**June 7, 1992**
**Hijacking:** An aircraft in Colorado was hijacked.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1992.

**June 7, 1992**
**Hijacking:** An Aeroflot–Russian International Airlines Tupolev-154 was hijacked en route from Grozny to Moscow.

**July 26, 1992**
**Hijacking:** A Corsica helicopter flying between Corsica and Sardinia was hijacked.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1992.

**August 13, 1992**
**Hijacking:** A Lvov Air Transport Enterprises TU-154 was hijacked en route from Simferopol to Lvov, Ukraine.

**August 28, 1992**
**Hijacking:** An Ethiopian Airlines 727 was hijacked en route from Addis Ababa to Bahir Dar, Ethiopia.

**September 4, 1992**
**Hijacking:** A Vietnam Airlines A-310 was hijacked between Bangkok and Ho Chi Minh City.

**September 4, 1992**
**Hijacking:** An Ethiopian Airlines Flight 727 from Dire Dawa to Addis Ababa was hijacked.

**December 29, 1992**
**Hijacking:** An AeroCaribbean flight from Havana to Varadero Beach, Cuba, was hijacked.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1996.

## 1993

**January 22, 1993**
**Hijacking:** An Indian Airlines flight en route to New Delhi was hijacked.

**February 11, 1993**
**Hijacking:** A Lufthansa flight from Frankfurt to Addis Ababa was hijacked.

**February 20, 1993**
**Hijacking:** An Aeroflot TU-134 was hijacked en route from to St. Petersburg, Russia.

**March 12, 1993**
**Hijacking:** An Ethiopian Airlines ATR-42 was hijacked en route from Gambela to Addis Ababa.

**March 27, 1993**
**Hijacking:** An Indian Airlines A320 was hijacked en route from New Delhi to Madras.

**April 6, 1993**
**Hijacking:** A China Southern Airlines 757 was hijacked en route from Shenzhen to Beijing.

**April 10, 1993**
**Hijacking:** An Indian Airlines 737 from Lucknow to New Delhi was hijacked.

**April 18, 1993**
**Hijacking:** An Intercontinental de Aviacion DC-9 from Arauca to Bogotá was hijacked.

**April 24, 1993**
**Hijacking:** An Indian Airlines 737 from Srinagar to New Delhi was hijacked.

**June 24, 1993**
**Hijacking:** A Xiamen Airlines B-737 from Changzhou to Xiamen was hijacked.

**July 4, 1993**
**Hijacking:** A Royal Swazi National Airways Fokker F-28 from Maputo, Mozambique, to Manzini, Swaziland, was hijacked.

**July 25, 1993**
**Hijacking:** An Ethiopian Airlines 757 was hijacked en route from Dire Dawa to Addis Ababa.

**August 10, 1993**
**Hijacking:** An Air China 767 was hijacked en route from Beijing to Jakarta.

**August 14, 1993**
**Hijacking:** An Aeroflot TU-154 was hijacked en route to Moscow from St. Petersburg.

**August 15, 1993**
**Hijacking:** A Royal Dutch Airlines (KLM) 737 was hijacked en route from Tunis to Amsterdam.

**August 27, 1993**
**Hijacking:** An Alyemda Airlines B-737 was hijacked en route from Ar-Riyan to Al-Ghaydah, Yemen.

**September 15, 1993**
**Hijacking:** An Aeroflot TU-134 was hijacked en route from Baku, Azerbaijan, to Perm, Russia.

**September 30, 1993**
**Hijacking:** A Sichuan Airlines TU-154 was hijacked en route from Jinan to Guangzhou, China.

**October 22, 1993**
**Hijacking:** Am Egypt-Air flight from Cairo to Sanaa, Yemen, was hijacked.

**October 25, 1993**
**Hijacking:** A Nigerian Airways Airbus A310 was hijacked en route from Lagos to Abuja, Nigeria.

**November 5, 1993**
**Hijacking:** A Xiamen Airlines B-737 was hijacked en route from Guangzhou to Xiamen.

**November 8, 1993**
**Hijacking:** A Zheijang Airlines Airbus A300 was hijacked en route from Hanzhou to Fuzhou, China.

**November 12, 1993**
**Hijacking:** A China Northern Airlines MD-82 was hijacked en route from Changchun to Fuzhou, China.

**November 27, 1993**
**Hijacking:** A China Eastern Airlines Fokker F-100 was hijacked en route from Nanjing to Fuzhou, China.

**November 29, 1993**
**Hijacking:** An Iran Air Fokker F-27 was hijacked en route from Gachsaran to Ahvaz, Iran.

**December 8, 1993**
**Hijacking:** A China Northern Airlines MD-82 was hijacked en route from Qingdao to Fuzhou.

**December 10, 1993**
**Hijacking:** An Air France Airbus A320 was hijacked near Nice, France.

**December 12, 1993**
**Hijacking:** A Xiamen Airlines 737 was hijacked en route from Harbin to Xiamen, China.

**December 28, 1993**
**Hijacking:** A Fujian Airlines YUN-7 was hijacked en route from Ganzhou to Xiamen.

**December 28, 1993**
**Hijacking:** An Air China flight from Beijing to New York was hijacked.

**December 28, 1993**
**Hijacking:** A Xiamen Airlines B-727 flight from Ningbo to Xiamen was hijacked.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1996.

## 1994

**January 13, 1994**
**Hijacking:** An Indian Airlines flight from Madras to Calcutta, India, was hijacked.

**January 23, 1994**
**Hijacking:** An Ethiopian Airlines 757 was hijacked en route from Dakar, Senegal, to Bamako, Mali.

**January 29, 1994**
**Hijacking:** China East Airlines Flight 5513 from Shanghai to Hanzhou was hijacked.

**February 9, 1994**
**Hijacking:** An Ethiopian Airlines B-737 was hijacked en route from Bahir Dar to Addis Ababa.

**February 18, 1994**
**Hijacking:** A Chinese Southwest Airlines 737 was hijacked en route from Changsha to Fuzhou.

**February 28, 1994**
**Hijacking:** An Air Algerie flight from Oran to Annaba, Algeria, was hijacked.

**March 8, 1994**
**Hijacking:** A Saudi Arabian Airlines A300 was hijacked en route from Jeddah to Addis Ababa.

**March 21, 1994**
**Hijacking:** A Meridiana DC-9 was hijacked en route from Palermo to Rome.

**April 6, 1994**
**Hijacking:** A Sudan Airways 737 was hijacked en route from Khartoum to Dongola, Sudan.

**April 7, 1994**
**Hijacking and attempted murder of pilots and deliberate crashing of plane into building:** A Federal Express flight was commandeered by an off-duty pilot who fractured the skulls of the pilots and planned to crash into the Federal Express hub at the Memphis, Tennessee, airport. The pilots fought with the hijackers and saved the plane.
Source: Many media reports and extensive media coverage.

**April 25, 1994**
**Hijacking:** An Ethiopian Airlines 757 was hijacked en route from Jeddah to Addis Ababa.

**May 26, 1994**
**Hijacking:** A Garuda Airlines flight from Indonesia to Australia was hijacked.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1994.

**June 7, 1994**
**Hijacking:** A China Southern Airlines 737 was hijacked en route from Fuzhou to Guangzhou.

**June 23, 1994**
**Hijacking:** An Ethiopian Airlines ATR-42 was hijacked en route from Gondar to Addis Ababa.

**July 17, 1994**
**Bombing:** An Alas Chiricanas Airlines EMB-110 exploded due to a bomb in the cabin area while en route from Colon City to Panama City.

**August 7, 1994**
**Hijacking:** A COPA 737 was hijacked en route from Panama City to Guatemala City.

**August 29, 1994**
**Hijacking:** A LATN airliner was hijacked en route from Pedro Juan Caballero to Asuncion, Paraguay.

**September 11, 1994**
**Crash into White House:** a Cessna P150 from Maryland flew through Washington's protected no-fly airspace and crashed into the White House.
Source: White House Security Review, May 1995, http://www.prop1.org/park/pave/rev6.htm.

**September 14, 1994**
**Hijacking:** An Alyemda Airlines 737 was hijacked en route from Aden to Sanaa, Yemen.

**October 22, 1994**
**Hijacking:** A LATN aircraft was hijacked en route from Itaituba to Belem, Brazil.

**October 25, 1994**
**Hijacking:** A Rostov Aviation Enterprises Yak-40 was hijacked en route from Ashgabad, Turkmenistan, to Rostov, Russia.

**November 3, 1994**
**Hijacking:** A Scandinavian Airlines System (SAS) MD-80 was hijacked en route from Bardafoss to Oslo, Norway.

**November 13, 1994**
**Hijacking:** An Air Algerie F-27 was hijacked en route from Algiers to Ouargla, Algeria.

**November 24, 1994**
**Hijacking:** A Komiavia TU-134 was hijacked en route from Syktyvkar, Russia, to Minsk, Belarus.

**December 5, 1994**
**Hijacking:** A Puntavia LET-410 was hijacked en route from Berbera, Somalia, to Djibouti.

**December 11, 1994**
**Bombing:** A bomb exploded in the cabin area of a Philippine Airlines 727 en route from Manila.

**December 15, 1994**
**Hijacking:** A TABA EMB 100 was hijacked between Carauari and Manaus, Brazil.

**December 23, 1994**
**Hijacking:** A Tongyong Airlines YAK-42 was hijacked en route from Xiamen to Nanjing.

**December 24, 1994**
**Hijacking:** An Air France flight hijacked in Algiers.
Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State"
Source for the 1994 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1996.

## 1995

**January 4, 1995**
**Hijacking:** A Sudan Airways Fokker was hijacked en route from Khartoum to Merowe, Sudan.

**March 17, 1995**
**Hijacking:** An Ethiopian Airlines 737 was hijacked en route from Addis Ababa to Bahr Dar, Ethiopia.

**April 10, 1995**
**Hijacking plot foiled:** This was a plan to fly a plane into the CIA headquarters, board any American commercial aircraft pretending to be an ordinary passenger, then hijack the aircraft, control its cockpit, and dive it at the CIA headquarters. No bomb or explosive was to be used. It was to be simply a suicide mission.
Source: FBI Documents; Congressional Testimony. September 18, 2002.

**June 21, 1995**
**Hijacking:** Ann All Nippon Airways 747 was hijacked en route from Tokyo to Hokkaido, Japan.

**July 1, 1995**
**Hijacking:** A Domodedovo Airlines IL-62 was hijacked en route from Yakutsk to Moscow.

**July 30, 1995**
**Hijacking:** A La Costena Airline commuter plane was hijacked en route from Managua to Bluefields, Nicaragua.
Source: Unconfirmed, but believed to be true.

**August 3, 1995**
**Hijacking:** A China Eastern Airlines Airbus 300 was hijacked en route from Shanghai to Guangzhou.

**August 15, 1995**
**Hijacking:** A Phoenix Airways B727 was hijacked en route from Cape Town to Johannesburg, South Africa.

**August 15, 1995**
**Terrorist attack threat:** The threat of a terrorist attack by Middle Eastern militants—possibly a "suicide massacre"—threatened New York's three major airports.

Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1996.

**August 15, 1995**
**Hijacking: A** Britten-Norman Islander aircraft was hijacked en route from Jackson's Airport in Port Moresby to Asimba, Oro Province, Papua New Guinea.
Source: Unconfirmed, but believed to be true.

**August 15, 1995**
**Hijacking:** A Phoenix Airways flight was hijacked en route from Cape Town to Johannesburg.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

**September 3, 1995**
**Hijacking:** An Air Inter flight from Palma de Mallorca, Spain, to Paris was hijacked.

**September 19, 1995**
**Hijacking:** An Iranian flight was hijacked by a flight steward.
Source: Aviation Safety Network Database: http://aviation-safety.net/database.

**November 9, 1995**
**Hijacking:** An Olympic Airways 747 was hijacked en route from Bangkok to Athens.

**December 8, 1995**
**Hijacking threat:** An Islamic group threatened to hijack Pakistani aircraft and attack Pakistani airports if the Pakistani government did not stop its campaign against al Qaeda.
Source: Unconfirmed, but believed to be true.

**December 15, 1995**
**Hijacking:** A Saudi Arabian Airlines flight from Jeddah to Addis Ababa was hijacked.
Source: Unconfirmed but believed to be true.

**December 26, 1995**
**Hijacking:** A Saudi Arabian Airlines flight from Jeddah, to Addis Ababa was hijacked.
Source for the 1995 section (unless otherwise stated): *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1996.

## 1996

**January 6, 1996**
**Hijacking:** A Transasia Airways Airbus 321 was hijacked en route from Taipei to Tainan, Taiwan. The hijacker claimed to have a bomb and threatened to blow up the plane.

**January 19, 1996**
**Bombing:** In Nigeria, in a Kano Airport departure lounge restroom, an explosive device detonated.

**March 8, 1996**
**Hijacking:** A hijacker entered the cockpit of a Cyprus Turkish Airlines 727 en route from Ercan Airport in northern Cyprus to Istanbul.

**March 10, 1996**
**Hijacking:** A Hainan Airlines 737 aircraft was hijacked over China by two married couples armed with knives and dynamite.

**March 10, 1996**
**Shootings at airports:** Rival motorcycle gangs opened fire on each other almost simultaneously at airports in Denmark and Norway.

**March 24, 1996**
**Hijacking: A** Sudan Airways flight from Khartoum to Port Sudan was hijacked by two Sudanese oppositionists.

**March 27, 1996**
**Hijacking:** An Egypt-Air A310 domestic flight from Luxor to Cairo was hijacked.

**April 4, 1996**
**Hijacking:** A Biman Bangladesh Airlines flight from Dhaka to Barisa, Bangladesh, was hijacked. The hijacker announced he had a revolver and explosives.

**April 14, 1996**
**Hijacking:** A Cessna 402 general aviation airport was hijacked in Papua New Guinea.

**April 15, 1996**
**Shooting at airport:** An Indonesian Special Forces officer fired into a crowd at Jakarta International Airport.

**April 25, 1996**
**Bombing:** A device exploded near an Indian Airlines Office in Imphal, India.

**April 28, 1996**
**Bombing:** A pipe bomb detonated outside an Aeroflot Airlines office in Istanbul.

**May 12, 1996**
**Attempted bombing:** A bomb threat called in to the Ataturk Airport in Turkey led to the discovery of an unexploded device left in a bathroom at the airport.

**June 6, 1996**
**Bombing:** The Black Mambas, a political group, were suspected of responsibility for an explosion at Lusaka Airport in Zambia in a restroom on the second floor of the main terminal.

**July 3, 1996**
**Attempted bombing:** A cleaning crew discovered an explosive device in a public restroom at the La Paz Airport in Bolivia.

**July 7, 1996**
**Hijacking:** A Cuban national air service (Cubanacan) Antonov AN-2, was hijacked and forced to land at the U.S. Navy base at Guantanamo.

**July 20, 1996**
**Bombing at airport:** In the passenger terminal at Reus Airport in Tarragona, Spain, an explosive device detonated, killing 35 people.

**July 22, 1996**
**Bombing at airport:** In the domestic departure lounge, a bomb contained in a briefcase detonated at Lahore International Airport in Pakistan.

**July 25, 1996**
**Hijacking:** An Air Algeria 767 was hijacked en route from Oran to Algiers by a man claiming to have an explosive device.

**July 26, 1996**
**Hijacking:** An Iberia DC-10 was hijacked en route from Barajas Airport in Madrid to Havana. The hijacker used items in his carry-on baggage to assemble a fake bomb.

**August 9, 1996**
**Hijacking:** An Air Mauritania Fokker 28 was hijacked en route from Las Palmas to the capital of Mauritania, Nouakchott.

**August 13, 1996**
**Robbery:** An Air Inter aircraft at Perpignan's airport in southern France was held at gunpoint while armed gunmen stole items from the baggage hold.

**August 16, 1996**
**Hijacking:** A single-engine Wilga charter aircraft en route from Cuba was forced to fly to the United States.

**August 26, 1996**
**Hijacking:** A Sudan Airlines A310 was hijacked en route from Khartoum to Amman.

**September 3, 1996**
**Hijacking:** A chartered Tupolev TU-154 aircraft was hijacked en route from Beirut to Varna, Bulgaria.

**October 17, 1996**
**Hijacking:** An Aeroflot TU-154 was hijacked en route from Moscow to Lagos, Nigeria.

**October 21, 1996**
**Hijacking:** An Indonesian Army sergeant hijacked a Twin-Otter cargo plane.

**October 30, 1996**
**Airport attack:** An unknown group fired a mortar round at the Houari Boumedienne International Airport in Algiers.

**November 2, 1996**
**Attempted hijacking:** A plot by four people, one of whom was a pilot, to hijack a Brazil Central Airlines plane was foiled when an informant disclosed the plot to police.

**November 3, 1996**
**Shooting:** A car pulled up as the plane of Yevhen Shcherban, reportedly the richest man in Ukraine, landed at Donetsk Airport, Ukraine, and opened fire.

**November 4, 1996**
**Shooting:** Several shots were fired at the Aeroflot Airlines office in the Philippines by an unidentified gunman on a motorcycle.

**November 15, 1996**
**Hijacking:** A domestic Xiamen Airlines flight from Xiamen to Guangzhou was hijacked.

**November 20, 1996**
**Attempted bombing:** An explosive device was found in an unattended bag on the arrival area's sidewalk at Manila Airport in the Philippines.

**November 23, 1996**
**Hijacking:** An Ethiopian Airlines 767 flying from Addis Ababa, to Nairobi, Kenya, was hijacked by three men claiming to have a bomb.

**November 27, 1996**
**Hijacking:** Two people chartered a plane to pick up passengers in Kwebanna, Guyana. They passengers held the pilots at gunpoint to force the plane to go to Trinidad.

**November 30, 1996**
**Attempted bombing:** On an All Nippon Airways flight from Matsuyama to Osaka, a timed incendiary device was found inside checked luggage.

**December 6, 1996**
**Hijacking:** A man came into the cockpit of a Krasnoyarsk Aviation Company YAK-40, demanding to be taken to Holland.
Source*: Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1996.

### 1997

**January 6, 1997**
**Grenade Attack:** Five grenades were thrown at Madrid's Barajas Airport, in Spain.

**January 7, 1997**
**Hijacking:** An Austrian Airlines MD-80 was hijacked en route from Berlin to Vienna.

**January 20, 1997**
**Hijacking:** An All Nippon Airways 777 was hijacked en route from Osaka to Fukuoka.

**January 22, 1997**
**Commandeering:** An Air Nelson Saab commuter aircraft was commandeered at the Nelson, New Zealand, airport.

**January 26, 1997**
**Attempted hijacking:** A Saudi Arabian Airlines chartered aircraft was hijacked at Casablanca's Mohamed V Airport.

**January 28, 1997**
**Bombing:** An explosive device detonated at the Air France offices in Nice, France.

**February 10, 1997**
**Hijacking:** A China Northwest Airlines flight was hijacked en route from Chongqing, Sichuan Province, to Zhuhai, Guangdong Province.

**February 12, 1997**
**Bombing:** This occurred the Barranquilla Airport, Colombia, when the Colombian president's plane was approaching.

**March 10, 1997**
**Hijacking:** A Far East Air Transport 757 was hijacked en route from Kaohsiung to Taipei in Taiwan.

**March 29, 1997**
**Grenade:** At Moscow International Airport, a preflight inspection on a TU-154 chartered aircraft found a live grenade in the passenger cabin.

**March 31, 1997**
**Bombing:** A device detonated at Ndjili Airport in Zaire either in a customs office or in an adjacent building.

**April 4, 1997**
**Attempted bombing:** An IED was placed outside an Alitalia Airlines office in Greece.

**April 8, 1997**
**Airport shooting:** A passenger shot at a 747 aircraft after it landed at the Phnom Penh Airport in Cambodia.

**April 15, 1997**
**Commandeering:** A DC-3 aircraft was hijacked en route from south central Zaire to Kinshasa's Ndjili Airport.

**May 9, 1997**
**Shooting:** A Nigerian Air Force Presidential Task Force (NAFPTF) member was prohibited from entering a restricted area at Lagos Airport, Nigeria, because of improper identification. Other NAFPTF members opened fire on the security guards.

**June 2, 1997**
**Hijacking:** An Air China 747 or 777 was hijacked between Beijing and Guangzhou.

**June 9, 1997**
**Hijacking:** An Air Malta 737 was hijacked en route from Valletta, Malta, to Istanbul by men claimed to have explosive devices.

**June 17, 1997**
**Attempted bombing:** A bomb was found in the customs cargo terminal at Almaty Airport, Kazakhstan.

**July 9, 1997**
**Bombing:** An in-flight explosion occurred on board a TAM F-100 on a domestic flight from Victoria to São Paulo, Brazil.

**July 26, 1997**
**Bomb hoax:** A device was discovered near a United Airlines ticket counter at San Francisco Airport, California.

**August 9, 1997**
**Hijacking:** A chartered 727 was hijacked en route from Franceville, Gabon, to Kigali, Rwanda.

**August 10, 1997**
**Bombing:** Outside Simon Bolivar Airport, Colombia, a car bomb exploded near the airport's fuel depot.

**August 12, 1997**
**Bombing:** A device exploded near the exit from the departure lounge at Begumpet Airport, Hyderabad, India.

**September 18, 1997**
**Bombing:** A parcel bomb among the luggage detonated at Agostino Neto Airport in Pointe Noire, Congo Brazzaulle.

**October 6, 1997**
**Hijacking:** An Iran Air flight from Tehran to Bandar Abbas, Iran, was hijacked by a passenger armed with a handgun.

**October 19, 1997**
**Bombing:** For the second time in six months, an IED detonated in front of the Alitalia Airlines office in Greece.

**November 29, 1997**
**Tampering with aircraft:** A United Express aircraft's preflight inspection at Chicago's O'Hare International Airport revealed that wires for the backup brake system were cut.

**December 10, 1997**
**Hijacking:** A Rossiya Airlines IL-62 was hijacked en route from Magadan, Russia, to Moscow.

**December 13, 1997**
**Bombing:** An IED exploded in a government security vehicle outside Abuja Airport, Nigeria.

**December 19, 1997**
**Hijacking:** An Aero Condor BE-200 was hijacked en route from Lima to Chimbote, Peru.

**December 22, 1997**
**Hijacking:** A China Eastern Airlines aircraft was hijacked on a domestic flight between Shanghai and Xiamen.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1997.

## 1998

**January 28, 1998**
**Shooting:** An unidentified shooter opened fire on two passengers who had just deplaned at Jakarta Airport, Indonesia.

**January 31, 1998**
**Hijacking:** An Atlantic Airlines twin-engine plane was hijacked after taking off from Bluefields on a domestic flight to Little Corn Island, Nicaragua.

**February 2, 1998**
**Airport attack:** Three timed projectiles were launched towards the cargo airplane hold at Tokyo's Narita Airport, Japan.

**February 6, 1998**
**Averted hijacking:** A security checkpoint in Fort Lauderdale, Florida, discovered an abandoned carry-on bag. The bag contained a handgun and several notes.

**February 24, 1998**
**Hijacking:** A Turkish Airlines Avro RJ100 was hijacked after taking off from Adana on a domestic flight to Ankara.

**March 12, 1998**
**Commandeering:** The FARC (Revolutionary Armed Forces of Colombia) took control of a Cessna 182 at the airstrip in Palmerito, Cumbaribo Municipality, Colombia.

**March 23, 1998**
**On-aircraft incident:** On a domestic flight between Taipei and Chiayi, Taiwan, a man tried to set fire to a Great China Airlines de Havilland Dash 8–300.

**March 30, 1998**
**Hijacking:** A Cyprus Turkish Airlines 727 was hijacked after taking off from Cyprus en route to Ankara.

**May 10, 1998**
**Commandeering:** A Portuguese Air Luxor Lockheed L-1011 was seized as passengers were boarding at Toronto's Pearson International Airport.

**May 17, 1998**
**Bombing:** An IED exploded in central Athens in front of the Olympic Airways Office.

**May 24, 1998**
**Hijacking:** A Pakistan International Airlines flight from Turbat, Pakastan, to Karachi was hijacked.

**June 23, 1998**
**Hijacking:** An Iberia 727 on a domestic flight from Seville to Barcelona, Spain, was hijacked. The plane was diverted to Valencia Airport.

**July 2, 1998**
**Attempted bombing:** Two people were arrested for a plan to detonate a bomb at Khartoum Airport.

**July 25, 1998**
**Hijacking:** An Aviones de Oriente Beech 1900 was hijacked en route from Caracas to Barinas State, Venezuela. The passengers and crew were released on a remote airstrip at a cattle ranch.

**August 2, 1998**
**Commandeering:** A Blue Airlines 727 was seized by Congolese rebels in Goma, Democratic Republic of Congo.

**August 4, 1998**
**Commandeering:** Two days later the Congolese rebels seized a Congo Air B-707 in Goma.

**August 4, 1998**
**Commandeering:** On the same day, the rebels also took over an Air Atlantic Cargo plane.

**August 9, 1998**
**On-aircraft incident:** A flight attendant for an East Line Aviation flight found an anonymous note on board. The note demanded money and fuel for the plane to be flown to another country.

**September 14, 1998**
**Hijacking:** A Turkish Airlines A-310 was hijacked on a domestic flight from Ankara to Istanbul.

**October 2, 1998**
**Hijacking:** A Dassault Aviation corporate jet shuttling employees between Marseille and Paris was hijacked by a former employee.

**October 10, 1998**
**Shooting:** An LAC (Lina Conog) evacuating citizens from Kindu to Kinshasha, Democratic Republic of Congo, was shot down by a missile that struck a rear engine.

**October 22, 1998**
**Bombing:** An IED exploded at Cabinda Airport's (Angloa) airline passenger guest house.

**October 27, 1998**
**Shooting:** A helicopter, flying near the town of Orito, Colombia, was shot down during a heavy fight between FARC guerrillas and the Colombia military.

**October 28, 1998**
**Hijacking:** A Air China 737 was hijacked en route from Beijing to Kunming by the pilot.

**October 29, 1998**
**Hijacking:** A THY 787 that had departed from Adana, Turkey, en route to Ankara was hijacked.

**November 13, 1998**
**Airport incident:** A man put a gun in the back of a ticketed passenger; when questioned at the security checkpoint, he doused the passenger in lighter fluid.

**November 25, 1998**
**Bombing:** One hundred thirty pounds of dynamite exploded in a car parked outside the Medellin Airport cargo warehouse in Colombia.

**December 14, 1998**
**Shooting:** An Antonov-12 cargo/passenger aircraft flying at a low altitude during a fight between Angolan government forces and UNITA rebels was shot down by the rebel forces.

**December 26, 1998**
**Shooting:** A C-130 charted by the United Nations was shot down near the village of Vila Nova, Angola, during a flight between Huambo and Suriname.

Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1998.

## 1999

**January 2, 1999**
**Shooting:** A C-130 plane evacuating UN staff from Huambo, Angola, crashed 20 minutes into the flight after being struck with gunfire. The plane was en route to Luanda, Angola.

**January 4, 1999**
**Robbery:** A Kenyan Airlines 737 was robbed while on the runway at Murtala Mohamed International Airport in Lagos, Nigeria. The taxiway had been blocked with several large pieces of wood that the pilot was unable to maneuver around.

**January 12, 1999**
**Threatening passenger:** A passenger on board a Southwest Airlines flight from San Diego to San Jose, California, threatened to kill other passengers if the plane was not taken to Hollywood, California.

**February 9, 1999**
**Averted hijacking:** Four previous hijackers being repatriated from China to Taiwan attempted to hijack their chartered flight.

**February 17, 1999**
**Robbery:** On the tarmac at Brussels National Airport two aircraft, a Virgin Atlantic plane and a Virgin Express plane, while transferring money and jewelry, were robbed at gunpoint. Maintenance workers at the airport helped the robbers gain access to the secure area.

**February 20, 1999**
**Bombing:** A demonstration group in support of Abdullah Ocalan threw large firecrackers at a Turkish Airlines office in Rome.

**March 2, 1999**
**Hijacking:** An Air France A-320 was hijacked en route from Marseille to Paris.

**April 9, 1999**
**Assassination:** As Niger's President Ibrahim Bare Mainassara boarded a plane at Niamey Airport in Niger, he was assassinated by members of his Presidential Guard.

**April 9, 1999**
**Incendiary device:** An improvised incendiary device was placed in the cockpits of aircraft at the El Monte, Virginia, general aviation airport.

**April 12, 1999**
**Hijacking:** An Avianca Fokker 50 was hijacked on a domestic flight between Bucaramanga and Bogotá.

**May 12, 1999**
**Shooting:** UNITA rebels shot down an Antonov-23 aircraft charted by Avita for cargo transport as it departed from Luzamba, Angola.

**May 27, 1999**
**Bombing:** A shopping bag containing an explosive device exploded when it was thrown into an American Airlines office in downtown Zurich.

**June 12, 1999**
**Hijacking:** A Xiamen Airlines 737 was hijacked en route from Xiamen to Taiwan.

**June 12, 1999**
**Commandeering:** Nearly 100 Special Presidential Security Group soldiers seized a Congo Air Lines aircraft at Gemena Airport, Democratic Republic of Congo.

**July 8, 1999**
**Airport attack:** In Mumbai, India, a Pakistan International Airlines office was pelted at a downtown office with stones and bottles by activists of Shiv Sena.

**July 23, 1999**
**Hijacking:** An All Nippon Airways 747 was hijacked after departing from Tokyo's Haneda Airport on a domestic flight to Sapporo's Chitose Airport.

**July 30, 1999**
**Hijacking:** A Venezuelan Aviones de Oriente Airlines (AVIOR) was hijacked en route from Caracas to Guasdualito, Colombia.

**August 25, 1999**
**Hijacking:** A Royal Air Moroc 737 was hijacked en route from Casablanca to Tunis.

**August 28, 1999**
**Commandeering:** A MAF Airline twin Otter was taken over by five armed men on a remote airstrip on Lake Kopiago in Southern Highlands Province in Papua New Guinea.

**August 29, 1999**
**Shooting:** Ethiopian military forces shot down a Learjet 35 en route from Naples, Italy, to Johannesburg.

**September 22, 1999**
**Bombing:** A hangar, five planes, and three gliders were damaged or destroyed when a device detonated at Ghisonaccia Airport in Corsica.

**October 11, 1999**
**Theft/suicide plot:** An Air Botswana pilot stole an ATR-42 and began to circle Gaborone. The pilot notified the control tower of his intention to commit suicide, and as the plane began to run out of fuel he threatened to crash into a building or other target.

**October 19, 1999**
**Hijacking:** A man entered the cockpit of an Egypt-Air 737 unobstructed (the door had been inadvertently been left open), shortly after departure from Istanbul.

**October 26, 1999**
**Hijacking:** An Iran Air domestic flight between Tehran and Orumiyah was hijacked.

**October 31, 1999**
**Airport attack:** A blast destroyed a navigational aid system at the Camilo Daza Airport in Cucuta, Colombia.

**November 23, 1999**
**Hijacking:** A Zhejiang Airlines domestic flight between Yiwu and Xiamen was hijacked. The crew overcame the hijacker.

**November 25, 1999**
**Bombing:** A device was thrown into an American Airlines ticket office in Zurich.

**November 2, 1999**
**Commandeering:** Two Bell 400 tourist helicopters were hijacked at Marcos A. Gelabert Airport, Panama City, Panama.

**December 8, 1999**
**Bombing:** A device in a suitcase was placed outside an Aeroflot–Russian International Airlines ticket office.

**December 24, 1999**
**Hijacking:** An Indian Airlines Airbus A300 bound for New Delhi from Kathmandu, Nepal, was hijacked.

**December 28, 1999**
**Hijacking:** A Lufthansa CRJ was hijacked en route from Prague, Czech Republic, to Duesseldorf, Germany.
Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 1999.

## 2000

**January 20, 2000**
**Robbery:** A Navajo twin-engine general aviation aircraft was hijacked at Brewarinna Airport in New South Wales, Australia.

**February 6, 2000**
**Hijacking:** An Ariana Afghan Airlines 727 was hijacked en route from Kabul to Mazar-I-Sharif, Afghanistan.

**February 16, 2000**
**Airport attack:** Urrao Airport in Colombia was taken over by the FARC.

**February 19, 2000**
**Hijacking:** A Colombian Aerotransportes Casanare SA (Aerotaca) Beech 1900 plane was forced to land at a remote airstrip.

**February 29, 2000**
**Hijacking:** A China Southwest Airlines flight to Fuzhou from Chengdu via Nanchang was hijacked.

**March 14, 2000**
**Bombing:** Three bombs were discovered near a terminal gate at Jakarta Airport, Indonesia.

**March 14, 2000**
**Airport attack:** Nepalese Maoist rebels made an unsuccessful attempt to capture Salle Airport, Nepal.

**March 16, 2000**
**Hijacking:** On board Alaska Airlines MD-80 en route from Puerto Vallarta, Mexico, to San Francisco, a passenger forced himself into the cockpit attempting to gain control of the plane's throttles and fuel controls.

**March 30, 2000**
**Bombing:** A bomb was found at the Sheremetyevo Airport (Russia) flight training center.

**March 30, 2000**
**Airport attack:** Kassala Airport in Sudan was attacked by Sudanese rebels.

**May 3, 2000**
**Airport attack:** Muslim guerrillas opened fire on Cotabato Airport in the Philippines. A grenade exploded beside one of the runways at the airport.

**May 11, 2000**
**Hijacking:** An Egypt-Air A321 was hijacked en route from Cairo to Aswan by a man claiming to have a bomb.

**May 22, 2000**
**Hijacking:** An aircraft belonging to the Missionary Aviation Fellowship was hijacked en route from Erave to Batiri, Papua New Guinea.

**May 25, 2000**
**Hijacking:** A Philippine Airlines Airbus A330 was hijacked en route from Davao International Airport, Philippines, to Manila.

**May 30 2000**
**Bombing:** A homemade device was found on board an Azerbaijan Airlines TU-154.

**June 4, 2000**
**Bombing:** A bomb exploded in a women's restroom at Manila's Ninoy Aquino International Airport.

**July 5, 2000**
**Hijacking:** A Royal Jordanian A320 was hijacked en route from Amman to Damascus by a hijacker with a pistol and hand grenade.

**July 7, 2000**
**Robbery:** A Viacao Aérea de São Paulo (VASP) airliner was stormed on the tarmac at Brazil's Sao Paulo International airport.

**July 17, 2000**
**Hijacking:** A British Airways City Flyer Express was hijacked en route to London's Gatwick Airport from Zurich.

**July 18, 2000**
**Bombing:** A bomb exploded between the international and domestic terminals at Cape Town Airport in South Africa.

**July 27, 2000**
**Commandeering:** A National Airlines 757 was hijacked en route from New York's JFK International to Las Vegas. The hijacker showed his gun at the security checkpoint then ran onto the Jetway to board the aircraft.

**July 30, 2000**
**Bombing:** An explosive device was discovered in a restroom at Vientiane's Wattay Airport, Laos.

**July 31, 2000**
**Commandeering:** A man held a female hostage on a Cathay Pacific Airways aircraft parked at Hong Kong's International Airport.

**August 1, 2000**
**Airport takeover:** Papua Task Force, an Irian Jaya pro-independence civilian militia, took over Wamena Airport in Indonesia.

**August 16, 2000**
**Hijacking:** A VASP airliner was hijacked the equivalent of almost US$3 million was stolen from the cargo hold.

**August 18, 2000**
**Hijacking:** An Azerbaijan Airlines TU-154 was hijacked between Nakhichevan and Baku, Azerbaijan.

**September 8, 2000**
**Hijacking:** A Colombian Aires S.A. flight from Nieva to Florencia, Colombia, was taken over by an armed prisoner.

**September 14, 2000**
**Hijacking:** A Qatar Airways Airbus A300 was hijacked en route from Doha, Qatar to Amman.

**September 16, 2000**
**Commandeering:** The Istabu Freedom Movement militia group seized control of a Solomon Airlines Britten Norman Islander aircraft in the Solomon Islands.

**September 24, 2000**
**Hijacking:** An Iran Air Fokker 100 was hijacked with a gasoline bomb and a fake pistol on a flight bound for Tehran from Shiraz.

**September 27, 2000**
**Hijacking:** A Xinhua Airlines 737 from Baotou in Inner Mongolia to Beijing was hijacked. Both the pilot and the copilot were stabbed.

**September 28, 2000**
**Hijacking:** A Royal Jordanian A310 was hijacked en route from Sanaa, Yemen, to Amman.

**October 13, 2000**
**Hijacking:** Sabena Flight 689 en route from Belgium to Spain was forced to make an emergency landing in Malaga, Spain.

**October 14, 2000**
**Hijacking:** A Saudi Arabian Airlines 777 bound for London was hijacked by two Saudi Airport security officers employed at Jeddah's King Abdul Aziz International Airport.

**November 1, 2000**
**Hijacking:** A North Coast Aviation flight from Wau to Port Moresby, Papua New Guinea, had its cargo of gold stolen.

**November 9, 2000**
**Bombing:** A homemade device exploded near the domestic terminal entrance at Wattay Airport in Laos.

**November 11, 2000**
**Hijacking:** A Vnukovo Airlines TU-154 was hijacked on a domestic flight between Makhachkala, Dagestan, and Moscow.

**November 13, 2000**
**Hijacking:** An Iranian Ariatour Airlines Yakovlev YAK 40 was hijacked en route from Ahvaz to Bandar Abbas, Iran, by a group of four families.

**November 17, 2000**
**Hijacking:** Under the pretext of taking flying lessons, a man hijacked a Vietnamese-American chartered aircraft south of Bangkok.

**December 4, 2000**
**Shooting:** A Sabena A300 came under fire upon its descent into Bujumbura Airport in Burundi.

**December 17, 2000**
**Commandeering:** A passenger attempted to seize a London-bound Pakistan International Airlines flight from Karachi with a butter knife and an oxygen bottle.

**December 28, 2000**

**Airport attack:** Damage to the control tower, three airplanes, and the runway occurred during a two-hour firefight between UNITA rebels and security officials at Benguela Airport, Angola.

**December 30, 2000**

**Bombing:** Five explosive devices placed around Manila Airport in the Philippines nearly detonated simultaneously.

Source: *Criminal Acts against Civil Aviation*, U.S. Department of Transportation, 2000.

## 2001

**January 17, 2001**

**Airport Seizure Attempt:** In India, six members of the Lashkar-e-Tayybah militant group were killed when they attempted to seize a local airport.

Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State."

**January 22, 2001**

**Hijacking:** A Yemenia Airways flight en route to Taiz-Al Janad Airport, Yemen, was hijacked. The Iraqi hijacker had a pen gun and claimed to have a briefcase with explosives.

**January 27, 2001**

**Hijacking:** A Gulf Air flight from Bangkok to Abu Dhabi was hijacked. The target was Australia.

**January 30, 2001**

**Hijacking:** A SATENA aircraft was hijacked while on the ground at San Vicente Airport, Colombia.

**March 15, 2001**

**Hijacking:** A Russian airliner was hijacked en route from Istanbul to Moscow. The plane was forced to fly to Medina, Saudi Arabia.

Source: "Significant Terrorist Incidents, 1961–2003: A Brief Chronology, U.S. Department of State."

**May 2001**

**Airline uniform/credential heist:** An American Airlines crew discovered that their uniforms, documents, and identification badges had been stolen from a Washington, DC–area hotel.

Source: Unconfirmed, but believed to be true.

**July 2001**

**Airspace closure due to potential terrorist attack:** The Italian government closed airspace over Genoa and mounted antiaircraft batteries, based on information that Islamic extremists were planning to use an airplane to kill President Bush during the Genoa summit of the Group of Eight industrial

powers. There was the possibility of an attack against the U.S. president using an airliner.
Source: Unconfirmed, but believed to be true.

**July 1, 2001**
**Thwarted terrorist attack plot:** Djamel Begal, an Algerian member of al Qaeda, was arrested in the United Arab Emirates upon the discovery of his plot to crash a helicopter into the U.S. Embassy in Paris.
Source: Unconfirmed, but believed to be true.

**July 2001**
Los Angeles International Airport was revealed as the target of an Algerian with bomb material, Ahmed Ressam, who was arrested in the state of Washington in late 1999 and later convicted, but the Los Angeles airport was not revealed as the terrorist target until the trial of an accomplice in July 2001. "The FAA asked all airports and air carriers to assess their vulnerability and come up with common sense ways they might improve security," said agency spokeswoman Rebecca Trexler. The New York trial disclosure prompted the request, she said.
Source: Unconfirmed, but believed to be true.

**September 1, 2001**
**Hijacking:** An Aero Lloyd flight was hijacked en route to Berlin from Catania-Fontanarossa Airport, Italy.

**September 11, 2001**
**Hijacking:** In a coordinated effort, 19 men hijacked four planes on the morning of September 11. Five hijackers seized American Airlines Flight 11 en route from Boston's Logan Airport to Los Angeles. The hijackers took over control and crashed the plane into the north tower of the World Trade Center in New York City.

**September 11, 2001**
**Hijacking:** Five hijackers seized United Airlines Flight 175 en route from Boston's Logan Airport to Los Angeles. The hijackers took control and crashed the plane into the south tower of the World Trade Center in New York City.

**September 11, 2001**
**Hijacking:** Four hijackers seized United Airlines Flight 93 en route from Newark to San Francisco. The hijackers took control of the aircraft and the plane was headed toward Washington, DC. The passengers on board fought back against the hijackers and the plane crashed in a field near Somerset, Pennsylvania.

**September 11, 2001**
**Hijacking:** Five hijackers seized American Airlines Flight 77 en route to Los Angeles from Dulles Airport in Washington, DC. The plane was flown into the Pentagon.

**November 14, 2001**
**Hijacking:** Four men seized a Trans Guyana Airways flight from Lethem to Ogle. The plane was forced to land on a remote airstrip in Brazil and the hijackers escaped on horseback.
Source for the 2001 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 2002

**February 20, 2002**
**Hijacking:** Four leftist guerillas seized an AIRES Colombia flight en route to Bogota, Colombia, and kidnapped a senator who was on board.

**April 17, 2002**
**Hijacking:** A China Northern flight from Dalian to Shenyang was hijacked. The target was the United States.

**May 10, 2002**
**Hijacking:** A Xiamen Airlines flight from Shenzhen to Xiamen was hijacked. The hijacker smuggled two knives past security by hiding them in his shoes. The target was Taipei.

**June 9, 2002**
**Hijacking:** Two people attempted to seize an Ethiopian Airlines flight from Bahar Dar to Addis Ababa. They had smuggled an explosive and two knives on board.

**September 9, 2002**
**Hijacking:** An Air Seychelles flight from Mumbai, India, was hijacked by a hijacker who had smuggled an eight-inch knife past security.

**October 15, 2002**
**Hijacking:** A Saudi Arabian Airlines flight from Khartoum to Jeddah was hijacked.

**October 28, 2002**
**Hijacking:** A Shanghai Airlines flight from Shanghai to Fuzhou was hijacked. The target was Taiwan.

**November 12, 2002**
**Hijacking:** A Gol flight from Cuiaba to Brasilia, Brazil, was hijacked. The hijacker used gas and lighters to try to force the crew to submit to his demand to fly over the National Congress in order to bring attention to his financial situation.

**November 17, 2002**
**Hijacking:** An El Al flight from Tel Aviv to Istanbul was hijacked after a dispute arose with a flight attendant though the passenger involved denied the allegations.

**November 27, 2002**
**Hijacking:** An Alitalia flight from Bologna to Paris was hijacked by a man who was mentally ill. The hijacker claimed to be part of the al Qaeda network.
Source for the 2002 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database

## 2003

**January 19, 2003**
**Hijacking:** An Air Algerie flight from Constantine to Algiers was hijacked. The target was North Korea.

**January 24, 2003**
**Hijacking:** A Sichuan Airlines flight from Chongqing to Chengdu was hijacked. The hijacker ignited a homemade bomb.

**February 2, 2003**
**Hijacking:** An Air China flight from Beijing to Fuzhou was hijacked. The hijacker attempted to light a can of gasoline he had smuggled onto the plane but was overpowered by crew members.

**February 7, 2003**
**Hijacking:** A THY flight was hijacked after landing in Istanbul. The hijacker demanded to be flown to Moscow to see his girlfriend.

**March 19, 2003**
**Hijacking:** Six men armed with kitchen knives, tape, and the airplane's emergency hatchet seized an Aerotaxi flight en route to Havana. The target was Miami.

**March 28, 2003**
**Hijacking:** A 20-year-old seeking to join his birth father after a dispute with his stepfather, seized a THY flight from Istanbul to Ankara.

**March 31, 2003**
**Hijacking:** A Cubana flight was hijacked en route to Havana. The target was Key West.

**May 29, 2003**
**Hijacking:** A QantasLink/Impulse flight from Melbourne to Launceston, Australia, was hijacked.

**August 19, 2003**
**Hijacking:** An Air Algerie flight was hijacked after departing from Algiers, Algeria. The target was Geneva.
Source for the 2003 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 2004

**April 17, 2004**
**Hijacking:** A Qatar flight from Casablanca to Doha, Qatar, was hijacked by a man with some type of mental disturbance. The target was Geneva.

**July 26, 2004**
**Hijacking:** An Air China flight from Beijing to Changsha was hijacked by a man claiming to have sulphuric acid. The target was South Korea.

**August 24, 2004**
**Bombing:** A Volga-AviaExpress flight exploded, nearly simultaneously with a Sibir flight departing from Moskva, in mid-flight en route to Volgograd. Two females were detained before the flight by a police captain on suspicion of terrorism, but were released without being searched. It was determined that one of them was one of the female suicide bombers.

**August 24, 2004**
**Bombing:** A Sibir Airlines flight en route to Adler from Moskva. Two females were detained before the flight by a police captain on suspicion of terrorism, but were released without being searched. It was determined that one of them was one of the female suicide bombers.

**September 29, 2004**
**Hijacking:** A Kato Air flight was hijacked upon its descent into Bodø Airport, Norway. It was reported that the hijacker's application for political asylum had been denied.

Source for the 2004 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 2005

**September 12, 2005**
**Hijacking:** A man in a wheelchair and his son seized an AIRES Colombia plane en route to Bogota. The man's application to the Council of State for social security benefits had been rejected.

Source for the 2005 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 2006

**June 17, 2006**
**Attempted hijacking:** A 21-year-old Zimbabwean student attempted to seize an SAA flight from Cape Town to Johannesburg. Armed with a hypodermic needle, he attempted to force his way inside the cockpit.

**October 3, 2006**
**Hijacking:** A THY flight was hijacked en route to Istanbul. A demand was made for political asylum. The target was Italy.

**December 28, 2006**
**Hijacking:** An Aeroflot Russian International flight from Moscow to Switzerland was hijacked. The target was Cairo.
Source for the 2006 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## 2007

**January 22, 2007**
**Hijacking:** An Air Botswana flight was hijacked en route from Gaborone, Botswana, to Johannesburg. The hijacker claimed to have a bomb and to be a member of al Qaeda.

**January 24, 2007**
**Hijacking:** An Air West flight was hijacked en route to El Fasher Airport from Khartoum. A demand for asylum was addressed to the French embassy. The target was Chad.

**February 15, 2007**
**Hijacking:** An armed man seized an Air Mauritanie flight from Nouakchott to Nouadhibou, Mauritania. The target was France.

**March 30, 2007**
**Hijacking:** A Sudan Airways flight from Tripoli, Libya, to Khartoum was hijacked. The target was South Africa.

**April 10, 2007**
**Hijacking:** A Pegasus Airlines flight from Diyarbakir to Istanbul was hijacked. The hijacker claimed to have a bomb and demanded to be flown to Ankara and later to Tehran.

**August 18, 2007**
**Hijacking:** Two men claiming to be members of al Qaeda seized an Atlasjet flight en route to Istanbul from Ercan.
Source for the 2007 section (unless otherwise stated): Aviation Safety Network Database: http://aviation-safety.net/database.

## CONCLUSION

The 9/11 Commission Report concluded that before September 11, 2001, the possibility of a suicide hijacking was indeed foreseeable and foreseen. The Federal Aviation Administration had discussed such a scenario in its August 4, 1999, intelligence report, "Osama Bin Laden/World Islamic Front Hijacking Threat," and the National Security Council Counterterrorism Security Group held a meeting on January 31, 2001, devoted to the possibility of an airplane hijacking by al Qaeda. Therefore, even though on September 11 "the possibility was imaginable and imagined,"[1] 19 out of 19 suicide hijackers breezed through security because the airlines were profiling for bombs in

checked bags, the threat vector utilized on Pan Am 103. The history of attacks on civil aviation did not support such a profiling assumption. Chief Justice Oliver Wendell Holmes, Jr., perhaps said it best: "Upon this point a page of history is worth a volume of logic."[2] His advice may prove especially sage when trying to predict the logic of terror.

## NOTES

1. *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton, Co., 2004), 345.
2. *New York Trust Co. v. Eisner*, 256 U.S. 345, 349 (1921).

# Financial Condition and Industry Responses Affect Competition

*Statement of JayEtta Hecker, Director, Physical Infrastructure Issues*

Mr. Chairman and Members of the Committee:

Thank you for inviting us to testify today on the economic state of the airline industry. Just over a year ago, we testified before this Committee on guidelines for providing financial assistance to the industry.[1] The Congress has long recognized that the continuation of a strong, vibrant, and competitive commercial airline industry is in the national interest. A financially strong air transport system is critical not only for the basic movement of people and goods, but also because of the broader effects this sector exerts throughout the economy. In response to the industry's financial crisis generated by the events of last September, the Congress passed the Air Transportation Safety and System Stabilization Act.[2] Thus, it is fitting that we now return to this Committee to review the state of the industry's financial health and competitiveness.

Over the past several years, we have issued a number of reports that focus on changes within the airline industry. They include analyses of the potential impacts on consumers of airline mergers and alliances, carriers' use of regional jets, and changes in service to the nation's smaller communities.[3] Our statement today builds on that body of work and provides a current overview of (1) the financial condition of major U.S. commercial passenger airlines; (2) steps taken by airlines to improve their financial condition; and (3) some public policy issues related to current conditions and changes in the aviation industry's competitive landscape.

In summary:

- Many, but not all, major U.S. passenger airlines are experiencing their second consecutive year of record financial losses. In 2001, the U.S. commercial passenger

airline industry reported losses in excess of $6 billion. For 2002, some Wall Street analysts recently projected that U.S. airline industry losses will approach $7 billion, and noted that the prospects for recovery during 2003 are diminishing. Such projections could worsen dramatically in the event of additional armed conflict, if travel demand drops and fuel prices rise. Several carriers have entered Chapter 11 bankruptcy proceedings. Yet Southwest Airlines, JetBlue, and AirTran continue to generate positive net income. These low-fare carriers have fundamentally different business structures than most major U.S. airlines, including different route structures and lower operating costs. However, federal security requirements have altered the cost of doing business for all carriers.

- Carriers have taken many actions to lower their costs and restructure their operations. Since September 2001, carriers have furloughed an estimated 100,000 staff, renegotiated labor contracts, and streamlined their fleets by retiring older, costlier aircraft. Carriers have reduced capacity by operating fewer flights or smaller aircraft, such as substituting "regional jets" for large "mainline" jet aircraft. In some cases, carriers eliminated all service to communities. For example, since September 2001, carriers have notified the Department of Transportation (DOT) that they intend to discontinue service to 30 small communities. At least two carriers are modifying their hub operations to use resources more efficiently by spreading flights out more evenly throughout the day. Finally, to increase revenues, some carriers have proposed creating marketing alliances under which the carriers would operate as code-sharing partners.[4] United Airlines and US Airways announced plans to form such an alliance on July 24, 2002, as did Continental Airlines, Delta Air Lines, and Northwest Airlines one month later.
- As the aviation industry continues its attempts to recover, the Congress will be confronted with a need for increased oversight of a number of public policy issues. First, airlines' reactions to financial pressures will affect the domestic industry's competitive landscape. Some changes, such as extending airline networks to new markets through code sharing alliances, may increase competition and benefit consumers. Others, such as carriers' discontinuing service to smaller communities, may decrease competition and reduce consumers' options, particularly over the long term. Second, airlines' reductions in service will likely place additional pressure on federal programs supporting air service to small communities, where travel options are already limited. Finally, while domestic travel has been the focus of our concern today, there are numerous international developments—especially regarding the European Union (EU)—that may affect established international "open skies" agreements between the United States and EU member states. Various studies have illustrated the benefits to both consumers and carriers that flow from liberalizing aviation trade through such agreements. As international alliances are key components of major domestic airlines' networks, international aviation issues will affect the overall condition of the industry.

## BACKGROUND

The Airline Deregulation Act of 1978 has led to lower fares and better service for most air travelers, largely because of increased competition. The experiences of millions of Americans underscore the benefits that have flowed to most consumers from the deregulation of the airline industry, benefits that

include dramatic reductions in fares and expansion of service. These benefits are largely attributable to increased competition, which has been spurred by the entry of new airlines into the industry and established airlines into new markets. At the same time, however, airline deregulation has not benefited everyone; some communities have suffered from relatively high airfares and a loss of service.

The airline industry is a complex one that has experienced years of sizable profits and great losses. The industry's difficulties since September 11, 2001, do not represent the first time that airlines have faced a significant financial downturn. In the early 1990s, a combination of factors (e.g., high jet fuel prices due to Iraq's invasion of Kuwait and the global recession) placed the industry in turmoil. Between 1990 and 1992, U.S. airlines reported losses of about $10 billion. All major U.S. airlines[5] except Southwest reported losses during those years. In addition, several airlines—most notably Braniff, Eastern, and Pan Am—went out of business, and Trans World Airlines, Northwest Airlines, and Continental Airlines entered bankruptcy proceedings. By the start of 1993, the industry had turned the corner and entered a period during which nearly all major U.S. airlines were profitable. The industry rebounded without massive federal financial assistance.

The events of September 11th accelerated and aggravated negative financial trends that had begun earlier in 2001. Congress responded quickly to address potential instability in the airline industry by enacting the Air Transportation Safety and System Stabilization Act. Among other things, that act authorized payments of $5 billion in direct compensation (grants) to reimburse air carriers for losses sustained as a direct result of government actions beginning on September 11, 2001, and for incremental losses incurred between September 11 and December 31, 2001 as a direct result of the terrorist attacks. The act provided $10 billion in loan guarantees to provide airlines with emergency access to capital and established the Air Transportation Stabilization Board (the Board) to administer the loan program.[6] The Board is tasked not only with providing financial assistance to airlines but also with protecting the interests of the federal government and American taxpayer. The act requires the Board to ensure that airlines are compensating the government for the financial risk in assuming guarantees. This requirement defines the loan guarantee as a mechanism for supporting airlines with reasonable assurances of financial recovery. In addition to the grants and loan guarantees, the federal government has also established other ways to ease the airlines' financial condition.[7]

## MANY CARRIERS FACE DEEP FINANCIAL LOSSES

Many major U.S. passenger airlines are experiencing their second consecutive year of record financial losses. In 2001, the industry reported a net loss of over $6 billion, even after having received $4.6 billion from the federal government in response to September 11th.[8] For 2002, some Wall Street analysts have projected that U.S. airline industry losses will total about $7 billion,

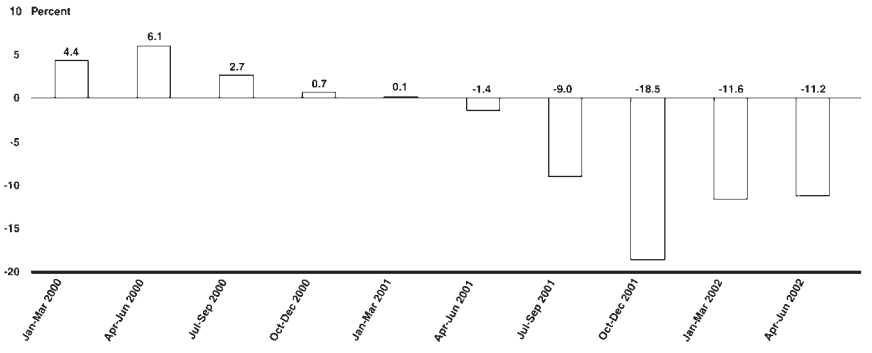
but this projection may worsen in the event of additional armed conflict, particularly if this results in decreasing travel demand and rising fuel prices. According to industry data, airlines' revenues have declined 24 percent since 2000, while costs have remained relatively constant. US Airways and Vanguard Airlines filed for Chapter 11 bankruptcy during this summer. United Airlines officials stated that they are preparing for a potential Chapter 11 bankruptcy filing this fall. Furthermore, some Wall Street analysts predict that it will likely take until 2005 for the industry to return to profitability. Attachment I summarizes the financial condition of major network and low-fare carriers.[9]

Major airline carriers' revenues have fallen because of a combination of a decline in passenger enplanements[10] and a significant decrease in average fares. As figure 1 shows, major carriers' enplanements increased for every quarter of 2000 compared to the same quarter of the previous year, but flattened in the first quarter of 2001 and then dropped, with the steepest drop occurring in the quarter following September 11, 2001.

Over the same period, major airlines have also received lower average fares. Data from the Air Transport Association indicate that the average fare for a 1,000-mile trip dropped from $145 in June 2000 to $118 in June 2002, a decrease of about 19 percent (see fig. 2). Average fares started dropping noticeably in mid-2001 and have not risen significantly since. Industry data suggest that the decline is due to the changing mix of business and leisure passenger traffic, and particularly to the drop in high-fare business passengers.

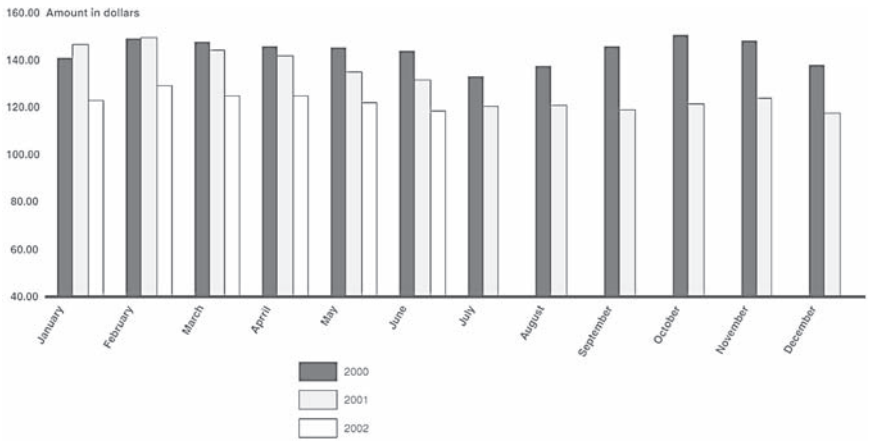
Through June 2002, all major network carriers generated negative net income, while low-fare carriers Southwest Airlines, JetBlue, and AirTran returned positive net income. Like the major carriers, these low-fare carriers' passenger enplanements dropped in the months immediately following September 2001. Attachment II summarizes passenger enplanements for individual major and low-fare carriers for 2000, 2001, and the first 5 months of 2002.

**Figure 1**
**Major Airlines' Passenger Enplanements (quarterly)—Percentage Change from Prior Year**




*Source:* GAO analysis of data from the Air Transport Association.

**Figure 2**
**Average Domestic Airfares for Major Network Carriers, January 2000 Through June 2002**




*Note:* Data are in nominal dollars for 1,000-mile trips on U.S. major airlines (excluding Southwest).
*Source:* GAO presentation of data from the Air Transport Association.

Why have some low-fare carriers been able to earn positive net income in current market conditions, while network carriers have not? The answer seems to rest at least in part with their fundamentally different business models. Low-fare carriers and major network carriers generally have different route and cost structures. In general, low-fare carriers fly "point-to-point" to and from airports in or near major metropolitan areas, such as Los Angeles, Chicago, and Baltimore–Washington. In comparison, major network carriers use the "hub and spoke" model, which allows them to serve a large number of destinations, including not just large cities, but small communities and international destinations as well. American Airlines, for example, can carry a passenger from Dubuque, Iowa, through Chicago, to Paris, France.

Low-fare carriers have also been able to keep costs lower than those of major airline carriers. For example, 2002 data reported by the carriers to DOT indicate that Southwest's cost per available seat mile (a common measure of industry unit costs) for one type of Boeing 737 is 3.79 cents. For the same aircraft type, United Airlines reported a cost of 8.39 cents—more than twice the cost at Southwest.

All airlines are now entering an environment in which some of the costs of doing business have increased. The federal Transportation Security Administration has taken over responsibility for many security functions for which airlines previously had been responsible. The Air Transport Association (ATA) estimated that the airline industry spent about $1 billion for security in 2000.[11] Despite the shift in functional responsibilities, airlines have stated that

they continue to bear the costs of other new federal security requirements. In August 2002, Delta Air Lines estimated the cost of new federal security requirements that it must bear to be about $205 million for 2002. This includes the cost of reinforcing cockpit doors, lost revenues from postal and cargo restrictions, and lost revenues from carrying federal air marshals.

## AIRLINES HAVE TAKEN NUMEROUS ACTIONS TO ADDRESS CHANGING MARKET CONDITIONS

To address mounting financial losses and changing market conditions, carriers have begun taking a multitude of actions to cut costs and boost revenues. First, many carriers have trimmed costs through staff furloughs. According to the Congressional Research Service, carriers have reduced their workforces by at least 100,000 employees since last September. Further, some carriers, including United Airlines and US Airways, have taken steps to renegotiate contracts in order to decrease labor and other costs. A US Airways official stated that its renegotiated labor agreements would save an estimated $840 million annually.

Carriers have also grounded unneeded aircraft and accelerated the retirement of older aircraft to streamline fleets and improve the efficiency of maintenance, crew training, and scheduling. Carriers accelerated the retirement of both turboprops and a variety of larger aircraft, including Boeing 737s and 727s. For example, United and US Airways retired the Boeing 737s used by United's Shuttle service and US Airways' MetroJet system, and the carriers discontinued those divisions' operations. Industry data indicate that the airlines have parked over 1,400 aircraft in storage, with more than 600 having been parked since September 2001.

Although carriers had begun reducing capacity earlier in 2001, those reductions accelerated after the terrorist attacks. Between August 2001 and August 2002, major carriers reduced capacity by 10 percent. Carriers can decrease capacity by reducing the number of flights or by using smaller aircraft, such as replacing mainline service with regional jets, which are often operated by the network carrier's regional affiliate and normally have lower operating costs. For example, American Airlines serves the markets between Boston, New York (LaGuardia), and Washington, D.C. (Reagan National) only with regional jet service provided by its affiliate, American Eagle. Another way carriers have reduced capacity is to discontinue service to some markets, primarily those less profitable, often smaller communities. Our previous work showed that the number of small communities that were served by only one airline increased from 83 in October 2000 to 95 by October 2001. Between September 2001 and August 2002, carriers had notified DOT[12] that they intend to discontinue service to 30 additional communities, at least 15 of which were served by only one carrier and are now receiving federally-subsidized service under the Essential Air Service (EAS) program.[13]

Some carriers are modifying their "hub and spoke" systems. American is spreading flights out more evenly throughout the day instead of operating

many flights during peak periods. American began this effort in Chicago and has announced that it would expand its "de-peaking" efforts to its largest hub at Dallas/Fort Worth beginning November 2002. American officials stated that these changes would increase the productivity of labor and improve the efficiency of gate and aircraft use. Delta officials said they are also taking steps to spread flights more evenly throughout the day.

Beyond the steps individual carriers are taking to restructure and cut costs, some carriers are proposing to join forces through marketing and codesharing alliances in order to increase revenues. Under these proposed alliances, carriers would sell seats on each other's flights, and passengers would accrue frequent flyer miles. Company officials stated that the carriers would remain independent competitors with separate schedules, pricing, and sales functions. On July 24, 2002, United and US Airways announced a proposed codesharing alliance to broaden the scope of their networks and potentially stimulate demand for travel. United and US Airways estimated that the alliance would provide more than $200 million in annual revenue for each carrier. One month later, Northwest announced that it had signed a similar agreement with Continental and Delta. According to Northwest, this agreement builds on the alliance between Northwest and Continental that had been in existence since January 1999. These alliances would expand both their domestic and international networks. The Department of Transportation is currently reviewing these proposals.[14]

## CRITICAL PUBLIC POLICY ISSUES ARE ASSOCIATED WITH THE INDUSTRY'S CHANGING COMPETITIVE LANDSCAPE

Because a financially healthy and competitive aviation industry is in the national interest, and because carriers' and the federal government's efforts to address the current situation may affect consumers both positively and negatively, Congress will be confronted with several major public policy issues. These policy issues underscore the difficulties this industry will encounter as it adapts to a new market environment. We are highlighting three of these issues: the effect of airlines' current financial situation, including new business costs, on industry health and competition; the impact of reductions in service on federal programs designed to protect service to small communities, and international developments that may further affect the domestic industry.

- **How will the carriers' reactions to current financial pressures affect the industry's competitive landscape?** There is a new aviation business reality that has increased the airlines' financial pressures and which ultimately will be felt by U.S. consumers. Increased federal security requirements, which are part of this new reality, are adding to the cost of competing in the industry. The cost of these policies will most likely be borne both by industry, through higher operational costs, and the consumer, through higher fares. In the current pricing environment, carriers may not be able to pass on these costs to consumers, and thus may be bearing their full

impact during the short run. On the other hand, these same security requirements may be helping the airlines maintain some of its passenger revenue; some portion of the airlines' current passengers may be flying only as a result of knowing that these heightened security requirements are in place. Thus, the question arises about the net impact of the new market environment and new security requirements on the carriers and their passengers while the industry restructures. While understandable from the perspective of an individual airline's bottom line, the restructuring activities of individual carriers will significantly change the competitive landscape. When carriers decrease available capacity in a market by reducing the number of flights, decreasing the size of aircraft used to meet reduced demand, or dropping markets altogether, the net result is that consumers have fewer options. In doing so, airlines reduce the amount of competition in those markets. As has been shown repeatedly, less competition generally leads to higher fares in the long run.

A related issue concerns the industry's consolidation, whether through marketing alliances among or mergers between carriers. Because of the potential that consolidation presents for competition, federal oversight has been critical. As we have noted before, while alliances may offer potential consumer benefits associated with expanded route networks, more frequency options, improved connections, and frequent flyer benefits, consolidation within the industry raises a number of critical public policy issues.[15] These include increasing potential barriers to market entry, the loss of competition in key markets, and a greater risk of travel disruptions as a result of labor disputes.[16] Since these alliances and mergers have a direct impact on the level of competition within the airline industry and would therefore influence the affordability of air travel to many consumers, these issues are still relevant.

- **How will the federal government's support of small community air service be affected?** The Congress has long recognized that many small communities have difficulty attracting and maintaining scheduled air service. Now, as airlines continue to reduce capacity, small communities will potentially see even further reductions in service. This will increase the pressure on the federal government to preserve and enhance air service to these communities. There are two main programs that provide federal assistance to small communities: the Essential Air Service (EAS) program, which provides subsidies to commercial air carriers to serve the nation's smallest communities, and the Small Community Air Service Development Pilot Program, which provides grants to small communities to enhance their air service.[17]

  As we reported in August, the number of communities that qualify for EAS-subsidized service has grown over the last year, and there are clear indications that that number will continue to grow. Federal awards under the program have increased from just over $40 million in 1999 to an estimated $97 million in fiscal year 2002.[18] As carriers continue to drop service in some markets, more communities will become eligible for subsidized EAS service.

  In 2002, nearly 180 communities requested over $142.5 million in grants under the Small Community Air Service Development Pilot Program. DOT awarded the total $20 million available to 40 communities in 38 states to assist them in developing or enhancing their air service. The grants will be used for a variety of programs,

**Summary of Network and Low-fare Airlines' Financial Condition, 2000–June 2002**

| *Network carriers* | *Net income (loss) 2000* | *Net income (loss) 2001* | *Net income (loss) 2002:2Q* |
|---|---|---|---|
| Alaska | ($70,300,000) | ($39,500,000) | ($4,500,000)[a] |
| America West | $7,679,000 | ($147,871,000) | ($366,759,000)[b] |
| American | $813,000,000 | ($1,762,000,000) | ($1,070,000,000)[c] |
| Continental | $342,000,000 | ($95,000,000) | ($305,000,000) |
| Delta | $897,000,000 | ($1,027,000,000) | ($583,000,000) |
| Northwest | $256,000,000 | ($423,000,000) | ($264,000,000) |
| United | $50,000,000 | ($2,145,000,000) | ($850,000,000)[d] |
| US Airways | ($269,000,000) | ($2,117,000,000) | ($517,000,000)[e] |
| **Total** | **$2,026,379,000** | **($7,756,371,000)** | **($3,960,259,000)** |
| *Low-fare carriers* | *Net income (loss) 2000* | *Net income (loss) 2001* | *Net income (loss) 2002:2Q* |
| AirTran | $47,436,000 | ($2,757,000) | $2,027,000[f] |
| American Trans Air | ($15,699,000) | ($81,885,000) | ($53,518,000)[g] |
| Frontier(8) | $54,868,000 | $16,550,000 | ($2,935,572) |
| JetBlue | - | - | $27,590,000[h] |
| Southwest | $603,093,000 | $511,147,000 | $123,683,000 |
| Vanguard | ($26,031,626) | ($30,914,459) | ($7,963,262)[i] |
| **Total** | **$663,666,374** | **$412,140,541** | **$88,883,166** |

*Source:* Airline annual reports and SEC filings.

*Notes:* Unless otherwise stated, 2002:Q2 data is for six (6) months ended 6/30/02. Spirit Airline's data is unavailable as it is a privately held concern.

[a] Three (3) months ended 6/30/02. Alaska Air Group, Inc.

[b] America West Holdings Corp.

[c] AMR Corporation.

[d] UAL Corporation.

[e] US Airways Group.

[f] AirTran Holdings, Inc.

[g] ATA Holdings, Inc. and subsidiaries. Formerly Amtran, Inc.

[h] Data reflects Frontier FY 2001 ended 3/31/01; FY 2002 ended 3/31/02; FY 2003:1Q three (3) months ended 6/30/02.

[i] JetBlue Airways Corporation went public on 4/11/2002.

[j] Three (3) months ended 3/31/02. Filed Chapter 11 on 7/30/02.

**Summary of Network and Low-fare Carrier Enplanements, 2000–2002 (January to May)**

| *Network carriers* | *2000* | *2001* | *Percentage change (2000–2001)* | *2002 (Jan to May)* | *2001 (Jan to May)* | *Percentage change (Jan to May 2001–2002)* |
|---|---|---|---|---|---|---|
| Alaska | 12,841,367 | 13,241,705 | 3.1% | 5,067,518 | 5,570,751 | –9.0% |
| America West | 19,989,290 | 19,432,305 | –2.8% | 7,506,559 | 8,484,761 | –11.5% |
| American | 69,431,436 | 62,661,131 | –9.8% | 31,772,755 | 27,156,822 | 17.0% |
| Continental | 37,118,040 | 35,085,749 | –5.5% | 13,445,688 | 15,311,743 | –12.2% |
| Delta | 100,389,816 | 88,928,779 | –11.4% | 34,372,033 | 38,791,329 | –11.4% |
| Northwest | 49,464,897 | 45,570,838 | –7.9% | 17,328,913 | 19,515,133 | –11.2% |
| United | 73,757,167 | 65,259,307 | –11.5% | 22,852,094 | 28,424,896 | –19.6% |
| US Airways | 58,035,050 | 53,806,153 | –7.3% | 19,428,304 | 24,287,301 | –20.0% |
| *Low-fare carriers* | *2000* | *2001* | *Percentage change (2000–2001)* | *2002 (Jan to May)* | *2001 (Jan to May)* | *Percentage change (Jan to May 2001–2002)* |
| AirTran | 8,014,274 | 8,306,772 | 3.6% | 3,868,744 | 3,661,883 | 5.6% |
| American Trans Air | 6,183,661 | 6,856,076 | 10.9% | 3,056,609 | 2,938,045 | 4.0% |
| Frontier | 3,065,564 | 2,907,611 | –5.2% | 1,468,583 | 1,329,633 | 10.5% |
| JetBlue | 1,147,761 | 3,118,096 | 171.7% | 2,055,962 | 1,131,841 | 81.6% |
| Southwest | 82,170,284 | 82,234,829 | 0.1% | 32,570,332 | 34,679,716 | –6.1% |
| Spirit | 2,817,734 | 3,290,277 | 16.8% | 1,443,537 | 1,537,719 | –6.1% |
| Vanguard | 1,880,257 | 1,421,062 | –24.4% | 664,479 | 587,492 | 13.1% |

*Source:* GAO analysis of data from BACK Aviation Solutions.

including financial incentives to carriers to encourage either new or expanded air service, marketing campaigns to educate travelers about local air service, and support of alternative transportation. We are currently studying efforts to enhance air service in small communities, and expect to report on these programs early next year.

- **How will future international developments affect established agreements between the US and EU member states?** There are a number of international issues that will influence the domestic aviation industry's attempts to recover from financial losses. The European Court of Justice is expected to reach a decision in the near future on the authority of individual European Union nations to negotiate bilateral agreements. This could raise uncertainties over the status of "open skies" agreements[19] that the United States has signed with individual European Union nations. This is especially critical with regard to negotiating an open skies agreement with the United Kingdom, our largest aviation trading partner overseas. Because almost all of the major U.S. carriers partner with European airlines in worldwide alliances, this decision could potentially impact the status of antitrust immunity for these alliances, which could in turn affect alliances established with airlines serving the Pacific Rim or Latin America. These alliances are key components of several major airlines' networks and as such significantly affect their overall financial status. Various studies have illustrated the benefits to both consumers and carriers that flow from liberalizing aviation trade through "open skies" agreements between the United States and other countries.

This concludes my statement. I would be pleased to answer any questions you or other members of the Committee might have.

## CONTACT AND ACKNOWLEDGEMENT

For further information on this testimony, please contract JayEtta Hecker at (202) 512–2834. Individuals making key contributions to this testimony included Triana Bash, Carmen Donohue, Janet Frisch, Patty Hsieh, Steve Martin, Tim Schindler, Sharon Silas, Pamela Vines, and Alwynne Wilbur.

## NOTES

1. Commercial Aviation: A Framework for Considering Federal Financial Assistance (GAO-01–1163T), September 20, 2001.

2. P.L. 107–42.

3. See list of related GAO products attached to this statement.

4. In general, "code sharing" refers to the practice of airlines applying their names—and selling tickets via reservation systems—to flights operated by other carriers.

5. For the purpose of this report, major airlines include Alaska Airlines, America West Airlines, American Airlines, American Trans Air, Continental Airlines, Delta Air Lines, Northwest Airlines, Southwest Airlines, United Airlines, and US Airways.

6. The Air Transportation Stabilization Board is composed of the Chairman of the Federal Reserve, the Secretary of Transportation, the Secretary of Treasury, and the Comptroller General. The Comptroller General is a non-voting member.

7. The Air Transportation Safety and System Stabilization Act (Title III) authorized the Secretary of the Treasury to change the due date for any tax payment due between September 10 and November 15 to some time after November 15 (with January 15, 2002 as the maximum extension). The act specifies taxes that may be postponed to include excise and payroll taxes. Under Title II (Aviation Insurance), the act also authorized DOT to reimburse qualifying air carriers for insurance increases experienced after the events of September 11th for up to 180 days. Funding constraints effectively limited the program to reimbursing carriers their excess war risk insurance premiums for only 30 days.

8. The federal government has provided significant amounts of financial assistance under the Stabilization Act. First, according to data from DOT, as of September 18, 2002, 396 passenger and cargo carriers had received payments totaling $4.6 billion. Second, 16 carriers submitted applications for loan guarantees. The Board approved a loan of $429 million to America West Airlines, and conditionally approved the applications of US Airways, Inc. for a federal guarantee of $900 million and American Trans Air for a federal guarantee of $148.5 million. The Board has denied the applications of four airlines. Third, various airlines have taken advantage of the tax deferment. For example, Southwest stated that it deferred approximately $186 million in tax payments until January 2002. Finally, the Federal Aviation Administration provided reimbursements to air carriers for up to 30 days of increased war risk insurance expense. To date, 188 air carriers have received $56.9 million in reimbursements. We are completing reviews of the $5 billion financial assistance program and the War Risk Insurance Reimbursement program to ensure that payments made were in compliance with the act.

9. Network carriers are defined as carriers using a hub and spoke system. Under this system, airlines bring passengers from a large number of "spoke" cities to one central location (the hub) and redistribute these passengers to connecting flights headed to passengers' final destinations. We adopted DOT's definition of low-fare carriers, which includes AirTran, American Trans Air, Frontier, JetBlue, Southwest, Spirit, and Vanguard.

10. "Enplanements" represents the total number of passengers boarding an aircraft. Thus, for example, a passenger that must make a single connection between his or her origin and destination counts as two enplaned passengers because he or she boarded two separate flights.

11. The amount that the industry paid for security in 2000 is in question. ATA's $1 billion estimate, made in August 2001, included $462 million annually for direct costs, $50 million for security technology and training costs, and $110 for acquisition of security equipment. Since then, ATA certified that the industry incurred only about $300 million in security-related costs. The amount is important, because the airlines are required to remit an amount equal to the security costs incurred by the airlines in calendar year 2000 to the U.S. government, which assumed certain civil aviation security functions through the Transportation Security Administration. DOT's Inspector General is examining the discrepancy between the $1 billion and the $300 million estimates.

12. Under 49 USC 41734, carriers must file a notice with DOT of their intent to suspend service, and DOT is compelled by statute to require those carriers to continue serving those communities for a 90-day period.

13. The EAS program, established as part of the Airline Deregulation Act of 1978, guaranteed that communities served by air carriers before deregulation would continue to receive a certain level of scheduled air service, with special provisions for

Alaskan communities. As of July 1, 2002, the EAS program provided subsidies to air carriers to serve 114 communities.

14. DOT is authorized under 49 U.S.C. 41712 to block the airlines from implementing their agreements, if it determines that the agreements' implementation would be an unfair or deceptive practice or unfair method of competition. Such a determination is analogous to the review of major mergers and acquisitions conducted by the Justice Department and the Federal Trade Commission under the Hart-Scott-Rodino Act, 15 U.S.C. 18a.

15. *Airline Competition: Issues Raised by Consolidation Proposals* (GAO-01–402T), February 7, 2001.

16. GAO has recently initiated an analysis of issues relating to airline industry labor-management relations conducted under the Railway Labor Act.

17. Congress created the Small Community Air Service Development Pilot Program under the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (P.L. 106–181). That act authorized $75 million over 3 years. DOT made no awards under the act in fiscal year 2001, because the Congress did not appropriate any funds for the first year of the program but $20 million was appropriated for fiscal year 2002.

18. Figures in constant 2002 dollars.

19. "Open skies" agreements are bilateral air service agreements that remove the vast majority of restrictions on how the airlines of the two countries signing the agreement may operate between, behind, and beyond gateways in their respective territories. DOT has successfully negotiated open skies agreements with 56 governments, including many in Europe.

*This page intentionally left blank*

# Index

*This page intentionally left blank*

# About the Editor and Contributors

ANDREW R. THOMAS is assistant professor of marketing and international business and associate director of the Taylor Institute for Direct Marketing at the University of Akron. He is founding editor-in-chief of the *Journal of Transportation Security*, the first peer-reviewed journal dedicated to the study and practice of this critical business component. A *New York Times* best-selling writer, Dr. Thomas is author, coauthor, or editor of:

- *Supply Chain Security and Innovation*
- *The Distribution Trap!*
- *Global Manifest Destiny: Growing Your Business in a Borderless Economy*
- *Direct Marketing in Action: Proven Strategies for Finding and Keeping Your Best Customers*
- *The New World Marketing*
- *Growing Your Business in Emerging Markets: Promise and Perils*
- *The Rise of Women Entrepreneurs: People, Processes, and Global Trends*
- *Defining the Really Great Boss*
- *Managing by Accountability: What Every Leader Needs to Know about Responsibility, Integrity—and Results*
- *Change or Die! How to Transform Your Organization from the Inside Out*
- *Aviation Security Management*
- *Aviation Insecurity: The New Challenges of Air Travel*
- *Air Rage: Crisis in the Skies*

Dr. Thomas has published articles in leading management journals such as *MIT Sloan Management Review*, *Business Horizons*, and *Marketing Management*.

He is a regularly featured analyst for BBC, UNIVISION, FOX NEWS, and CNBC. He has been interviewed by more than 800 television and radio stations around the world. A successful global entrepreneur, Professor Thomas has traveled to and done business in more than 120 countries on all seven continents.

GARY E. ELPHINSTONE, contributor to this volume and adviser to the editor, is currently managing director of AVSEC AusAsia Pty Ltd., an international aviation security consultancy. Elphinstone's distinguished career in aviation began with the Royal Australian Air Force, where he specialized in signals intelligence and communications. During his service, he was promoted to serve at the British GCHQ, Hong Kong, for two and half years and, later, served as a fully rated flight services officer with the then Australian Department of Civil Aviation (DCA), working out of Sydney International Airport, Airways Operations. This was followed by an engagement with NASA at the deep space tracking station DSS 42, participating as electronics communications technician in a support role for the Apollo missions 8–13 and other NASA Deep Space Network programs. He rejoined the Federal Department of Aviation's Security Branch in 1978 and subsequently was chosen for an assignment with ICAO (the International Civil Aviation Organization) as aviation security adviser team leader with the aviation security project team, based in Thailand. The ICAO project (RAS 087/003) provided assistance to some 23 countries with the purpose of enhancing the capabilities of governments in the region to minimize acts of unlawful interference against civil aviation. This was the forerunner to the current ICAO USAP (Universal Security Audit Programme). Elphinstone retired from government service in 1997 as superintendent AVSEC Western Region, after 19 years. He resides with his family in Perth, Australia.

MOSES A. "MOE" ALEMÁN has over 55 years of professional experience in the investigations and security field, with over 35 of those years in civil aviation security. His professional experience consists of 8 years as a special agent, OSI (IG) USAF (1952–60); 4 years 3 months as Special Agent, FBI, U.S. Dept. of Justice (1960–64); 7 years 6 months as chief investigator, General Dynamics Corp. (1965–72); 22 years 3 months as aviation security specialist, FAA U.S. Dept. of Transportation (1972–95); and 13 years as owner and president of AVSEC, Inc., an aviation security consulting firm (1995–present). During his FAA career, Alemán was detailed on numerous occasions to the International Civil Aviation Organization (ICAO), during which time he directed or provided aviation security technical assistance expertise to member states of ICAO, serving as an aviation security advisor to the governments of over 50 countries in English or in Spanish. He was detailed as coordinator of an ICAO Regional AVSEC Project in the Asia/Pacific Region, based in Bangkok, Thailand, supervising four specialists in providing technical assistance to 23 nations (1987–89) and also served as section chief of the ICAO AVSEC Mechanism (1990–92) in Montreal, an initiative that resulted from the bombing of Pan Am

Flight 103 over Lockerbie, Scotland, in 1988. Since his retirement from the U.S. government, Mr. Alemán has served as a consultant or training instructor in 30 countries, most recently for ICAO, IATA, U.S. embassies in Mexico and the Dominican Republic, the Boeing Service Co., and projects funded by the Inter-American Development Bank (IDB) and by the Japan International Cooperation Agency (JICA). He also has provided AVSEC Quality Control Training sponsored by TSA and TDA of the United States under contract to Aerospace Services International (ASI) and in Colombia under contract to the International Aviation Services Group (IASG). From 2000 to 2007, Mr. Alemán conducted 63 aviation security training courses, in either English or Spanish, in 19 member nations of ICAO.

STEPHEN E. ATKINS is a professor at Texas A&M University. He is a librarian/historian working at the Cushing Library and teaching in the Texas A&M University History Department. His specialty is extremism and terrorism. His *Encyclopedia of American Extremism and Extremist Groups* (2002), and *Encyclopedia of Worldwide Extremism and Extremist Groups* (2004) have won honors. Dr. Atkins' next book, scheduled for release in the summer of 2008, is *Encyclopedia of 9/11.* He also has a contract for a book entitled *Holocaust Denial as an International Movement.*

JAMES J. F. FOREST is director of terrorism studies and associate professor in the Combating Terrorism Center at West Point. He has published over 10 books on terrorism, counterterrorism, homeland security, and other topics, including *Countering Terrorism and Insurgency in the 21st Century* (2007), *Teaching Terror* (2006), and *The Making of a Terrorist: Recruitment, Training and Root Causes* (2005). His research has also appeared in the *Cambridge Review of International Affairs*, the *Journal of Political Science Education*, and *Democracy and Security.* Dr. Forest holds degrees from Georgetown University, Stanford University, and Boston College.

G. TOM GEHANI is a senior business analyst for Target Corporation in its supply chain operations center at Target's headquarters in Minneapolis, Minnesota. He played a leading role in Target's pioneering initiative to develop and roll out a national supply network for frozen foods. He majored in economics at the University of Michigan at Ann Arbor, MI.

R. RAY GEHANI is the director of graduate programs in management of technology and innovation at the University of Akron. He is a fellow of the Fitzgerald Institute of Entrepreneurship and a fellow of the Center for Intellectual Property in its School of Law. His research and teaching interests are in global innovation strategies, and he has taught executive, graduate, and undergraduate classes in global supply chain management, production and operations management, strategic management, management of technology and innovation, and more. Dr. Gehani has earned two doctorate degrees, one in polymer science and technology from the Tokyo Institute of Technology in Japan, and the other in business from the Graduate Center of the City

University of New York. He is a past chairman of the Technology Management Section of the Institute of Operations Research and Management Science (INFORMS), and a lieutenant governor (education) for the Toastmasters International, Greater Cleveland Region. His research has been published in many scholarly journals such as the *International Journal of Production and Operations Management*, *Quality Progress*, *Long Range Planning*, *Academy of Management Executive*, *Global Focus*, *Management Decisions*, and many more. His seminal solo-authored book on *Management of Technology and Operations* was published in 1998 by John Wiley & Sons.

JOHN HARRISON is an assistant professor at the S. Rajaratnam School of International Studies and head of terrorism research at the International Center for Political Violence and Terrorism Research. He was also the coordinator for the Transportation Security Program at the Center for Excellence in National Security. He is one of the leading specialists on aviation security and has made presentations at many international conferences including the Supply Security Asia Conference, Singapore, the 2007 Malaysia American Studies Association 10th Anniversary Conference, Kuala Lumpur, 2006, the Harvard Program Asian International Relations Conference, Singapore, 2006, the 34th IAASP Annual Conference in Taipei in 2005, the EuroDefense Conference, Edinburgh, 2004, the Air Cargo Conference, Brussels, 2004, the International Society of Aviation Psychologists, Dayton, Ohio, 2003, and the Changing Face of Terrorism Conference in Singapore in 2003. His presentation at that conference, "The Changing Face of Aviation Terrorism," was later published in *The Changing Face of Terrorism*. He has briefed a wide range of government and private sector bodies. Harrison holds a PhD in international relations from St. Andrews University, and an MLitt in international security studies from St. Andrews, as well as an MA in political science from the American University in Washington, DC, and a BA in political science from Wheeling Jesuit University. He has also worked for and on various political campaigns in the United States and Scotland.

MOHAMMAD KARIMBOCUS is a member of the management team of the Air Traffic Management Division of the Department of Civil Aviation, Mauritius. He holds a degree in mathematics and a degree in transport, and he is a corporate member of the Chartered Institute of Logistics and Transport.

BARRY E. PRENTICE is a professor of supply chain management, at the I. H. Asper School of Business, University of Manitoba, and the former director (1996–2005) of the Transport Institute. His major research and teaching interests include logistics, transportation economics, urban transport, and trade policy. Dr. Prentice holds a degree in economics from the University of Western Ontario (1973) and graduate degrees in agricultural economics from the University of Guelph (1979) and the University of Manitoba (1986). Dr. Prentice has authored or coauthored more than 250 research reports, journal articles, and contributions to books. His scholarly work has

been recognized for excellence in national competitions and awards. In 1999, National Transportation Week named him "Manitoba Transportation Person of the Year." Through the Transport Institute, Dr. Prentice has organized national and international conferences on sustainable transportation ("Railways and the Environment"), supply chain logistics ("Planes, Trains and Ships"), agribusiness logistics ("Fields on Wheels"), and the potential use of airships for northern transportation ("Airships to the Arctic"). In 1999 and 2003, he received University of Manitoba outreach awards. Dr. Prentice was instrumental in founding a major in transportation and logistics within the BComm (Hons.) program at the I. H. Asper School of Business (fall 2003). Since that time, a new Department of Supply Chain Management has been formed, and plans are well advanced to commence a graduate program in supply chain management. Dr. Prentice has served on the boards of directors of several transportation organizations: the National Transportation Week (president, 2001 and 2003); the Canadian Institute for Traffic and Transportation (honorary president, 2001–3), and the Canadian Transportation Research Forum (past president, 1997). He is associate editor of the *Journal of Transportation Research Forum*. In addition, Dr. Prentice has served on the Winnipeg Airports Authority, Inc. (1998–2003), Winnipeg TransPlan 2010, the Mid-Continent International Trade Corridor Task Force, the Rapid Transit Task Force, and expert committees, and he is frequently asked to speak on the topics of trade and transportation.

MARY F. SCHIAVO. Throughout her distinguished career in law and public service, Mary Schiavo has held corporations, institutions, and the government accountable for their obligation to protect the safety and security of the traveling public. From 1990 to 1996, Schiavo served as the inspector general for the U.S. Department of Transportation. Under Schiavo's direction, she and her staff of over 400 employees secured more than 1,000 criminal convictions and uncovered billions of dollars of fraud, waste, and abuse of taxpayers' money at the U.S. DOT. She is the author of the *New York Times* bestseller, *Flying Blind, Flying Safe*, to which *Time* magazine devoted its cover and 12 pages of the magazine, and which exposed the poor safety and security practices of airlines and the failures of the federal government to properly police aviation. She also served as professor of aviation and public administration at the Ohio State University, prosecuted federal cases for the U.S. Department of Justice as an assistant U.S. attorney, and served as a prosecutor in the Organized Crime and Racketeering Strike Force. Schiavo received her pilot's license soon after her driver's license and completed private and commercial flight training at the Ohio State University. She is a cum laude graduate of Harvard University, and she earned a master's degree in public administration from the Ohio State University. Schiavo earned a juris doctorate from New York University and was a Root-Tilden Public Interest Law Scholar. At the Smithsonian Institution's Air and Space Museum in Washington, DC, Schiavo was honored with the 1996 Aviation Laurel Award for her

many years of work to combat bogus aircraft parts. The following year, she was inducted into the Aviation Laurel Hall of Fame, also at the Smithsonian Institution. After leaving the Transportation Department, Schiavo joined the international plaintiffs' powerhouse law firm, Motley Rice, where she leads the aviation team. She represented passenger and crew families in every major U.S. air crash and in many foreign crashes. She represents clients in all major aviation-related litigation, including family members of the passengers and crew aboard the four planes hijacked on September 11, 2001. Besides passengers, she also represents pilots and flight attendants. Recognized by television audiences worldwide, Schiavo has served as an on-air consultant for NBC and ABC news and frequently appears on Fox, CNN, CBS, the History and Discovery Channels, and the BBC. She was a White House fellow, assistant secretary of labor, and a special assistant to the U.S. attorney general, and as a million-mile frequent flier, she cares deeply and personally about aviation safety and security.

# Aviation Security Management

# Aviation Security Management

## Volume 2

## The Elements of Aviation Security Management

Edited by
Andrew R. Thomas

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

**Library of Congress Cataloging-in-Publication Data**

Aviation security management / edited by Andrew R. Thomas.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978–0–313–34652–1 ((set) : alk. paper)
ISBN-13: 978–0–313–34654–5 ((vol. 1) : alk. paper)
ISBN-13: 978–0–313–34656–9 ((vol. 2) : alk. paper)
ISBN-13: 978–0–313–34658–3 ((vol. 3) : alk. paper)
1. Airlines—Security measures. I. Thomas, Andrew R.
HE9776.A95 2008
363.28'76068—dc22 2008018728

British Library Cataloguing in Publication Data is available.



Library of Congress Catalog Card Number: 2008018728

ISBN-13: 978–0–313–34652–1 (set)
978–0–313–34654–5 (vol. 1)
978–0–313–34656–9 (vol. 2)
978–0–313–34658–3 (vol. 3)

First published in 2008

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the United States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48–1984).

10 9 8 7 6 5 4 3 2 1

# Contents

# Preface

Because of September 11, 2001, there is an almost universal recognition that aviation security is a deadly serious business. Yet, still, today around the world, the practice of aviation security is rooted in a hodgepodge of governmental rules, industry traditions, and local idiosyncrasies. In fact, seven years after the largest single attack involving the air transport industry, there remains no viable framework in place to lift aviation security practice out of the mish-mash that currently exists. The purpose of this three-volume set is to begin to change that. It is my sincere hope that this work, written from a truly global point of view, will be the first of many on this most important topic.

The fact that over half of the contributors to this set come from outside of the United States is no coincidence. Although roughly 40 percent of all air transport today takes place within the United States, the long-term trend is for dramatic increases in global system usage, driven by high-growth emerging markets like China, India, Russia, and Brazil. It is widely estimated that the total volume of passengers and cargo moved via the international air transport system will nearly triple in the next 25 years. Although America will remain the single largest player, the surge will come from emerging markets.

This evolving reality mandates that aviation security management be viewed not merely on a country by country basis but as a global endeavor, where best practices—regardless of where they originate—are integrated into a new paradigm that is truly global in scope and scale. With that in mind, *Aviation Security Management* is intended to serve as a foundation for researchers, practitioners, and educators around the world who are looking to develop new knowledge and pass it along to the next generation of aviation security managers.

Dishearteningly, however, there is only a handful of academic programs—currently less than a dozen—where someone can actually study transportation security management. The number of schools where an aviation security management curriculum is available is even smaller. Such a lack of educational opportunities means that unless something is done quickly, the tens of thousands of new aviation security mangers who will join the profession in the coming years will not have had the opportunity to learn the best in transportation security management research and practice.

To professionalize the field of transportation security management, in general, and aviation security management, in particular, several requirements need to be met. First and foremost, there must be a body of knowledge and a repertoire of behaviors and skills needed in the practice of the profession, knowledge, behavior, and skills that are not normally possessed by the nonprofessional. To date, very little of that body of knowledge and repertoire exists in a clear and cogent format. While many researchers and practitioners across multiple disciplines have been engaged in their own worthwhile pursuits, there remains a deficiency in the availability of clearinghouses for that knowledge. Bluntly asked, where does one go to learn about the emerging ideas, thoughts, technologies, and best practices in transportation and aviation security management?

Clearly there is neither the need nor the desire to provide those who seek to harm transportation networks with information they can use against us. As researchers, practitioners, and educators, we must be ever vigilant, striving to balance the need for open knowledge with the necessary parameters of sensitive information. I am certain we can do both—that is, provide cutting-edge knowledge to a growing body of well-intentioned researchers and practitioners while maintaining the integrity needed to ultimately make transportation more secure.

Which brings us back to those clearinghouses. This set of volumes and the recently founded *Journal of Transportation Security* are intended to be some of the first building blocks of a much more extensive foundation, which will ultimately serve to prepare for the arrival of a true profession: transportation security management.

The second volume in this set delves into several of the emerging issues that are impacting aviation security managers and will continue to do so in the future. It almost goes without saying that aviation is a business, with various stakeholders, many of which are driven by purely financial motives. Cletus C. Coughlin, Jeffrey P. Cohen and Sarosh R. Kahn review the economic issues posed by aviation security and terrorism.

Because of its global aspects, aviation brings together disparate groups. How these groups interface with each other, especially when it comes to security, has long been a question for researchers and managers. Borrowing from the world of sociology, AnneMarie Scarisbrick-Hauser and William J. Hauser put forward the concept of convergence as providing a way for people to come together in pursuing effective aviation security management techniques.

In past years, many felt that passengers were left out of the discussion as to what is enough security. Noted attorney, author, and researcher Kathleen Sweet explores the often contentious relationship between passengers and their rights and aviation security measures. In the following chapter, the same author looks at how aviation security and response management might operate in concert.

Although the overwhelming focus of this set of volumes is on commercial aviation security, the role of general aviation in the security calculus cannot be overlooked. James Jay Carafano notes both the challenges and the responses faced by general aviation in the realm of security management since September 11.

Like other stakeholders, airports around the world have confronted the reality of the post–September 11 environment in a myriad of ways. David Jarach and Fulvio Fassone look at the hard decisions that had to be made and what the future holds for the historically crucial component of airport retailing.

The threats posed to transportation networks are human. The solutions, therefore, must be human ones, aided by new technology, not the other way around. Training is not sexy, nor it is glamorous. However, it must drive the human component of the security equation. This is the foundation of a true risk-based approach. Mark B. Salter explores the human component as it relates to passenger screening.

Central to the study of management is the role of operations systems and research applications. A team of researchers from University of Illinois–Champaign, led by Sheldon H. Jacobson, along with John J. Nestor of the Transportation Security Administration, investigate the integration of operations systems with aviation security management.

The state of the security of the millions of tons cargo that are moved around the world using civil aviation is discussed by Erik Hoffer, a longtime leader in the cargo security field.

A study of the selection and preemployment assessment of aviation security screeners is undertaken by Diana Hardmeier and Adrian Schwaninger.

Finally, noted photo essayist Ross Rudesch Harley takes us on a journey through airport terminals, reminding us of the scope and magnitude of the system we are trying to protect.

The two appendices contain reports from the U.S. Government Accountability Office. One focuses on how vulnerabilities in the security systems were exposed through covert testing of TSA's passenger screening processes, and the other looks at efforts to secure U.S.-bound air cargo and areas where security could be strengthened.

*Andrew R. Thomas, University of Akron*
*Editor*

*This page intentionally left blank*

# CHAPTER 1

# Aviation Security and Terrorism: A Review of the Economic Issues

*Cletus C. Coughlin, Jeffrey P. Cohen, and Sarosh R. Khan*

> Protecting this system demands a high level of vigilance because a single lapse in aviation security can result in hundreds of deaths, destroy equipment worth hundreds of millions of dollars, and have immeasurable negative impacts on the economy and the public's confidence in air travel.
>
> —Gerald L. Dillingham, United States General Accounting Office, in testimony before the Subcommittee on Aviation, Committee on Commerce, Science, and Transportation, U.S. Senate, April 6, 2000

The terrorist attacks exploiting weaknesses in U.S. aviation security on September 11, 2001, did indeed produce the catastrophic results identified in the prophetic testimony cited above.[1] Immediately, security issues rose to paramount importance in the nation's policy agenda.[2] Despite general agreement on what aviation security entails and the goals of the system, controversy abounds on how to regulate and provide this vital service.

If airplanes and passengers, as well as property and people on the ground, are to be protected, potential perpetrators of terrorism must be prevented from breaching security checkpoints and gaining access to "secure" airport areas and aircraft. Given the interconnectedness of the air transportation system, a sufficiently high level of security must be provided throughout the system. Flexibility to respond quickly to new information about security threats is a must. Moreover, incentives must exist for regulators and security providers so

A similar version of this article, without the appendix, was published in the *Federal Reserve Bank of St. Louis Review* 84, no. 5 (September/October 2002): 9–25. Note that this chapter refers to the situation in the months after the September 11 terrorist attacks.

that improvements can be devised and implemented. At the same time, the costs of providing security must be weighed against the benefits.

We examine the economic issues relevant to airline and airport security in the United States. Understanding these issues is crucial in evaluating the various methods of regulating and providing aviation security and for appraising the conflicting positions over the appropriate scope of governmental involvement.

We begin by highlighting key features of the airline industry, one of which is its network structure. Security at one airport can affect security elsewhere—an example of a network externality.[3] Next, we use elementary economics to show that unregulated private markets will likely provide too little aviation security, which sets the stage for examining the alternatives for regulating and providing aviation security. We review the Aviation and Transportation Security Act of 2001 and the characteristics of the resulting policy. A summary of major points completes the article.

## OVERVIEW OF THE AIRLINE INDUSTRY

Prior to September 11, 2001, the air transportation sector accounted for approximately 1 percent of U.S. employment. In 2000 there were 14 "major" certified carriers in the U.S. airline industry. Although our primary focus is on the passenger carriers, freight transport is a significant factor for several reasons. A security breach at any one airport will undoubtedly affect the smooth movement of freight through the network as well. Federal Express, one of the 14 major carriers, employed more workers than either American or United. Freight revenues overall comprise about 10 percent of total operating revenues for the major carriers, with operating revenues exceeding $20 million for each carrier. Finally, the recently passed legislation states that cargo and passengers will be screened.

### Airports and Airlines: The Hub and Spoke System

Airports are a crucial component of the infrastructure for the airline industry. The United States has over 18,000 airports, 3,304 of which are eligible for federal funding. Approximately 430 airports, designated as "primary" airports by the Federal Aviation Administration (FAA), handle virtually all scheduled passenger service in the United States.

Subsequent to the deregulation of the industry that was propelled by legislation in 1978, many of the major U.S. airlines developed a "hub and spoke" system. With this structure, passengers on airline flights from various remote airports (the nodes on the spokes) converge on a single airport (the hub). After providing time for passengers to make their connections by changing planes, they depart for their final destinations.

This hub and spoke system leads to interdependencies that give rise to externalities. Namely, delays at one node often cause additional delays

throughout the entire system. Thus, delays through one particular city due to security breaches can cause further delays at other nodes. For example, after a security breach at Hartsfield International Airport, the *Atlanta Journal-Constitution* reported: "Hundreds of flights around the country were canceled or delayed . . . [and] dozens of planes heading to Atlanta were diverted to other airports."[4] Thus, by reducing travel delays throughout the system, improvements in security screening at a single airport can be viewed as a good with spillover benefits. Furthermore, security improvements at one node can result in an increased feeling of safety perceived by passengers at other nodes. In fact, this additional safety can accrue to those who are not even traveling, such as individuals who work in any potential target of an airline terrorist attack.

### September 11 and Airline Passenger Travel

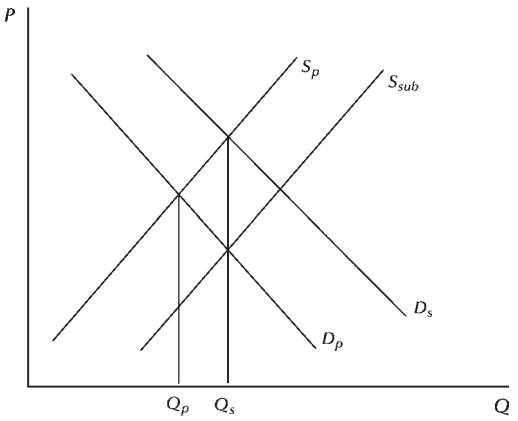
The events of September 11 curtailed airline travel in various ways. First, these events reduced the demand for air travel as a result of the increased safety concerns. Second, these events reduced air travel by exacerbating the recession that began in March 2001. Third, the cost of travel was effectively increased because of the necessity of arriving earlier for departures, the increased frequency of delays resulting from security breaches, and new security surcharges.

During September 2001, revenue passenger miles declined more than 30 percent from the previous September. Despite some recovery during the fourth quarter of 2001, revenue passenger miles were down 15 percent year-over-year in December 2001. For the first five months in 2002, revenue passenger miles were 10 percent below the level in 2001. What is unclear is how long this shock will continue to affect passenger travel. A major uncertainty is the effect of the new security environment.[5]

## PROVIDING THE RIGHT AMOUNT OF AVIATION SECURITY—IN THEORY

Unregulated private markets are unlikely to provide adequate aviation security. We can illustrate this claim by using a supply and demand diagram. Assume that, similar to the case in the United States prior to September 11, airlines are ultimately responsible for aviation security. Assume further that consumers of airline services have a demand for security represented by the demand curve, $D_p$, in Figure 1.1.[6] The negative slope reflects the fact that, as the price of aviation security declines, the quantity of security that consumers desire increases. This demand curve reflects the marginal private benefits of aviation security. The supply curve is represented by $S_p$. The positive slope indicates that increases in security can be provided only by incurring higher per-unit costs. The intersection of these curves generates the quantity of this good, $Q_p$, that is likely provided in equilibrium by private markets. This quantity, however, is unlikely to be the optimal (or efficient) amount of security.[7]

**Figure 1.1**
**Optimal Quality of Aviation Security**




The primary reason for underprovision is that there are important benefits from aviation security that extend beyond the passengers on a flight. Occupants of high-rise buildings as well as those occupying other potential targets for terrorist acts (e.g., nuclear power plants and government buildings) can benefit and, in fact, the benefits can extend beyond those individuals to their families and much further. When positive externalities, also termed spillover benefits, exist, then the social demand for aviation security diverges from the private demand. This social demand encompasses the private demand plus the demand of those who benefit but are not flying. This demand curve, $D_s$, lies above and to the right of the private demand. The intersection of this demand curve and the supply curve determines the efficient quantity of aviation security. As Figure 1.1 shows, this quantity, $Q_s$, exceeds the quantity that would be provided by private markets.

An important issue is how to induce an increase in security from $Q_p$ to $Q_s$, which leads to questions about the potential role of government—government regulation, provision, and subsidies are all possibilities.[8] Figure 1.1 also illustrates the effect of a subsidy. A subsidy effectively lowers the cost per unit of security and, thus, can be represented by a downward (rightward) shift of the supply curve. Assuming the optimal subsidy is provided, this new supply curve, $S_{sub}$, intersects $D_p$ at the point where the quantity of security is the socially desirable amount, $Q_s$. However, if the optimal subsidy is not provided, then either too little or too much security is possible.

## AVIATION SECURITY PRIOR TO SEPTEMBER 11

Historically, aviation security has been provided jointly by airlines, airports, and the FAA. Generally speaking, providing security has been the responsibility

of air carriers and airports. Government, via the FAA, performed primarily a regulatory role.

The airlines were responsible for passenger and baggage screening. The usual practice was for airlines to contract with private companies who provided screeners at security checkpoints. The airlines were also responsible for security from the screening checkpoints to the aircraft. Airports were responsible for law enforcement and general security in the airport vicinity, including exterior areas, parking areas, the airport perimeter, and interior areas up to the security checkpoints. The airports also hired law enforcement officers for the security checkpoints. The FAA was responsible for providing threat information; establishing security policies, regulations, and protocols; conducting security audits of airlines and airports; supporting research and development of security technology; and overseeing the installation of security equipment.

## Aviation Security Issues

Studies and legislation throughout the 1990s identified problems with aviation security and attempted to improve it.[9] The bombing of Pan Am Flight 103 led to the passage of the Aviation Security Improvement Act of 1990, which raised employment, education, and training standards for security personnel. In 1996, the crash of TWA Flight 800 led to the creation of the White House Commission on Aviation Safety and Security. This group recommended new screening technologies and equipment as well as the development of uniform performance standards for training and testing screeners. Congress also passed legislation—the Federal Aviation Reauthorization Act of 1996 and the Omnibus Consolidated Appropriations Act of 1997—that provided funding for implementing many of the commission's recommendations. Over the four years prior to 2000, Congress provided the FAA with $1 billion for security. Roughly one-third of this funding was for the purchase and deployment of security equipment at airports. Finally, the Airport Security Improvement Act of 2000 required additional security actions.

The preceding studies and legislation highlighted numerous problems with aviation security. Problems existed in three major areas: computer security; access to aircraft, airfields, and other facilities; and the detection of dangerous objects.

With respect to computer security, two major problems were well known. One problem involved the physical security at facilities housing air traffic control systems. A Government Accounting (now Accountability) Office (GAO) study reported in 1998 that most facilities (87 of 90) had not performed threat analyses for the air traffic control systems in the five years prior to the review.[10] A second problem involved the management of computer systems. As of December 1999, the FAA was violating its security requirements by failing to conduct background searches on contractor employees who were reviewing and repairing critical computer system software. These employees

possess critical knowledge that could prove useful for computer hackers. If hackers were to penetrate the air traffic control system, they could attack the computer systems used to communicate with and control aircraft.

With respect to access to aircraft, airfields, and other facilities, controls for limiting access to secure areas had not worked as intended. Tests during 1998 and 1999 revealed that the inspector general's staff of the Department of Transportation successfully gained access to secure areas 68 percent of the time. These results stimulated improvements; however, additional testing between December 1999 and March 2000 revealed a rate of unlawful access of 30 percent.

The problem area that has attracted the most attention involves the detection of dangerous objects. An increase in hijackings prior to 1972 led to passenger-screening requirements. The goal was to identify passengers carrying metallic weapons that could be used to hijack an airplane. With respect to passenger screening, personnel issues have received the most attention because screeners are not adequately detecting dangerous objects. Three reasons have been provided for this poor performance: inattention to training, high turnover, and low pay.

The previously cited GAO report revealed that the FAA was two years behind schedule in issuing a regulation implementing a congressional mandate to certify screening companies and improve the training and testing of screeners. All passengers and their carry-on baggage must be checked for weapons, explosives, or other dangerous articles. Until recent legislation, the FAA and air carriers shared this responsibility. The FAA set the screening regulations and established the standards for the screeners, the equipment, and the procedures to be used, while the air carriers were responsible for screening passengers and their baggage prior to their entry into secure areas or onto an aircraft. Generally, air carriers hired security companies to do the screening.

Concerns about the effectiveness of screeners have existed for many years. A GAO report noted that, in 1978, screeners were not detecting 13 percent of potentially dangerous objects that FAA agents carried through checkpoints during tests.[11] In 1987, tests revealed that 20 percent of potentially dangerous objects were passing undetected through checkpoints. Despite features of the Federal Aviation Reauthorization Act of 1996 that attempted to increase the effectiveness of screeners, testimony by a GAO official stated that performance remained a problem.[12] Based on the FAA's test results, the GAO official concluded that screeners' ability to detect dangerous objects was not improving and, in some cases, was deteriorating.

High turnover of security personnel is a well-known problem. From May 1998 through April 1999, turnover averaged 126 percent at 19 large airports. Skilled and experienced screeners are rare. High turnover is attributed to low wages, low benefits, and job stress.

In addition, some human factors contribute to poor performance. Screening requires repetitive tasks and intense monitoring for the very rare event when a dangerous object might be observed. To improve performance, the

FAA began a number of programs, including establishing a threat image projection system to keep screeners alert and to monitor their performance; a screening company certification program; and screener selection tests, computer-based training, and readiness tests. However, the GAO found that the FAA's implementation was behind schedule.

### Technology Issues

In addition to the personnel issues involved in detecting dangerous objects, there are technology issues. The technical performance of existing machines might not be adequate to detect dangerous objects that do not contain metal. Atkinson argues that superior information technologies could and should be applied to increase aviation security.[13] At the same time, however, the consideration of technical solutions requires the consideration of many nontechnical issues that can affect whether the technology can be implemented successfully.

New scanning technology can do a better job than the existing machines that scan only for metal. Many security experts are pushing for the use of screening machines capable of detecting a broader range of metals and alloys, plastic explosives, and other materials.

Experts are also pushing for the increased use of biometrics. Biometrics technology uses unique biological data to identify and authenticate an individual almost instantaneously. Various biological data, such as fingerprints, facial geometry, hand geometry, retinas, and voice patterns, can provide the necessary information. Plus the technical application of biometrics to increase aviation security is reasonably straightforward. For example, after background checks, an employee, such as a pilot, could be issued a card with his unique biometric information embedded on a computer chip with encrypted software. Entrance to a secure area, such as the cockpit, would require the pilot to put his card in a slot and submit to a biometric identification process to ensure that the card and the person holding it match.

A similar procedure could be used for passengers. The screening could take place both prior to entering the gate concourses and upon entering the boarding ramp to the plane. The latter authentication would allow accurate passenger manifests in real time. This would enable airline personnel to identify individuals who have checked in, but not boarded. A related feature would allow airlines to match passengers with their luggage. Luggage for an unboarded passenger could be removed.

The use of sophisticated technology is not simply a technology issue. In assessing the costs and benefits of using new technology, various nontechnical issues arise. First, health issues arise because the use of a technology embedded in a machine, especially one that emits radiation, might harm some individuals. Even the perception that a machine might be dangerous could create adverse economic effects for the airline industry.

Second, the use of technology requires the consideration of legal and privacy issues. The technology could violate an individual's guarantee against

unreasonable searches. Even if the search is legal, some potential travelers might be deterred because they feel uncomfortable with some personal information no longer being private. Many are concerned about scans that produce images of their bodies.

Finally, the operation of machines raises space issues because of their size and the resulting lines of passengers. Moreover, airlines are concerned about maintaining their flight schedules and the inconveniences experienced by passengers. In certain cases, it is possible that the technology can assist airlines in meeting their schedules and increase passenger convenience.

## AVIATION SECURITY IN THE AFTERMATH OF SEPTEMBER 11

The events of September 11 forced public decision makers to examine how aviation security was being provided and how to improve it.[14] Generally speaking, three primary options for screening passengers and controlling access to secure areas were proposed before September 11, although shortly thereafter attention focused primarily on how to implement the third option listed below. For each option identified by the GAO,[15] an underlying assumption was that the FAA would continue to regulate screening, oversee performance, and impose penalties for poor performance. These security management and provision options are as follows:

1. continue with the responsibility assigned to air carriers but with new requirements,
2. assign the responsibility to airports, or
3. assign the responsibility to the federal government via creation of a new federal agency (for example, a new agency within the Department of Transportation) or a federal corporation (for example, a corporation similar to the Tennessee Valley Authority).

### Option One

The first option is the same as the pre–September 11 arrangement with the FAA promulgating new requirements. As we highlighted previously, unregulated private markets will likely provide too little aviation security. The events of September 11 indicated to many that even with regulation by the FAA, too little aviation security was being provided; however, the events do not necessarily eliminate this option.

Continuing with this option implies that this system is the best way to provide aviation security. One can argue that this option worked for a number of years. The pre–September 11 security arrangements date from the early 1970s and hijackings went down markedly after these arrangements were put in place. Obviously, the hijackings of September 11 occurred, but it is not clear that any option under consideration would have prevented them. It is

not clear that these hijackings would have been prevented if airport security personnel were federal employees rather than privately contracted personnel. In fact, federal rules as of September 11 would have allowed the hijackers' knives and box cutters on board because the blades were shorter than four inches. Thus, detection might not have mattered. Nor is it clear that a federal force would prevent potential hijackers from entering secure areas any better than a private force. Moreover, the shortcomings in the FAA performance cited previously justify some caution in providing more authority to a governmental body.

One can argue that the events of September 11 revealed only that the security threat was much greater than anticipated. Furthermore, one can argue that this underestimation of the threat was not the fault of the FAA, but rather of the intelligence community at large. Of course, apart from this failure to fully recognize the security threat, our prior discussion identifying specific security shortcomings revealed that this security management and provision option, while possibly the best, is far from ideal.

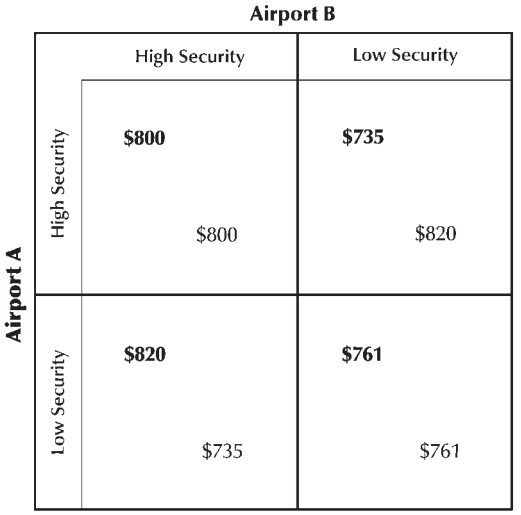
As mentioned previously, this option is utilized infrequently outside of the United States. Only 2 of 102 other countries with international airports had airlines handling the security function. The primary rationale for excluding airlines from the security function was the concern that airlines would focus unduly on lowering costs and providing passenger convenience and, therefore, shirk on providing safety.

### Option Two

The second option, which excludes airlines from the security function, involves assigning the security responsibilities to airports. A simple example using game theory can be used to model the network aspects of aviation security. Assume two airports—A and B—and two levels of aviation security—high and low. We can think of the high level of security as allowing air travelers to have more confidence that their flight will be safe than if a low level of security were provided. In other words, the higher level of security reduces the probability of successful terrorist attempts. Table 1.1 shows the hypothetical payoffs of each level of aviation security for each airport. For example, the payoffs for airports A and B when A provides low security and B provides high security are \$820 for A and \$735 for B.

The economics underlying the payoffs in Table 1.1 require some elaboration.[16] Assume that the profits (payoffs) of each airport are \$1000 prior to any security expenditures or any losses stemming from successful terrorist attacks. The expense of providing a high level of security is \$200, while the expense of providing a low level of security is \$50. Assume further that a successful act of terrorism imposes a cost of \$1300 at the airport where the act occurs. If both airports provide a high level of security, acts of terrorism are prevented. If one airport provides a high level of security and the other provides a low level, then a successful terrorist act can occur at either airport; a successful terrorist

**Table 1.1**
**A Game Theory Example of Airport Provision of Safety**




*Note:* Playoffs in bold are for Airport A.

act damaging the high-security airport would have emanated from the low-security airport. Assume that the probability of a successful terrorist act is 0.1 at an airport providing a low level of security and that the probability is 0.05 that the successful terrorist act, whose roots can be traced to the airport providing a low level of security, occurs at the other airport.

These assumptions produce the payoffs in Table 1.1. In the first arrangement, assume both airports provide a high level of security; both airports then receive a payoff of $800, which is simply $1000 less the $200 expense of providing a high level of security. There are no other cost calculations for this arrangement.

In the second arrangement, assume airport A provides a high level of security and airport B provides a low level of security. The payoff for airport A is $735: Starting from $1000, this airport incurs the $200 expense of providing a high level of security and an expected loss of $65. (The latter expense is the cost of a successful terrorist act [$1300] times the probability that it occurs at airport A [0.05]). Meanwhile, the payoff for airport B is $820: Starting from $1000, this airport incurs the $50 expense of providing a low level of security and an expected loss of $130. (The latter expense is the cost of a successful terrorist attack [$1300] times the probability that it occurs at airport B [0.1]). Thus, if one airport provides a high level of security and the other airport provides a low level of security, the payoff for the first airport is $735 and the payoff for the second airport is $820.

In the third arrangement, assume both airports provide a low level of security; they would each receive a payoff of $761. Starting from $1000, each airport incurs the $50 expense of providing a low level of security as well as two expected losses. The first is the $130 loss associated with a successful terrorist act occurring due to the airport's own low level of security and the second is a $59 loss ($65 times 0.9) due to the other airport's low level of security.

Given the preceding payoffs, what levels of security will likely be provided by the airports? Assuming that the airports make their security decisions simultaneously without communicating directly with each other, the answer is that both will provide the low level. Assume airport B thinks airport A will provide the high level. If so, then if airport B also provides the high level, the payoff for airport B is $800. If airport B provides the low level, the payoff for airport B is $820. Thus, airport B will choose the low level of security because it provides the larger payoff. What happens if airport B thinks airport A will provide the low level of security? Once again, airport B will choose to provide the low level of security because the payoff to airport B is larger with the low level of security (that is, $735 versus $761). Thus, regardless of what airport A chooses, airport B will choose the low level of security. By the same reasoning process, airport A will choose the low level of security regardless of airport B's choice.

The dominant strategy is for both airports to choose the low level of security. Note that the payoff for both airports is $761 and that such a payoff is inferior to the payoff of $800 to both airports if they had both chosen to provide the high level of security. Thus, when the airports choose their security level simultaneously without coordinating their decisions, there is a high probability that they will end up with lower security throughout the network. In addition, the airports will achieve lower payoffs than if they had coordinated their security decisions and jointly provided a high level of security.[17]

### Option Three

The conclusion, similar to that of the first option where airlines were responsible for security provision, is that in a world in which each airport is left to provide security on its own without governmental intervention, underprovision of aviation security is likely. Thus, regardless of whether airlines or airports provide security, a role for the federal government as a regulator should not be seen as a contentious issue. Instead, the major choice for policy makers is whether the federal government should contract out the provision of aviation security services or provide those services in-house. The former scenario entails some form of public-private partnership handling aviation security. This became the norm in Western Europe during the 1990s when countries privatized aviation security following security failures by government-run operations.[18] Under this scenario, the government sets the security standards and either assigns screening responsibilities to the airport authorities or hires firms directly. Regardless, the agent is held accountable for meeting the security standards.

Under this third policy option, the government is assigned full responsibility for providing security.

Economic theory highlights a number of considerations regarding this option relative to the first two options. The theory of fiscal federalism indicates the possibility of a tradeoff between (1) accounting for an externality by having a higher level of government involvement and (2) allowing residents in individual jurisdictions to choose the desired level of public service for their own community.[19] If the federal government were to take over the provision of security at an airport, then it would be able to account for the spillover benefits by providing a higher level of airport security. However, it might do so at the cost of preventing demand diversity from being satisfied at individual airports because the level of security is determined by the federal government. In many instances, individual communities might prefer less security at their airports than the level chosen by the federal government.

Economic theory also highlights a number of other potential problems with assigning security responsibilities to a federal agency. First, the public agency is a monopoly supplier. Similar to any monopolist, the public agency might not be forced by competitive pressures to ensure an efficient provision of services. In addition, because of civil service restrictions, the public agency might be faced with a labor environment that precludes efficient delivery of services.[20] Moreover, public agencies are frequently characterized as being slow in adjusting to changed circumstances and unlikely to innovate.[21]

Additional problems might arise because the public agency is likely judged primarily on its security record. Overprovision of aviation security is possible because government bureaucrats have an incentive to protect themselves from the damage that could result if too little security is provided. In this case, the agency will have an incentive to ignore the tradeoffs that occur between security and other attributes of air transportation services that consumers demand.[22] For example, the public agency might tend to underestimate the cost of waiting incurred by passengers when it determines whether to institute a specific security measure. Waiting is a cost that airlines are sensitive to because of their profit incentive. On the other hand, the lack of a profit incentive when security is provided by the government might lead public managers to consider extended waits as simply an unavoidable cost of travel.

Heightened security measures have already produced some examples of what could be viewed as security considerations taking precedence over other attributes of air transportation services demanded by consumers. However, one can also argue that the following examples are simply temporary costs associated with the transition to the new security environment.[23] Between October 30, 2001, and February 4, 2002, there were 35 airport terminal evacuations. Between October 30, 2001, and December 31, 2001, a total of 1,361 flights were delayed, with a cumulative delay time of 2,173 hours. During this period, 587 planes were stopped and evacuated.[24]

On the other hand, there are arguments supporting federal government provision of aviation security. First, the federal government can account for

the spillover benefits associated with the provision of aviation security in its production decision. Second, governmental provision might be preferable to privatization because, relatively speaking, the former limits the incentives of managers to reduce quality by cutting costs.[25] In other words, relative to managers in private firms, managers of a government operation have less incentive to reduce quality by cutting costs because of the relatively smaller financial gains for the public employees.

In the case of aviation security, a specific concern is that private providers hire unqualified personnel to minimize their costs. These attempts to cut costs undermine security throughout the air transportation network. Public provision tends to mitigate this problem. This advantage of public provision is likely more pronounced the more difficult it is to specify the quality of a service. Aviation security seems to be such a case.

## THE AVIATION AND TRANSPORTATION SECURITY ACT OF 2001

The Aviation and Transportation Security Act was signed into law (Public Law 107–71) on November 19, 2001, by President Bush. The act is a comprehensive approach to increasing aviation security. The objective of the act is to create, develop, and streamline security procedures and protocols that radically reduce the chances of any security breach or violation.

The Aviation and Transportation Security Act considerably alters the security responsibilities of airlines, airports, and the federal government. In the context of the options discussed previously, this legislation is the third option. A substantial increase in the resources committed to aviation security will occur as well.

The act establishes the Transportation Security Administration (TSA) in the Department of Transportation (DOT). The TSA is to be headed by the under secretary of transportation for security. As of February 17, 2002, the TSA assumed the civil aviation security functions and responsibilities of the FAA. In addition, the legislation identifies some new responsibilities. The responsibilities of this office include coordinating and directing aviation security at all times and all domestic transportation security in case of a national emergency.

The most controversial feature of the legislation is the requirement that the attorney general and the secretary of transportation develop a program that ensures the screening of all passengers and baggage for illegal and dangerous items. The attorney general is given the responsibility to develop a workforce of federal employees in accordance with the guidelines of the act. This workforce, which will be implemented as workers become qualified, is expected to be fully deployed by November 19, 2002. The legislation stipulates that the screeners should be subjected to background checks and that they be U.S. citizens. The TSA is also charged with ensuring sufficient explosive detection systems to screen all checked baggage at U.S. airports by December 31, 2002.

This latter objective might prove to be especially hard to achieve, especially if passenger convenience is considered in the actions necessary to meet this objective. According to Spagat, fewer than 150 luggage-scanning machines capable of detecting bombs and plastic explosives were in place at 47 U.S. airports at the end of September 2001.[26] In addition to being costly—the initial cost is roughly $1 million plus yearly costs of $700,000 to $1 million for operation and maintenance—these machines are currently slow and inaccurate. A scanner can handle only about one planeload of luggage per hour, and false alarms sound for roughly 22 of every 100 bags. Personnel must then open and search these bags. In addition, the machines can be as long as 16 feet, which poses the challenge of fitting them into existing spaces. Finally, producers of these machines might not be able to expand production rapidly enough to meet this objective.[27]

Another change is that air marshals may be deployed on all commercial flights. While the attorney general is responsible for developing this program, the day-to-day administration of the program would be the DOT's responsibility.

Federal law enforcement officers will also be deployed to secure all areas in the larger airports, including the perimeter. A related requirement is for the DOT to improve access control systems and equipment for secured areas.

As part of a compromise to ensure passage of the legislation, the act allows for the following program. Depending on authorization by the under secretary of transportation for security, some airports may employ the services of a qualified private company for the provision of airport security for up to three years. The legislation also allows other airports to opt out of the screening program after three years and contract with private security providers.

The legislation also contains a number of other noteworthy features. The legislation authorizes the DOT to reimburse airports for their additional costs of complying with increased security measures in the aftermath of September 11. The act expands the scope of the DOT's research and development activities related to aviation security. The act requires strengthening cockpit doors and raising the quality of screening. In addition, the act allows for the needs of small airports to be dealt with by the attorney general's office on a case-by-case basis.

The key features of the legislation can be summarized by using a production function, which shows the relationship between output and inputs. The production of aviation security requires labor, capital, and technology. The labor inputs take various forms, such as passenger and baggage screeners, law enforcement officers in airports and in airplanes, managers/administrators, and researchers. The capital inputs are items such as passenger and baggage screening machines, access control systems for secured areas, and reinforced cockpit doors. Underlying the amount of output that can be produced by combining these labor and capital inputs is the level of technology, which is the body of available knowledge concerning how to combine inputs to generate maximum output. One way to increase knowledge that contributes to

the increased aviation security is through research and development. Frequently, this new knowledge is embodied in machines and other productive resources.

Generally speaking, the legislation increases the labor and capital inputs devoted to aviation security; however, the availability of selected labor and capital inputs could prove to be a major obstacle in the near term. In addition, the legislation assigns control of these inputs to the federal government. The major unanswered question is whether the incentive system for government employees will lead to a better system in terms of the efficient production of the desired level of aviation security than any other system. Another question is how much the preceding changes might cost.

## Estimated Federal Government Cost

Table 1.2 shows a cost estimate of $9.4 billion by the Congressional Budget Office (CBO) for the expenses of the federal government.[28] The focus is on the changes in spending that are subject to appropriation for 2002–4.[29] The funds would be used for paying expenses in the following categories: passenger and baggage screening, air marshals, airport security measures, reimbursements to airports stemming from the additional security expenses due to September 11, general aviation aircraft security, research and development on chemical and biological weapons, and research and development on aviation security technology.[30]

**Table 1.2**
**Cost of the Aviation and Transportation Security Act (in millions of dollars)**

| | *2002* | *2003* | *2004* | *2005* | *2006* | *Total* |
|---|---|---|---|---|---|---|
| Passenger and baggage screening | 889 | 1,942 | 2,181 | 242 | 0 | 5,254 |
| Air marshals | 92 | 316 | 561 | 59 | 0 | 1,028 |
| Airport security measures | 268 | 582 | 631 | 63 | 0 | 1,544 |
| Reimbursement of airport authorities | 553 | 552 | 0 | 0 | 0 | 1,105 |
| General aviation aircraft security | 19 | 41 | 45 | 4 | 0 | 109 |
| R&D chemical and biological weapons | 13 | 22 | 11 | 11 | 3 | 60 |
| R&D aviation security technology | 39 | 51 | 50 | 50 | 50 | 240 |
| Regulations and reports | 2 | 1 | 0 | 0 | 0 | 3 |
| Estimated total cost | 1,875 | 3,507 | 3,479 | 429 | 53 | 9,343 |

*Source:* Congressional Budget Office.

### *Passenger and Baggage Screening*

The CBO estimate assumed that the attorney general would maintain a staff of screeners similar to the existing staff employed in the private sector and that this staff would increase to keep pace with increases in passengers on domestic flights. The existing staff in the private sector consisted of 16,200 screeners, 2,800 supervisors, and 100 managers. Based on the federal pay schedule, the CBO estimated that the screeners would receive an average annual base salary of $35,500, substantially higher than the average salary of screeners in the private sector of roughly $15,000. To generate an estimate of the actual costs per screener, this average base salary was adjusted upward by benefits of 35 percent of the base as well as by overtime pay. The CBO estimates used an average salary of $52,600 for supervisors and $74,900 for managers. These salaries were adjusted for benefits identical to the screeners, but no overtime pay was anticipated.

The legislation also authorizes the attorney general to deploy at least one law enforcement officer at each of the existing 754 airport checkpoints. Thus, at a minimum, to staff each checkpoint around the clock requires 2,262 officers. The attorney general has the authority to deploy more officers at the 100 largest airports. The CBO estimates used an average salary of $46,500 for these officers. Benefits plus overtime increase the average cost for each officer to $73,000.

In addition to the personnel involved directly in screening and law enforcement, there are a number of other costs. First, there are expenses associated with the required administrative staff. Second, there are costs for training, testing, and auditing screeners and for performing background checks. Third, the legislation requires a senior level security officer at each airport (about 450 positions) and two ground security coordinators at each checkpoint (about 1,500 positions). Fourth, additional screening equipment must be purchased, installed, and maintained. The total costs for screening and law enforcement are estimated to be $5.3 billion.

### *Air Marshals*

The legislation authorizes the presence of air marshals on all scheduled flights. Whether or not an air marshal would fly on all scheduled flights is to be determined by the attorney general. The CBO assumed that an air marshal would fly on 20 percent of all flights.[31] As a result, the number of required air marshals would be 2,800. The CBO estimated an average cost per marshal, including salary, benefits, training, supervision, equipment, and other administrative expenses, of $170,000 and a total cost of $1 billion.

### *Airport Security Measures*

The legislation authorizes a variety of measures estimated to cost $1.5 billion to increase security at airports. First, the legislation authorizes the deployment

of federal law enforcement officers to secure all areas in the nation's largest airports. Second, the secretary of transportation is to work with small- and medium-sized airports to determine their needs. This might lead to the deployment of federal law enforcement officers in these airports as well. Third, the secretary of transportation is to work with airport operators to improve access control systems and equipment for secured areas.

The CBO estimates that 6,990 federal law enforcement officers would be deployed at an average cost per officer of $85,000. Each of the 120 largest commercial airports would have 50 federal law enforcement officers. On average, the smaller airports would have three federal law enforcement officers.

### *Reimbursement of Airports for Increased Security Costs*

The legislation authorizes the secretary of transportation to reimburse airports for their fiscal year 2002 costs associated with complying with the September 11–induced security measures. The costs cover additional law enforcement personnel, access-control equipment, and operating costs. Some of these upgrades will not be completed in 2002, so roughly one-half of the $1.1 billion cost will be incurred in 2003.

### *General Aviation Aircraft Security*

The legislation requires the FAA to develop a program to search general aviation aircraft (i.e., private aircraft and charter planes) as well as screen crew members and others who might board a flight prior to takeoff. The CBO estimates the cost of this security enhancement to be $109 million for the 2002–4 period.

### *Research and Development*

The legislation authorizes the FAA to expand research in two areas. First, the FAA is authorized to conduct research concerning chemical and biological warfare and to develop technologies to prevent the successful use of these weapons in planes and airports. Second, the FAA is to increase support for research and development related to all aspects of aviation security involving technology, such as detecting explosives; screening baggage, passengers, and cargo; training employees; and constructing aircraft. The FAA would provide grants to industrial, academic, and governmental entities for promising projects. In addition, the FAA is authorized to provide grants dealing with biometrics, longer-term airport security, and information sharing among federal agencies. In total, the estimated cost of research and development is $300 million.

## Estimated Impacts on Nonfederal Governments and the Private Sector

The legislation requires numerous actions by airport operators and, depending on how the FAA and Department of Justice choose to implement

other requirements in the legislation, may necessitate other actions. In the former category are requirements that airport operators use technology to detect weapons, develop security awareness programs for airport employees, and conduct background checks on employees with access to planes and secure areas. In the latter category are requirements involving security around airport perimeters, the screening of passengers at smaller airports, and the screening of personnel and supplies entering secure areas.

Generally speaking, airport operators have already taken actions to comply with FAA regulations following September 11. The additional costs are not expected to exceed $56 million annually (in 2001 dollars). Moreover, the legislation authorizes funding for airports to cover the costs of security improvements resulting from post–September 11 requirements.

With respect to the impact on the private sector, the legislation imposes mandates affecting air carriers, commercial airplane manufacturers, persons providing training in operating aircraft, and aliens. The Department of Transportation has imposed a $2.50 fee for each passenger enplanement that will be remitted by the airlines to the federal government to pay for the federal government's costs of providing aviation security. Because air carriers would no longer be responsible for screening passengers and baggage, it is uncertain whether the net income of air carriers would rise or fall.

The bill requires commercial manufacturers to increase the security involving the doors separating the pilots from the passengers on new large aircraft as well as on new commuter aircraft. The cost of this mandate depends on the standards set by the FAA.

Finally, the legislation mandates that persons who provide aircraft training report certain information on those they train. Aliens would be required to undergo a background check from the attorney general prior to training. The expectation is that the costs of these mandates would be small.

## CONCLUSION

One unsettling conclusion following the events of September 11 was that both the quantity and quality of aviation security, each difficult to measure, were inadequate. Quite likely both demand and supply factors underlie this conclusion. On the demand side, the catastrophic events of September 11 increased the demand for aviation security by increasing awareness of the very real security threat that existed and likely continues to exist. Moreover, the events of September 11 focused attention on how aviation security was being provided and regulated. This attention revealed numerous shortcomings that prompted increased scrutiny of not only how much aviation security was being provided, but also how it was being provided.

Public decision makers have been prompted to ensure that more resources will be devoted to providing aviation security today as well as to research and development activities that should lead to future improvements. In addition, changes were made in who has the authority concerning aviation security

decisions. The hope is that these changes will result in the provision of an efficient level of aviation security.

Economic theory can be used to make a strong case that the federal government play an important role in aviation security. The basic question is whether the federal role should be restricted to setting and monitoring security standards or whether the role should also include the financing and implementation of security. The most contentious change emanating from September 11 is that the federal government has assumed responsibility from the airlines and airports for the actual provision of aviation security. Policymakers assigned the responsibility for aviation security to the federal government, primarily through the authority vested in the Transportation Security Administration and the Department of Justice.

Will this substantial enlargement of governmental involvement, which is in contrast to the public-private partnerships that dominate aviation security in Europe, be a change for the better? In theory, public provision of aviation security can adequately account for security externalities. Moreover, relative to private provision, public provision reduces the incentives to reduce quality by reducing costs. Proponents of in-house provision argue that the quality of public services delivered by government employees is superior to that delivered by private firms. This feature of public provision might be especially relevant for aviation security, whose quality is hard to observe.

On the other hand, a public agency might not provide security services efficiently because it can operate similar to a monopolist. Proponents of government contracts with private suppliers argue that private firms deliver public services at a lower cost than the government does. In addition, responsiveness to the consumer is not a trademark of monopolistic markets.

Furthermore, it is possible that a public agency with one objective might provide an excessive amount of security (and incur excessive costs) because it is likely to be judged primarily on its security record and not on all the attributes encompassed by air transportation services for consumers. If either or both situations occur, then adverse consequences would result for both consumers and suppliers of air transportation services. At this point, given the still vivid memories of September 11, the general public is likely to prefer too much aviation security to too little. However, one cannot conclude that public provision is a panacea.

The more important question is whether public provision will be an improvement relative to the less-than-perfect pre–September 11 system for providing aviation security. It is too early to answer this difficult question.

## NOTES

1. Four planes were hijacked by 19 terrorists on September 11, 2001. Two of the flights—American Airlines flight AA 11 and United Airlines flight UA 175—departed from Boston's Logan International Airport. The former flight crashed into the north tower and the latter into the south tower of the World Trade Center. The

third flight—American Airlines flight AA 77—departed from Washington's Dulles International Airport and ultimately crashed into the Pentagon. The fourth flight—United Airlines flight UA 93—departed from Newark International Airport and, after heroic passenger actions, crashed in Stony Creek Township in Pennsylvania. More than 3,000 people perished.

2. Aviation security is part of the larger issue of transportation security, which, in turn, is part of homeland security. See Flynn (2000, 2002).

3. An externality, also termed a spillover, is said to exist when either the consumption or production activity of one consumer/firm directly affects either the utility or production activity of an external party. In other words, some benefits or costs are experienced by a party that is not part of a specific consumption or production decision. The benefits or costs are not reflected in market prices.

4. See Hansen and Tamman (2001, A.1).

5. A number of incidents since September 11 have increased the fear of flying for some people. On November 4, 2001, screeners at O'Hare International Airport let a passenger with seven knives, a stun gun, and pepper spray pass through a checkpoint. On December 22, 2001, during a flight from Paris to Miami, Richard Reid was overpowered by flight attendants and passengers as he tried to ignite the explosives contained in his shoes. See McTague (2002) for additional examples.

6. Aviation security is simply one of the many aspects of air transportation service. As Moses and Savage (1990) stressed with respect to aviation safety, aviation security is not easily measured. We assume that a well-defined measure for safety exists, such that the smaller the probability that an airline flight will be disrupted maliciously, the larger the amount of aviation security.

7. Private markets might provide the efficient quantity even when externalities exist. In the present case, however, the conditions for the Coase theorem are unlikely to exist. See Cooter (1987) for a discussion of this theorem.

8. In our illustration, the private costs include all the costs of providing security. Thus, the private costs are equal to the social costs. In a later example, we focus on how externalities associated with the network of airline transportation affect the supply of aviation security.

9. See U.S. Government Accountability Office (GAO; 2000a).

10. See GAO (2000b).

11. See GAO (2000a).

12. See GAO (2000b).

13. See Atkinson (2001)

14. Our analysis focuses on the legislated changes in aviation security rather than the changes implemented shortly after September 11. The latter changes have not eliminated aviation security problems. See McTague (2002) and Morrison (2002).

15. See GAO (2001).

16. A similar example can be found in Kunreuther and Heal (2002); however, their focus is on airlines providing security, whereas we concentrate on a network of airports that provide security.

17. The numbers underlying the example were chosen to illustrate a point. It is possible that the dominant strategy could be providing a high level of security. A Nash equilibrium is also possible. In this case, an airport's best alternative depends on the security choice of the other airport. In addition, the results can be sensitive to whether the game is played just once or is repeated.

18. This privatization as very successful because there were 21 hijackings in European airports during the 1970s, 16 during the 1980s, and 4 during the 1990s. Overall, only 3 of these 41 hijackings originated from airports with private security. See the American Enterprise Institute's Web site, http://www.aei.org/oti/oti13442.htm.

19. See Oates (1972) for additional discussion of fiscal federalism.

20. Glaeser (2002) shows that the more labor intensive the production process, the less desirable it is to nationalize the activity. Such a result could apply to airport security firms because the searching process is labor intensive.

21. Lott, among others, makes these points. See http://www.aei.org/oti/ oti13442.htm.

22. Holmstrom and Milgrom (1991, 1994) show that an agent with strong incentives to pursue one objective might well slow to attend to other objectives.

23. The examples can be found in Power (2002a).

24. The increased scrutiny of passengers by screeners has sparked a privacy debate. The FAA has responded by providing detailed guidelines on performing security checks. See the FAA's Office of Civil Rights at http://www.faa.gov/acr. To complicate the matter further, several instances of harassment and abuse have been reported since the new security measures have taken effect. See Marks (2002) and Power (2002a) for details.

25. Hart, Schleifer, and Vishny (1997) show that if contracts are incomplete, the private provider has a stronger incentive to improve quality and reduce costs than a government employee has. However, the private provider's incentive to reduce costs is excessive, because this provider ignores the adverse effects on quality that are not contractable.

26. See Spagat (2001).

27. Spagat (2001) notes that the FAA had planned to wait until 2009 to phase in requirements for scanning all checked bags for explosives. The events of September 11 prompted the FAA to accelerate the phase-in to 2004.

28. The CBO's cost estimate dated October 26, 2001, was found at http://www.cbo.gov/cost.shtml. The bill number is S. 1447.

29. Because the appropriations will occur later, the actual expenses during 2005 and 2006 for selected categories, such as "passenger and baggage" and "air marshals," are substantially understated.

30. A final category involving regulations and reports is not discussed because of its small (less than $3 million) budgetary effects.

31. McTague (2002) argues that two air marshals should travel on every commercial flight in the United States. Since the Israelis began such a program in 1986, no El Al flight has been hijacked.

## REFERENCES

Atkinson, Robert D. 2001. "How Technology Can Help Make Air Travel Safe Again." Policy Report, Progressive Policy Institute, September.

Cooter, Robert. 1987. "Coase Theorem." In *The New Palgrave: A Dictionary of Economics*, ed. John Eatwell, Murray Milgate, and Peter Newman, Vol. 1, A to D, 457–60. New York: Macmillan.

Flynn, Stephen E. 2000. "Transportation Security: Agenda for the 21st Century." *TR News*, November–December, 3–7.

———. 2002. "America the Vulnerable." *Foreign Affairs* 81 (1): 60–74.
Glaeser, Edward L. 2002. "Public Ownership in the American City." Working Paper No. W8613, National Bureau of Economic Research, December.
Hansen, Jane O., and Tamman, Maurice. 2001. "UGA Fan's Hunt for Camera Bag Turns World's Busiest Airport into Haltsfield." *Atlanta Journal-Constitution*, 17 November, A.1.
Hart, Oliver, Andrei Schleifer, and Robert W. Vishny. 1997. "The Proper Scope of Government: Theory and Application to Prisons." *Quarterly Journal of Economics* 112 (4): 1127–61.
Holmstrom, Bengt, and Paul Milgrom. 1991. "Multitask Principal-Agent Analyses: Incentive Contracts, Asset Ownership, and Job Design." *Journal of Law, Economics and Organization* 7 (Special Issue): 24–52.
———. 1994. "The Firm as an Incentive System." *American Economic Review* 84 (4): 972–91.
Kunreuther, Howard, and Geoffrey Heal. 2002. "Interdependent Security: The Case of Identical Agents." Working Paper No. W8871, National Bureau of Economic Research, April.
Marks, Paul. 2002. "Flight Attendants Find Security Abusive." *Hartford Courant*, February 18.
McTague, Jim. 2002. "Wanted: Wyatt Earps." *Barron's*, March 4, 21–22.
Morrison, Blake. 2002. "Tests Show No Screening Improvements Post-Sept. 11." *USA Today*, March 25, A4.
Moses, Leon N., and Ian Savage. 1990. "Aviation Deregulation and Safety." *Journal of Transport Economics and Policy* 24 (2): 171–88.
Oates, Wallace E. 1972. *Fiscal Federalism.* New York: Harcourt Brace.
Power, Stephen. 2002a. "Airport Screens Cause Conflicts with Carriers." *Wall Street Journal*, February 22, A3.
———. 2000b. "Airlines and Stadiums Have Boosted Security, but Much Remains Undone." *Wall Street Journal Online*, March 8.
Spagat, Elliot. 2001. "Sophisticated Bag Scanners Fail to Catch On as Airlines Complain of Delays, False Alarms." *Wall Street Journal Online*, October 29.
U.S. Government Accountability Office. 2000a. *Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance.* Washington, DC: GPO, June.
———. 2000b. *Aviation Security: Vulnerabilities Still Exist in the Aviation Security System.* Washington, DC: April.
———. 2001. *Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Operations.* Testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives. Washington, DC, September 12.

# APPENDIX

# Related Developments and Research since 2002

A significant expansion in federal power and spending has occurred in response to the events of September 11. One major change was the creation of the U.S. Department of Homeland Security (DHS). The DHS was established on November 25, 2002, and began operating in early 2003. It is charged with preparing for, preventing, and responding to domestic emergencies, most notably those associated with terrorism. A key function of the DHS is to provide aviation-related security. As part of the creation of this department, the Transportation Security Administration, which handles security for all modes of transportation and was created in late 2001, was relocated from the Department of Transportation to the DHS in early 2003.

Coinciding with developments involving security in general, federal power and spending associated with aviation-related security has increased. Federal law-enforcement powers to detect and arrest terrorists as well as funding for counterterrorist intelligence have increased.[1] National Guard troops are frequently seen at airports. Armed air marshals fly on domestic flights. One indicator of the increased effort is the budget of the Transportation Security Administration. With over 50,000 employees, for fiscal year 2007 the budget exceeds $6 billion, which is a more than fourfold increase from 2002. For fiscal year 2008, the budget requested by President Bush is $6.4 billion.[2]

Given that the DHS has existed for only a short time, few studies about its performance have been undertaken. A recent review by the U.S. Government Accountability Office (GAO) concluded that the DHS was falling short of performance expectations in many areas.[3] For example, after identifying 171 performance expectations in 14 mission and management areas, the GAO

1. The recent foiling of a plot to bomb aviation fuel tanks and pipelines at John F. Kennedy International Airport is suggestive of the benefits of this type of activity. See Faiola and Mufson ("N.Y. Airport Target of Plot, Officials Say").
2. Information concerning the Transportation Security Administration's budget can be found at http://www.dhs.gov/xabout/budget/.
3. U.S. Government Accountability Office (GAO), *Department of Homeland Security: Progress Report.*

concluded that nearly half (83) were "generally not achieved." Regarding aviation security, the GAO concluded that 17 of 24 (70 percent) performance expectations were "generally achieved." Not surprisingly, the DHS disagreed with many of the GAO's unfavorable conclusions.[4]

In addition to the GAO, economists have begun to examine the DHS. The substantial increase in spending has generated questions concerning whether the additional funding has been spent to serve the public interest of providing more security. No definitive answer has been provided. In the July 2006 issue of *Public Choice*, which is devoted to the political economy of terrorism, Coats, Karahan, and Tollison examine the allocation of Homeland Security grants.[5] They attempt to shed some light on whether the grants appear to be directed for protection against terrorist activities. They find that some funds are spent in a manner consistent with the public interest. For example, some of the variation across states in per capita grant allocations is explained by airport traffic and population density. On the other hand, however, the formula for some grants allocates almost 40 percent of the funds equally to each state. Such a distribution raises doubts as to whether these funds are used efficiently.

## BIBLIOGRAPHY

Basuchoudhary, Atin, and Laura Razzolini. "Hiding in Plain Sight—Using Signals to Detect Terrorists." *Public Choice* 128 (1–2) (July 2006): 245–55.

Coats, R. Morris, Gökhan Karahan, and Robert D. Tollison. "Terrorism and Pork-Barrel Spending." *Public Choice* 128 (1–2) (July 2006): 275–87.

Faiola, Anthony, and Steven Mufson. "N.Y. Airport Target of Plot, Officials Say; 3 Held in Alleged Plot to Bomb JFK." *Washington Post*, June 3, 2007, A1.

U.S. Government Accountability Office. *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions.* Testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate. Washington, DC, September 6, 2007.

4. The DHS's response to the GAO report is contained in a July 20, 2007, letter to Comptroller General David Walker from the department's undersecretary for management, Paul A. Schneider.

5. An article by Basuchoudhary and Razzolini ("Hiding in Plain Sight") addresses the interaction between a security agency and a terrorist organization. For example, the analysis pertains to the attempt by the Transportation Security Agency's airport screeners to prevent terrorists from getting by security checkpoints. Using a signaling framework, the authors derive the optimal strategy for a security agency attempting to infer whether a passenger is a terrorist based on visible attributes and the optimal strategy for the terrorist, who must decide which attributes to hide. Not surprisingly, they find that always and only checking passengers of a certain ethnic origin or racial type is likely to have adverse national security effects. The authors show that an optimal mixed strategy is possible. In other words, in some cases it is optimal to check passengers with a certain attribute as long as those passengers are not the only ones checked.

# CHAPTER 2

# Convergence and Aviation Security

*AnneMarie Scarisbrick-Hauser and William J. Hauser*

> Attention, Airlines, This is Your Passenger Speaking!
>
> —Eric Weiner, NPR.org

Every day, thousands of people around the world pay for an airplane ticket and come together at centralized assembly areas in airports. These people arrive individually and then join other passengers to be processed and to board a flight under the direction of a team of pilots and flight attendants. Up to this time they are a loose gathering of individuals who are there for only one common purpose, that is, catching the flight. However, by virtue of the fact that they are now gathered in a restricted area (gate, plane) with rules and regulations, a common social bond is created and the individuals become more of a social group. This process is known as convergence, in which a group is created (albeit normally for the short term), the members of the group deal with the social situation, and then normally disperse on arrival.

Usually the flight is completed without incident. The passengers disembark, dispersing quickly into the "brick and mortar world" without any further or future interaction or social bonding with other individual passengers on that flight. Occasionally, some passengers manifest inappropriate behavior on the flight and are sanctioned (formally or informally) for that behavior by airline personnel. Infrequently, however, there are passengers intent on behaving in a way that might endanger the crew, other passengers, and the plane itself. At this point, the social bond created is further strengthened by the perceived need of the group to do something to subdue and restrain the offending passenger.[1]

Social scientists use convergence theory to study the everyday social rituals associated with the assembly, interaction, and dispersion of groups of people participating in conventional group activities, such as concerts and sporting events. More recently, this theory has been used to study how individuals come together to form groups responding to potentially dangerous and ultimately traumatic situations. The assembly processes are studied in order to understand and evaluate ways to get large groups of individuals to come together in an orderly manner and efficiently and safely respond to the behavior requested of them, especially during emergency situations. At the same time, dispersion processes are examined to identify quick, effective, and secure methods of evacuating large buildings, major roads, stadia, and airports when an emergency situation arises. Therefore, by definition, convergence processes are studied to ascertain the factors that lead to the formation of a unified force across a diverse group of individuals who create a social bond and take steps to resolve issues, from customer service issues at one end of the continuum to subduing threatening passengers at the other.

It is recognized that, over time, specific social norms related to behavior in crowds and events have been established and institutionalized, including how to behave as a football fan, a church attendant, a funeral mourner, a protestor, and even an airline passenger. However, the fact that people know how to behave in an airport waiting for a flight and on an airplane during a flight does not mean that we are looking at a unified group of passengers with established social bonds. The creation of new social bonds among passengers may never occur unless the need arises. The emergence of social bonds does not alone explain recent behavior by individual passengers who have formed lasting social bonds with other passengers and crew to address perceived problems on and off the ground. In addition to the social norms associated with passenger behavior, certain activities and perceptions by individual passengers assist in the development of a clear unified focus and purpose leading to the presence of convergence. This sense of purpose or convergence leads to the formation of a unified group of passengers who otherwise would have little in common with each other except for their choice of mode of transportation.

Concurrently, passenger complaints about airline personnel behavior, on and off flights, have dramatically increased since the late 1990s. This has led to government hearings in 2001 and the legislation of nine well-publicized congressional bills related to airline service.[2] At the same time, groups of passengers have lobbied for the establishment of more formalized recognition of the status and rights of passengers as an integral part of the air transportation industry. This has led to the consideration of new federal legislation to create a passenger bill of rights.[3]

It appears that there is increasing convergence within the aviation community concerning the functionality and integration of increasing security in an already stressed and pressured airline business environment. "Convergence" is defined here as the presence of focused activities and reactions by many different interest groups and individuals following a major event, such as occurred following September 11, 2001. A number of examples of

convergence following disasters emerge and disappear within days following a disaster while others remain in place for many years. For example, emergency management responders arrive on disaster scenes within hours and retire once their roles and responsibilities have been completed, while investigators and counselors stay on site for longer periods of time. Convergence activities can emerge as formal or informal: the increased presence of security and Transportation Security Agency (TSA) personnel at check-in points during a security alert, passengers bonding together to fight perceived customer service injustices, passengers and crew bonding against perceived unjust airline personnel, or passengers seeking formal rights through the legal process.

This chapter will identify examples of convergence such as assembly behavior prior to boarding, passenger bonding activities during flight, convergence that may evolve in response to a threat or generalized belief of the need for action on the part of passengers, and convergence that follows an airplane crash where there is a recognized acute need to implement formalized institutionalized social and community responses. The goal of this chapter is to stimulate awareness of the social factors at play in the daily operational experience of air transportation as issues for future consideration in the planning of aviation security strategy.

Air emergencies occur and are resolved daily, receiving minimal local media attention. Fortunately, mass casualty and fatality accidents do not occur frequently. However, they are usually accompanied by significant media coverage and the convergence of services and resources as part of an emergency response plan. More recently, a resurgence of air-related terrorist activities has resulted in a dramatic loss of life, global media coverage, and the increased security scrutiny of those associated with the daily air transportation process.[4] Today there is an enhanced awareness on the part of most passengers of the challenges associated with navigating airport security, the overall cabin experience, and in some cases the need for alertness and responsiveness for fight or flight.[5]

Thinking about airline personnel and passenger behavior today, it is not hard to understand that with the recent increase in federal security screening–related activities and the financial challenges faced by the airlines, an overtly contentious relationship has evolved between passengers and airlines. Unfortunately the first line or face of the airline, the flight crew, has become the target of irate passengers facing the increasing number of flight delays, planes loaded for hours with stranded passengers, and baggage handling issues. These experiences have recently led to the creation of passenger activist groups who are increasing their demands for appropriate civility and customer service, but who are also more willing to band together to assist the crews where perceived threats exist.[6]

## EMERGENCE OF CONVERGENCE

Look up at the sky sometime and see if you can imagine how many planes and people are in the air at this particular point in time. Consider that approximately 660 million passengers were airborne in 2001, with expected

annual increases leading to an estimated volume of 1 billion passengers by 2010.[7] Of course, this means another billion pieces of luggage! Although many of you have jaded eyes from years of working in the airline business, it is still a fascinating concept if you stop to think about it for a moment. Every day, thousands of people arrive at designated airport departure points with their choice of luggage, computers, cell phones, and iPods, not to mention their own unique personality quirks and personal habits. They begin the process of mental and physical transformation into a loose group of passengers who wind their way through the various boarding and security processing lines. Next, they voluntarily sit inside a narrow steel tube with other strangers on top of two wings filled with explosive aviation fuel, laying their fates and lives in the hands of the pilots and flight attendants. If this proposition is not daunting enough, some travelers become aggravated when they cannot bring their guns, knives, pet snakes, dogs, and other interesting personal effects on board. Other individuals forget that they are carrying loaded weapons on board. Worse yet, some are determined to use these tools of violence on board to wreak havoc. Somewhere in the midst of this activity an air marshal slips into his or her seat to keep a watchful eye ready to respond if necessary during the flight.

## THE PASSENGER CONVERGENCE PHENOMENON

In the early 1980s, the authors had numerous occasions to fly both domestically and internationally to attend academic conferences. We initially used to think that airline passengers were just people like us who needed to fly somewhere for some special reason and seemed to be just a temporary collective of individuals. Usually we traveled economy class and found it amusing to see how passengers would go through the check-in and boarding process on the ground following strange rituals such as storing extra drinks in carry-on bags and stuffing food and drinks as if they were never going to eat or drink again. Last, but not least, we observed with much amusement how some passengers aboard would go to great lengths to mark their territory in those small confined spaces known as seats.

Over time, as our flying needs increased and varied from business reasons to personal leisure activities, we began to appreciate the differences associated with passenger seating, meals, inclusive and exclusive in-flight activities, and differentiated levels of service as part of the flying experience. Passengers look alike but are not all similar; they run the gamut from the uninitiated first time flyer to the leisure traveler to the time-starved road warrior. These differences make for interesting observations of how passengers interpret and interact with their cabin experience.

The concept of passenger is an important, multifaceted one that is interpreted differently according to situational demands. First, from an assembly and frequency perspective, there are hundreds of neophyte fliers who join the ranks of passengers every day with little to no experience of the flight

assembly protocols on the ground or what happens in the cabin. They learn as they go through the process. Next, there are those fliers who travel at regular intervals each year for personal reasons such as vacations, weddings, attending college, and holidays. Last, but by no means least, are the "road warriors," that is, business travelers who travel daily or weekly throughout the year engaging every time-saving gadget in order to maximize every aspect of the cabin experience in their time-starved lives. For example, it is now possible to access a Web site designed to describe the comfort rating associated with every seat number on every plane configuration in service in the world today. Thus, flying for some passengers is an integral part of their daily life while it is an infrequent, temporary experience for others.

Another perspective of the concept of passenger is associated with incentives for loyalty and potential for revenue generation. The airlines have established dynamic segmentation pricing models to increase pricing control and fill the plane seats. As a result, the airline rewards certain segments of passengers with first class or business class seats, larger economy seats, bonus prices, and other incentives. By doing this, the airlines have created a special class of airline passengers who have been trained to expect certain levels of service in return for their loyalty. However, this negotiated loyalty provides little protection against increased security screening, delayed flights, lost or delayed luggage, enforced stays on board planes on runways when flight schedules are mangled, and the threat of arrest and seizure in the event of direct complaint to an airline staff member on the ground or crew member on board.

Much has been written about the increase in the air rage phenomenon. However, it is important to note that there is a difference between the need for sanctions and anger management on the part of certain individual passengers who violate the expected norms and the behavior generated as part of a group of passengers who have been trapped on an airplane for eight hours without food, drink, fresh air, working toilets, or communication.[8] Why anyone would think that there would not be anticipated consequences around loading passengers (some with medical or social issues) into a confined space designed to fly that subsequently sits out on a runway with a captive crew and flight attendants for an extended period of time is mind boggling and brings to mind old jokes about how many engineers or sociologists does it take. . . .

Irrespective of who is responsible for these types of decisions, the impact of the experience has the potential to change the social dynamics in the relationship between passengers and airlines with far-reaching effects. Positive and negative effects can be seen as a result of the fact that passengers no longer regard themselves as individual flyers but as members of a collective who are ready to develop connections with other passengers to address customer service issues with airline representatives. Convergence activities have usually been observed occurring as the result of a disaster or unanticipated event but can now increasingly be observed in passengers responding to onboard threats and displaying altruistic behavior toward other participants as part of emergency evacuation or rescue activities.[9]

## POST–SEPTEMBER 11 CHANGES

Following the events of September 11, 2001, an increased awareness of the dangers of flight and potential terrorist attacks was still fresh in the minds of all passengers and flight attendants. From the flight attendants' point of view, their jobs have changed from being safety and service professionals to being potentially the last line of defense before the cockpit. Being viewed publicly as an "air waitress" as opposed to being viewed according to their real job of readiness to evacuate passengers in emergencies has long been a bone of contention in the profession. However, the post–September 11 world has changed the relationship dynamic for flight attendants, moving them from customer service to a hybrid position of service mixed with a healthy dose of suspicion.

While passengers complain about their experiences, flight crews also have numerous complaints about treatment from passengers. Flight attendants report that tension has increased between crews and passengers. This has directly contributed to flight delays, arrests, forced emergency landings, and potential safety risks during flights.[10] While there is no centralized government database to track incidents, between 2000 and 2006, at least 1,992 incidents of passenger misconduct were reported to NASA's Safety Reporting System. Likewise, the Federal Aviation Administration has identified a yearly average of 248 unruly passenger citations between 2000 and 2006. This is an increase of 50 citations per year over the 198 citations recorded in 1999.[11]

Flight crews, on the other hand, feel that while citations are moving back to the level recorded prior to September 11, the working conditions within the company and on the front line have changed for the worse. However, when asked about passenger willingness to assist with subduing those exhibiting risky behavior, flight attendants are comfortable that they will be given assistance when needed. Increasingly, flight crews have come to anticipate assistance from passengers and convergence, if necessary, to overpower risks to the plane's safety. This may be fueled by the story of the Flight 93 passengers' convergence and has yielded numerous reports of unsolicited offers of help, especially from male passengers, should assistance be needed.[12]

Passengers also view their onboard experiences differently since September 11. In addition to the general challenges associated with flying today, many passengers feel strongly about the need to respond to threats to their personal safety as well as to that of the plane.[13] Over the past two years, the increased popularity of blogs and grassroots Web sites, complete with webcam interviews and videos of the events, have led to a higher exposure and profile of passenger issues on board flights.[14]

For example, in August 2007, 120 passengers found themselves stranded on board Continental Flight 1669 bound for Caracas. The plane had been diverted to Baltimore due to bad weather and was forced to park away from the gate, making it impossible for the passengers to disembark. Five hours later, after the toilets failed, the passengers organized themselves and began

clapping and drumming on the overhead bins, ignoring the threat of arrest. The police were called to deal with a report that passengers were violent and out of control and, upon viewing the situation, decided to deplane the passengers. Finally the passengers were deplaned. Following their ordeal, 70 passengers signed a petition that was sent to Continental Airlines' management outlining the fact that there were children and special needs passengers (including a diabetic) that were in need of timely attention that was not given. The details of this story were covered by the news media, both domestically and internationally.[15]

Also, the increased adoption of digital devices such as cell phone recording and video taping technology has provided passengers with a number of options for tracking and monitoring the experiences of others. YouTube, Facebook, and other electronic media have become useful platforms for lobbying for change in flying conditions. For example, video footage of a June 2007 Delta Airlines flight from New York to Dallas/Fort Worth that sat on the tarmac for seven hours was viewed over 100,000 times on YouTube within one week of its posting. The alacrity of convergence around this issue in the summer of 2007 led quickly to lobbying activities in Congress and the passage of regulations that held airlines to higher standards of service, especially barring them from leaving passengers stranded for hours without relief or communication.[16]

Citizens who have experienced the role of passenger in such straits have joined Kate Hanni, founder of the Coalition for the Airline Passengers' Bill of Rights, in their thousands and spend time explaining that they are normal, sane, rational people who have put up with enough disruption and are seeking change. With assistance from other interested passengers, Hanni has developed an emergency manual outlining activities useful for surviving being stranded on a plane, including taking enough food, water, and a change of clothing on board to survive 24 hours.[17]

It is interesting to note that complaints related to aviation security rank very low on passengers' radar, which either speaks well to the acceptance of the processes put in place or to ignorance regarding the efficacy of current procedures. There is no doubt that presentations and complaints leveraged as a result of passenger convergence inside and outside the cabin has created a sympathetic ear in Congress. It remains to be seen whether calls for additional passenger protection legislation will yield success. It is a well-known fact that airlines do not compete on their customer service. It is the price of the ticket!

Against this backdrop of perceptions, recent events, and media reports, it is imperative to look at passengers' increased sensitivity to risk and threat to safety and readiness for mobilization and evacuation. A number of unanticipated passenger reactions since September 11, 2001, on a number of flights leading to passenger-initiated evacuations has resulted in the emergence of an dynamic dubbed the "Let's Roll" effect, in deference to Todd Beamer's last words that fateful day when on board Flight 93, which crashed in Shanksville,

Pennsylvania.[18] John Cox, a U.S. Airways captain and then safety chairman for the Airlines Pilots' Association, stated in an interview in 2004 that the airline industry has recognized the emergence of a heightened attitude of self-empowerment among air travelers and noted that more passengers challenge his explanation when a mechanical problem delays their flights.[19] Federal agencies do not keep track of commercial aircraft evacuations, so data related to passenger-initiated evacuations are restricted to proprietary airline data.[20]

It makes perfect sense that in the absence of information and direction, passengers will engage their own rational decision-making processes and make decisions to safeguard their families and themselves. In the event of a disaster, the survivors, the crew, and the passengers are the first line of response at the scene and many of the search and rescue activities are completed by these on-site individuals.[21] According to Steve Huettel, attitudes since September 11, 2001, have changed for many passengers and they want to be in control of their fate. As a result, previously passive passengers are more likely to take action when they sense danger and are also more likely to evacuate without the benefit of crew instructions or oversight or even in violation of countermanding orders. For example, all but 12 of the 169 passengers vacated a Delta Boeing 757 at Tampa International Airport in June, 2003, in a self-initiated evacuation without crew oversight, as an overreaction to a harmless engine fire that was perceived as an explosive situation by the passengers. While these passengers were viewed as panicking by the Delta crew, they viewed themselves as being strident and purposeful in exiting the aircraft and jostling for position in a queue with the obvious objective of getting off the plane quickly. By the end of the evacuation, 33 passengers had been injured, mostly from falling off emergency slides and sustaining injuries from the left engine, which had not been turned off during the evacuation.[22]

As a result of other, similar actions by passengers, a number of airlines have recognized the enhanced take-charge attitude of passengers and the potential for additional passenger-initiated evacuations. In turn, they have redirected airline crew training to assertively assist and manage passenger-initiated evacuations by providing more instructions to and communications with the passengers.[23]

## CONVERGENCE—POSTEVENT

The activities following a multifatality disaster such as an air crash deserve special mention here. Families and friends become the face and voice of the crash victims, bonding together to find ways to return their lives and social order to a state of normalcy while preserving the memory of their loved ones. Increased attention to the cause and nature of the air crash may result in criminal investigations, enhanced media coverage, and prolonged waits for the retrieval and release of remains, burial, and closure.

The events associated with the terrorist attacks on September 11, 2001, caused communities, from the local to the global level, to unite in an attempt

to understand the tragedy, grieve over the loss of lives, and then find a way to return to normal behaviors. Due to the magnitude of these events and the fact that they are viewed across the country and the whole world, formal and institutionalized responses are an important and expected factor in the healing of both the individuals' and the community's wounds.

## NATURE OF THE DISASTER—AIR CRASHES

Natural disasters, such as hurricanes, tornadoes, floods, and earthquakes, tend to be localized in a geographic area and elicit community responses that are immediate and direct. Most of these events are extraordinary and uncontrollable, and individual and community responses tend to emphasize resolving the immediate situation, mourning the losses, and then rebuilding individual lives and the community. As news of the disaster travels across the world, a number of institutionalized responses are usually initiated, including memorial services, investigations, and the establishment of permanent memorials serve as societal responses to a significant and unexpected event or disaster. Societies react differently to disasters based on the nature and cause of the disaster.

Man-made disasters tend to manifest a different level of socio-emotional attachment. Was it an unintended accident such as a chemical leak, train crash, or multifatality apartment fire? Or was it a planned act of aggression or terrorism (e.g., a plane bombing, a suicide bombing, building explosions)? Accidents, not unlike natural disasters, can be viewed as being at a level of deviance that is unintentional and, while requiring sanctioning, can be normalized after a period of communal mourning and adjustment.[24]

Man-made disasters such as acts of aggression/terrorism generate the highest level of social and emotional response. Their impact has the potential to change the normal way of life or social fabric of the community forever. There is a perceived need to elicit a response in order to identify and punish those who planned and carried out the event. The community, in this case, will acknowledge a sense of healing only when the guilty parties are apprehended and appropriately punished. The community response process for natural disasters is substantially different than for acts of aggression or terrorism. For example, formal institutionalized responses to natural disasters emphasize mourning the loss of lives and property and then looking for ways to minimize the possibility of a similar occurrence in the future. Man-made disasters, on the other hand, are viewed as more deviant and in need of a direct response. In the case of a man-made accident, the response is to punish the guilty parties and to investigate ways to prevent comparable accidents from happening again. Acts of aggression elicit the most socio-emotional fervor in the community, and much time is spent seeking meaning and seeking an understanding of the reasons for the actions.[25]

In a time of social crisis, as when a plane containing passengers and crew is deliberately destroyed by terrorist acts, individuals look for explanations for

what has occurred, seek ways to pay respect to the memory of those who died, and subsequently accommodate the memory in society's social fabric and then move on with their lives.[26]

Acts of terrorism evoke feelings of fear and grief, not only in the community affected by the event but on a national scale, and then mobilize the need for public responses to the death of its citizens. Large-scale formalized institutionalized community responses, for example, memorial services and congressional hearings, fulfill these needs. They create a common ground from which individuals derive common meanings. They allow concerned individuals to share their support with others facing the same circumstances. Not only does this process provide support to the individual and community, but it enables concerned individuals to express their emotions without fear of feeling or acting differently from others around them. Most importantly, institutionalized responses offer a socially acceptable direction for the members of the community to follow in order to return to an acceptable level of comfort.[27]

Over the years, a series of expected ritualistic ceremonies and social markers have been established that recognize the need for acknowledgment of the pain of loss and disruption of normal life with the hope that life will return to some semblance of normalcy in the future. The need to repair the damage arouses the need for collective or institutionalized commitment toward cleansing, closure, and renewal.[28] While the feelings of pain, anger, and loss may never go away, these rituals enable a community to achieve closure and then move forward.

## COMMUNITY CLEANSING

Following the experience of a disaster or large-scale traumatic event such as a multifatality air crash, it takes time for individuals to determine the relationships between themselves as they now are and their lives prior to the accident. How do people make sense of the changes in their lives as the result of the disaster? In many cases, meaningful social interaction is damaged and results in what Ball-Rokeach[29] defines as "the persuasive ambiguity of the situation or the inability to establish meaningful links between events in a total social situation." In disrupted social situations such as the aftermath of airplane crashes or terrorist attacks, efforts must be made to resolve fundamental issues of meaning, for example, understanding what is happening and what will be done and why to mitigate the risk in the future for all involved.

According to Ball-Rokeach, attention must be given to solving the problem, but with the assumption that the group or community has the motivation to resolve the ambiguity, handle the stress, and resume meaningful social action. Thus, the ambiguity is resolved when a person or community of individuals constructs a new definition of the situation, accommodating the loss of privacy due to enhanced security procedures. Families and friends of victims of air crashes have demonstrated tremendous resiliency and tenacity

in the face of difficult challenges, forming their own formal organizations to support each other and engage in political, financial, and social activities to protect their rights and the memories of their families.

When society responds to a crisis in a functionally predictable and sequential manner at the community response level, five factors appear to be involved. First, the event must have a significant impact on the community so that members demonstrate a strong social opinion or consensus that something extraordinary has polluted the normal ebb and flow of societal life. Second, the government must evaluate the scope and consequences of the event in conjunction with the public response and then decide whether or not the polluting event has a harmful effect on core social values. Third, institutional social controls including increased security protocols and loss of privacy must be operationalized to respond to the situation. Fourth, as more diversified groups become involved in the resolution of the event, the potential for power struggles between business and private interests must be considered. Fifth, after the first four stages have been acted upon, the public is ready to participate in the ritual of community cleansing and renewal, including memorial services, announcements of support for increased security, and the prosecution of those responsible.[30]

It is also apparent today that responses to crisis occur in temporally defined patterns or rituals. These institutionalized rituals of community purification include, but are not limited to, public statements, site visits, religious and secular memorial services, public funeral services, pilgrimages, and fundraising activities. Individually and collectively, these processes help to functionally reintegrate members into the community and concurrently turn the community's attention to symbolically accepting the damage, placing closure around the event and then recreating a collective definition of repaired social reality.[31]

While all these processes are designed to provide comfort, a sense of community, or an affirmation of the culture, there are differences between their secular and sacred dimensions. On the secular side, community responses include public statements, Web site shrines on social networks, visits to the site, moments of silence at major public events in any of the community zones affected, government inquiries, crime scene investigations, the establishment of community organizations of family and friends, the establishment of fundraising campaigns, the introduction of songs and poems inspired by the event, and the establishment of lasting physical memorials.

Responses on the sacred side include public prayers, nondenominational services and other religious services, pilgrimages to the site, the establishment of shrines including tokens left by visitors, funeral services at the site of the event or in special locations, floral bouquets, anniversary memorial services, and memorial dedications. Politicians and clergy play an important role in providing support and counsel. Representatives of the local government typically attend every funeral, visit those in hospital, go to the homes of the victims' families at their request for comfort, counsel families, relatives, and

friends where necessary, and participate in many of the religious ceremonies as service readers, servers, pall bearers, or attendants at graveside services. The local politician is also a powerful advocate in facilitating decision making and progress in discussions between families and airline personnel.[32]

## COMFORT, COMMUNITY, AND CULTURE

As previously mentioned, formalized institutional responses to large-scale disasters or grieving events are designed to return the community to its normal social order as soon as possible. As might be expected, the members of the community are, first, seeking meaning for the event that occurred and, second, looking for approval from family members that their acts of mourning and acknowledgment of the loss caused by the event can be completed and life can return to its usual pace. Institutionalized community responses to the event must provide members of the community with some form of explanation or meaning for the event. Community-based ceremonies must demonstrate shared feelings among the participants and allow them a means to release their emotions in a controlled environment. Finally, institutionalized responses must create a comfort zone for the participants based on cultural attitudes and values familiar to the individual and shared by the group, quite a challenge when dealing with an international air crash situation.[33] For example, when 230 passengers and crew from 14 countries died in the TWA Flight 800 crash in 1996, a number of support groups were created in different countries and influenced the effort to establish a permanent memorial on a land site in Long Island, New York, closest to the point of the ocean impact.[34]

Planning for those postdisaster activities specific to providing support and response to the needs of surviving passengers and their family members is a complicated task. The delivery of support occurs as part of three interrelated areas of support and response: comfort, community, and culture. Comfort represents the actions providing support to the families and friends of the crash victims. Community represents a sense of belonging to some space of which people are members and can gain comfort. Third, the integration of cultural values and behaviors helps maintain the social order and provide the socially accepted framework around the grieving process for all impacted by the event and around the return to normal behavior.

Institutionalized community responses, for example, memorial services and the placement of mementoes at a man-made shrine, create a structured process that enables individuals to express their opinions and feelings in an environment that is socially acceptable and shared. In the case of an air crash at the hands of terrorists, inexplicable and unexpected events create a state of anomie or disconnectedness in which the individual does not comprehend what has happened, how it happened, or why it happened. The immediate purpose of a ceremonial institutional response is to provide the members of the community with a way to express their emotions or feelings over the loss or the need for resolution.

The second dimension of the institutionalized process is the reinforcement and enhancement of a sense of community. Through the demonstration that the recognition of loss is collectively shared, individuals become acutely aware that others around them are not only feeling the same pain but are also looking for the same explanations and a direction for the future. Institutional responses bring the community together for a common purpose, for at least a short period of time. Community differences and issues are temporarily set aside as all share in the collective grief. It is also common for members of the community to band together to find solutions to problems, many times to problems other than those causing the traumatic situation. This spirit of cooperation becomes a socially acceptable response that creates solidarity in the community. This solidarity gives the members something to focus their attention on and a sense of hope for the future. Complete strangers will bond together and participate in activities including volunteer work, fund-raising, song writing, providing free legal aid, and so on.

The emergence of culture, the third dimension, provides a social context that bonds all of the processes together. Unexpected events such as disasters not only produce high levels of emotional reaction, but they magnify anxiety and the fear of an unknown future. When this situation occurs there is a need to find a moral anchor around which to stabilize the community's attitudes and actions. This was strongly evidenced in the aftermath of the September 11, 2001, tragedies. Individuals and communities looking for meaning and direction relied heavily on existing social institutions and values. Institutions such as religion and the family dramatically emerged in an attempt to re-create social equilibrium. Religiosity and spiritualism increased as a way to provide solace and meaning. Community responses, such as memorial services, became ecumenical in an attempt to unite a community of victims. At the same time, families became the medium through which coping with the situation was defined, shared, and acted upon. The membership and definition of family expands quickly for the families and friends of air crash victims, based on a bond that is formed as the result of the disaster and is seared in their hearts forever. At the heart of all of this is the feeling that bonding in a family environment is the natural thing to do in response to the uncertainty of the recent events and the even greater uncertainty of future events.[35]

Another example of major convergence and bonding occurred when patriotism reemerged as a key societal principle following September 11, 2001. The symbolic reawakening of patriotic fervor was observed at both the local and national levels across American society. In addition, there was for a period of time social agreement that everyday differences would be set aside, uniting the national image as one entity against the terrorists. Communities united from the neighborhood level to the national level and provided a socially approved way to express their confidence in the American spirit. Whether it was a temporary shrine at a disaster site, a memorial service, a rock concert, or even a sporting event, all were anchored in a serious display of patriotism.

The expressions and social rituals of comfort, community, and culture are interdependent and, whether separately or in combination with the others, provide meaning and direction to members of the community. Each plays an essential role in providing the community with stability during a time of uncertainty. Most importantly, each provides a common, socially approved way for members of the community to converge and express their feelings in the knowledge that others are sharing in the same anguish and pain. It then provides a communal way of dealing with the problems and eventually returning to a level of comfort in the belief that things are approaching some sense of normalcy.

## DEFINITION OF COMMUNITY

The concept of community and the process of convergence are multidimensional and can range from involving a relatively small group to encompassing the "global" community.[36]

Communities have historically been defined according to their geographical and social relationship to the event. Over the past decade we have watched disasters unfold in real time across the world via satellite and digital technology. Entire generations of younger adults spend much of their daily interaction online with others and through the use of social networking sites such as YouTube, MySpace, and Second Life to create communities. The functionality available today enables online users across the world not only to access images and views of disaster sites without leaving their chairs but also to pay their respects and engage in community response activities as well. Thousands of online users flocked to social networking sites to leave comments and condolences and view shrines built by the family members and friends of the deceased Virginia Tech students.[37] It is now common practice for family members and friends of disaster victims to establish their own association and Web site irrespective of an airline's mandatory requirements for the care and support of passengers.

Does a community's social context and emotional proximity to an event help us gain a richer understanding oft the types of actions that take place? At an atomic level lies the core community directly impacted by the event. This core area or community is traditionally identified as "ground zero." For example, in December, 1988, Pan Am Flight 103 crashed in the middle of a street in the village of Lockerbie, Scotland, killing 11 village residents and forever forging core community relationships between the Lockerbie residents and the families of the victims. The village residents later decided to dedicate and protect the crash site as a sacred burial ground for the victims' families to visit.[38]

In September, 2001, United Flight 93 crashed in the quiet and peaceful area of Shanksville, Pennsylvania, narrowly missing houses and strewing personal effects across gardens in the area. The people of Shanksville bonded together and decided to take whatever steps were necessary to maintain the

sanctity of the crash area in deference to the victims and their families.[39] In both cases, the events directly affected members of the community and the memorial sites are constant reminders of these events.[40]

Outside the core area lie communities that have also been impacted by the event. In the case of TWA Flight 800, it was not easy to create community bonds for the families of the victims as the crash site was ten miles offshore. However, they were able to bond as a unique community while sequestered in a Ramada Inn for three weeks. The members of the families' group today spans two continents and uses virtual space or Web site to remain connected with each other.[41]

Beyond these communities lies the national context within which the event took place. The likelihood that the passengers may originate from any part of the country or the world quickly focuses attention on the disaster. While the nation may be physically removed from the actual events and the personal bereavement process, there is a substantial amount of mourning over the loss of lives. This is further impacted by the speed with which the media coverage of the event will turn to assigning blame for the event, which, in turn, increases concern that similar events can occur in other communities across the nation and possibly even in one's own hometown. An air crash generates immediate national press attention and removes any possibility that the local community will be able to maintain a normal state for some time to follow. As the event gains more national recognition as a public issue, a collective call for action moves the coverage and discussion of the event to the next community level, that of the national government. As mandated by law, immediate investigational steps are deployed to assist in deciding whether the event occurred as the result of human error or whether it occurred at the hands of terrorists and is in need of a national investigation and/or some form of sanctioning.

The passenger manifest and severity and scope of the tragedy will dictate the level of involvement at the next level, the international community. The terrorist attacks in the United States on September 11, 2001, were responded to very quickly by the international community through expressions of sympathy, outrage, mourning, and calls to action. It is important to remember that while the disaster occurred in New York City in the United States, it immediately became international in scope. Whether it was as a result of outrage over the number of lives lost, anger and grief over the deaths of citizens representing over 200 countries who were working in the World Trade Center, or fear that these events could happen again, the international community immediately viewed the events of September 11, 2001, as a global issue.

Historically, in a "brick and mortar" world, these different community levels would have come into operation sequentially, but today the speed of digital data transmission has created simultaneous action and reaction within hours of an event. The media display a seamless, real-time stream of coverage across time zones and international boundaries. More importantly, the coverage is presented in such a way that all observers can become members of the community without ever physically coming near the disaster site.[42]

The media play an essential role in defining the level of community responses to grief. The importance and depth of coverage of the tragedy creates the parameters by which others perceive the severity of the event. It also helps those outside the core community to decide whether the event is specific only to that community or something that could also affect their own community. As many of these events begin with a period of normlessness and confusion, the media serve as the informational/definitional gatekeepers, that is, the more the media view the event as a large-scale social crisis, the greater the likelihood that other communities at the national and international levels will do likewise.[43]

## SUMMARY AND CONCLUSION

Flying used to be one of those activities to be endured in order to get to one's scheduled destination. A certain level of aggravation about service was to be expected, and sometimes flights were delayed or cancelled. Prior to September 11, 2001, planes were rarely hijacked, but all that changed in one day. Since that day the entire aviation landscape, the business of aviation. and the passenger experience have changed forever.

On any given day, we see a recognized set of conventional convergence behaviors associated with the flight experience that are not always familiar to new passengers and, in many cases, are ignored by others. Experienced passengers have created their own particular behavioral patterns to manage their confined and challenged environments. Since September 11, 2001, most passengers are more aware of the dangers inside and outside the cabin, they are ready to respond if asked, and they will take independent action, as in passenger-initiated evacuations or restraining passengers causing disruption on flights. Passenger convergence events occur in situations where there is a perception that passengers need to take responsibility and put an end to actions that they perceive as a risk to their safety or as unfair business practices.

The challenges facing airlines over the past 10 years have generated the expectation that air transportation is less than satisfactory, leading to increased anxiety and tension prior to a flight, contentious relationships with aircraft crew, a readiness to mobilize aboard the flight to fight perceived unfair business practices (e.g., being stranded on aircraft on snowy runways for hours on end), evacuate themselves if necessary, and subdue any overtly disruptive act that might pose a risk to their safety. Overall, it would appear that an air transportation experience is an ordeal to be endured as necessary to get from one place to another. While it is a positive sign that the enhanced airline security procedures on the ground do not figure prominently in the challenges facing passengers today, it is not a good sign that passengers are simmering about their recent negative experiences and planning how to react to future perceived issues. It would appear that recent examples of convergence have assisted the government in moving forward with an investigation and recommendations designed to address passengers' complaints and issues.

## NOTES

1. Steve Huettel, "Flying on Edge," *St. Petersburg Times Online*, November 1, 2001, http://www.sptimes.com/News/110101/news_pf/Business/Flying_on_edge.shtml; Steve Huettel, "'Fight or Flight' Tramples Airlines," *St. Petersburg Times Online*, June 20, 2004, http://www.sptimes.com/2004/06/20/news_pf/Business/_fight_or_flight_tra.shtml.

2. Eric Weiner, "Attention, Airlines: This Is Your Passenger Speaking," *NPR*, December 4, 2007, http://www.npr.org/templates/story/story.php?storyID=16352567; Colleen, Muldowney, "Finding the Solution to Airline Customer Service: Is Introducing a Passenger 'Bill of Rights' the Answer?" Madison Magazine, http://www.madison magazine.com/article.php?xstate=view story&story id=231779&view=text. (Accessed on 12/4/2007).

3. The Travel Insider. " You Can Help Pass our Airline Passenger Bill of Rights." February, 2007. http://thetravelinsider.info/airlines/helppassourbillofrights.htm.

4. Robert A. Stallings, "Threats to Cities: Large Scale Disasters and September 11, 2001," background paper prepared for remarks at the Institute for Civil Enterprise Seminar, School of Policy, Planning, and Development, September 4, 2002.

5. Fighting Arts, "Fighting Back at 40,000 Feet: Responding to Airborne Terrorists, Group Principles, Individual Strategies," http://www.fightingar.com/reading/article.php?id=293.

6. Gary Stoller, "Flight Attendants Feel Wrath of Fliers," *USA Today*, June 10, 2007, http://www.usatoday.com/travel/flights/2007–06–10-air-abuse-usat_N.htm.

7. Timothy Ravich, "Legislating Grid Lock—Why New Laws Will Not Improve U.S. Airline Service," *Airliners.net*, May 28, 2001, http://www.airliners.net/articles/read.main?id=10 on May 28, 2001.

8. James M. Kendra and Tricia Wachtendorf, "Rebel Food. . .Renegade Supplies: Convergence after the World Trade Center Attack," presentation made to annual meeting of the American Sociological Association, Chicago, Illinois, August 16–19, 2002; Joe Sharkey, "Right There on the Tarmac, the Inmates Revolt," *New York Times*, August 14, 2007, http://www.nytimes.com/2007/08/14/business/14road.html?ei=5090&en=f4a809a52ad148a5&ei=5090&partner=rssuserland&emc=rss.

9. The Travel Insider, "We Need an Airline Passenger Bill of Rights," February, 2005, http://thetravelinsider.info/2005/weneedapassengerbillofrights.htm.

10. Stoller, "Flight Attendants,"

11. Ibid.

12. Huettel, "Flying on Edge."

13. Steve Huettel, "Fight or Flight."

14. Sharkey, "Right there on the Tarmac"; Stoller, "Flight Attendants"; Eric Weiner, "Attention, Airlines"; Coleen Muldowney, "Finding the Solution to Airline Customer Service: Is Introducing a Passenger 'Bill of Rights' the Answer?" *Madison Magazine*, July 2006, http://www.madisonmagazine.com/article.php?xstate=view story&story id=231779& view=text; Peter Greenberg, "The Fight for Airline Passengers' Bill of Rights," September 20, 2007, http://www.msnbc.msn.com/id/20888793/print/1/displaymode/1098/.

15. Sharkey, "Right There on the Tarmac."

16. Weiner, "Attention, Airlines."

17. Ibid.

18. Huettel, "Fight or Flight."

19. Del Quentin Wilber, "Less Free to Move about the Cabin," *Washington Post*, December 3, 2007, http://www.msnbc.msn.com/id/22074357/print/1/displaymode/1098/.

20. Huettel, "Fight or Flight."

21. Stallings, "Threats to Cities."

22. Huettel, "Fight or Flight."

23. Daniel Yee, "Flying the Friendlier Skies? Delta Offers Videos on Air Etiquette," Associated Press, December 14, 2007, http://www.eventpub.com/includes/datafiles/CP_print.php?id=80474&title=Flying+the+friendlier+skies?+Delta+offers+videos+on+air+etiquette.

24. William J. Hauser and AnneMarie Scarisbrick-Hauser, "Death and Community Responses: Comfort, Community and Culture," in *The Handbook of Death and Dying*, ed. C. Bryant, 721–29. (New York: Sage, 2003).

25. Ibid.

26. Charles, E. Fritz, "Disaster," in *Contemporary Social Problems*, 1st ed., ed. Robert K. Merton and Robert A. Nisbet, 651–94 (New York: Basic Books, 1961); Gary T. Marx and Douglas McAdam, *Collective Behavior and Social Movements: Process and Structure* (Upper Saddle River, NJ: Prentice Hall, 1996); Russell R. Dynes and Kathleen J. Tierney, *Disasters, Collective Behavior and Social Organization* (Newark: University of Delaware Press, 1994).

27. Jeffrey C. Alexander, "Three Models of Culture/Society: The Watergate Crisis in the U.S," *Sociological Theory* 2 (1984): 290–314; AnneMarie Scarisbrick-Hauser, "Societal Reactions to the Hillsborough Disaster" PhD diss., University of Akron, 1990); Hauser and Scarisbrick-Hauser, "Death and Community Responses."

28. Emile Durkheim, *The Elementary Forms of the Religious Life* (New York: Free Press, 191).

29. Sandra J. Ball-Rokeach, "From Pervasive Ambiguity to a Definition of the Situation," 36 (1973): 378–89.

30. Alexander, "Three Models of Culture/Society."

31. Jerry M. Lewis and Michael J. Veneman, "Crisis Resolution: The Bradford Fire and English Society," *Sociological Focus* 20 (1987): 155–168; Scarisbrick-Hauser, "Societal Reactions."

32. Hauser and Scarisbrick-Hauser, "Death and Community Responses."

33. Alexander, "Three Models of Culture/Society."

34. "TWA Flight 800: Families Try to Move On," *WCBStv*, July 17, 2006, http://www.wcbstv.com/topstories/TWA.Flight.800.2.236378.html.

35. The Families of TWA 800 Inc., Non-Profit Organization Website and Newsletters, 1996, http://hometown.aol.com/hseaman275/newslttr.html; Hauser, and Scarisbrick-Hauser, "Death and Community Responses."

36. Fritz, "Disaster"; Kendra and Wachtendorf, "Rebel Food"; Lysia Palen et al., "Crisis Informatics: Studying Crisis in a Networked World," presentation at Third International Conference on e-Social Science, Ann Arbor, Michigan, October 7–9, 2007.

37. Ibid.

38. "Forensics and Families—Lessons from Lockerbie," *Guardian Unlimited*, February 23, 2006, http://blogs.gaurdian.co.uk/news/archives/2006/02/23/forensics_and_families_lessions from_lockerbie.html.

39. Nancy Grant, David H. Hoover, AnneMarie Scarisbrick-Hauser, and Stacey L. Muffett, "The Crash of United Flight 93 in Shanksville, Pennsylvania," in *Beyond September 11: An Account of Post-Disaster Research*, special publication #39, 83–108

(Boulder, CO: National Hazards Research and Applications Information Center, University of Colorado).

40. Frank Eltman, "TWA Flight 800 Memorial Dedicated," July 17, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/07/17/AR2006071700429_pf.html.

41. Families of TWA 800 Inc., "Point de Repere, Montoursville, and Flight 800," http://www.kbsb.com/flt800/#top_01.

42. Palen et al., "Crisis Informatics."

43. Stallings, "Threats to Cities"; Hauser and Scarisbrick-Hauser, "Death and Community Responses."

# CHAPTER 3

# Aviation Security and Passenger Rights

*Kathleen Sweet*

The balance between the need for effective law enforcement and the need for the protection of the rights of individuals remains a controversial issue. Many security officials feel that the U.S. courts have gone too far in protecting the rights of accused criminals. On the other side, critics feel strongly that police have been given a dangerous amount of leeway in exercising police powers. Many years ago, in the majority opinion on *Mapp v. Ohio*, Justice Tom Clark wrote, "Nothing can destroy a government more quickly than its failure to observe its own laws."[1] The government contends, however, that due to the magnitude of the danger caused by air piracy, searches of boarding passengers should be based on either mere or unsupported suspicion.

No one has ever stated that being a federal judge is an easy job. However, the jobs of U.S. District Court Judge Leonie M. Brinkman and U.S. District Court Judge T. S. Ellis III have taken on aspects of particular complexity. They have been assigned the cases of John Walker Lindh and Zacarias Moussaoui, respectively. For example, Judge Ellis was faced with the prickly task of balancing Mr. Lindh's Sixth Amendment right of confronting the witnesses against him versus the government's interests in protecting its security personnel and the integrity of the detainee system in Quantanamo Bay. Meanwhile, Judge Brinkman was forced to deal with the defendant's in-court request to represent himself. The judge felt it was necessary to issue a four-page written order educating Moussaoui on the proper procedures to file motions under seal and ex parte. The judges have precious little precedent upon which to base their rulings.

In the end, John Walker Lindh was sentenced to 20 years in federal prison after tearfully telling a courtroom that he made a mistake in joining the

Taliban. Zacarias Moussaoui will spend the rest of his life in a maximum security prison for his role in the September 11 attacks, after a federal jury rejected the government's four-year quest to secure his execution for the deadliest terrorist strike on U.S. soil.[2] In this chapter, we will examine the measures taken and the extent to which the Constitution and legal precedent regulate the conduct of security officers and the police at airports.

## THE FOURTH AMENDMENT

The Fourth Amendment reads,

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[3]

The amendment itself needs to be broken down into two critical elements. The amendment contains, first, a prohibition against unreasonable searches and seizures, and second, the requirement of probable cause to issue a warrant. Case law has limited the first element to the right to be secure against unreasonable searches and seizures by government agents. The courts have yet to designate airport security officers, acting within specific parameters, as government agents. Consequently, if no search or seizure occurred or if it was done by a private entity, such as airport security, it is not even necessary to determine whether it was reasonable under the Fourth Amendment.[4]

Basically, to a certain extent, airport security officials, when not considered agents of the state, are not technically subject to the restrictions of the Fourth Amendment. Airport security officials are considered to be functioning in the place of state agents, which may make constitutional protection applicable. Since the FAA required airlines to institute security procedures to screen passengers (Federal Aviation Administration, 14 CFR, section 108, FAA, Washington, DC, 1977), some courts have reasoned that "the government's involvement in promulgating the FAA guidelines to combat hijacking is so pervasive as to bring any search conducted pursuant to that program within the reach of the Fourth Amendment."[5]

However, once it has been determined that a search has been done by the government, the Fourth Amendment requires that the search must either have been supported by a warrant or that it must fit into a few specific and well-delineated exceptions. Airport searches, if they are determined to be searches in the context of the Fourth Amendment, must fit into one of three established exceptions applicable to the airport security context: the administrative search exception, the stop and frisk exception, or the consent exception. Depending on the circumstances, other exceptions to be discussed include exigent circumstances or a search incident to a lawful arrest based upon probable cause.

## THE ADMINISTRATIVE SEARCH EXCEPTION

The Supreme Court has upheld a rather broad range of searches and seizures even when they are conducted without the usual apportionment of probable cause. Collectively, the court cases reflect two kinds of departures from the traditional probable cause requirement. One situation, as in *Terry v. Ohio*, is to require individualized suspicion or reasonable suspicion less compelling than that needed for arrest.[6] The other kind of exception is to require no reasonable suspicion at all but instead to require that the search be conducted pursuant to some neutral criteria, which guard against the arbitrary selection of those subjected to such procedures and also serve a public purpose. Those searches have become known as administrative searches.

Administrative searches are justified on the basis that they serve a societal purpose other than the standard criminal law enforcement aim of detecting contraband. An example of an administrative search held to fall within these guidelines is the situation illustrated in *Veronia School District 47J v. Acton*.[7] The administrative search exception enables some people, in this case school officials, to exercise search authority toward select groups of individuals simply because society deems it necessary and appropriate. The case upholds drug testing in schools and notes the importance of limiting the searches to those athletes for whom the risk of physical harm is particularly high. The court specifically stated that "by choosing to go out for the team voluntarily, student athletes subject themselves to a degree of review even higher than that imposed on students generally."[8] This argument lends itself to the theory that passengers choose to fly instead of to travel by other modes of transportation.

The Supreme Court is particularly sensitive to the exact nature of the search. In evaluating the appropriateness of searches they have often focused on the invasiveness of the search. In supporting drug testing of the students, Supreme Court Justice Scalia states, "the student enters an empty locker room accompanied by an adult of the same sex. Each boy produces a sample of urine while remaining fully clothed with his back to the monitor who stands approximately 12–15 feet behind the student . . . no less privacy than in a public restroom."[9]

In determining whether a particular search falls within this exception, the courts first evaluate in detail the privacy interests being violated. The first hurdle is to determine whether a search scheme falls into the administrative search exception by balancing the privacy interests sacrificed against the societal purpose or the need for which the search scheme was undertaken. It must still be determined whether the special need could have been met in a less intrusive manner and whether the particular search was really made pursuant to the special need. If it meets all these criteria, then society as a whole has agreed that the threat is sufficient to warrant giving up the Fourth Amendment rights of certain citizens under certain circumstances. In the case of drug testing at schools, the governmental need to detect and prevent drug use among athletes outweighs the Fourth Amendment rights of the students.

As regards airports, the issue is whether the government's need to detect and prevent terrorist acts, implemented by airline-paid security officers and federal employees, outweigh the Fourth Amendment rights of passengers. So far, the courts have determined that it does. Relying on the rationale of the *Terry* case, the court balanced the competing interests of law enforcement in the context of the current air piracy problem against the rights of individuals choosing air travel. They decided that airport searches could legally be conducted under less stringent standards than ordinary probable cause.

## BALANCING THE APPROACH

The challenge for airport security officials is to figure out when the courts will conclude that the intrusiveness of the search is equally balanced against the level of the threat from hijacking and therefore acceptable. The nature of the security interest will change according to the perceived threat level. If the passengers and subsequently the courts believe that the public need for protection against terrorist activity is greater than the need for the preservation of Fourth Amendment requirements, airport searches will likely continue to be deemed appropriate.

Another factor balanced against the special needs of the government is the nature of the privacy intrusion. For example, at airports, "the intrusion is not insubstantial, it is inconvenient and annoying and in some case it may be embarrassing and at times even incriminating," but is it reasonable.[10] *U.S. v. Skipwith* has held in the case of airport searches that once the passenger enters the screening process, he or she forfeits the right to withdraw. Generally the passenger can not withdraw simply because the search discloses items the passenger did not want discovered, regardless of a Fourth Amendment challenge. In the context of reasonableness, the *Skipwith* case involved a man convicted of possession of cocaine. He had presented himself at an Eastern Airlines boarding gate in Tampa, Florida. Clearly, the gate was a place at which he knew or should have known that he was subject to being searched. His only reason for being at the gate was to board the aircraft. An officer approached him because of his suspicious conduct and an apparent bulge in his pants that the officer thought could have been a gun. Cocaine was discovered and the defendant contested the legitimacy of the search. The court ruled that it had become general knowledge that citizens boarding planes are subject to special scrutiny and to weapons searches. Consequently, it determined that the defendant had little if any expectation of privacy and that the search was reasonable.

However, the privacy issue has many aspects. For example, strip searches in schools, in prisons, and of airline passengers all present a variety of unique and distinct legal issues. All three may be legal under certain circumstances. The difference between them stems from the fact that all three classes of individuals, students, prisoners, and airline passengers, have very different and sometimes different levels of expectations of privacy than others. Based on

these expectations, the level of the perceived threat is crucial in determining what the acceptable levels of the searches will be. Prisoners clearly have a much lower expectation of privacy than an airline passenger does. Consequently, more intrusive passenger screening might not be acceptable if the government's need for ensuring air travel security can be met through less intrusive means. On the other hand, if the threat is high for a specific airport or a whole nation, extra intrusiveness may be quite appropriate. For example, passengers seem more amenable to the very stringent requirements of El Al Airlines, especially when the aircraft is flying directly to Israel. Passengers flying from Minneapolis to Honolulu are much less patient with extra security.

## LESS INTRUSIVE ALTERNATIVES

The courts have generally upheld the idea that a security search must be limited as is consistent with the administrative need that justifies it.[11] If the same level of security can be maintained with a less intrusive means of search, the less intrusive means must be used. Newer technologies will have to be evaluated in these terms. For instance, to justify a passenger screening technology that produces an image of the passenger's body beneath the passenger's clothes, the privacy of the individual must be protected as far as possible. Future security measures will also need a guarantee that the image data will neither be preserved nor archived.

No matter what the new technology is, questions may arise about whether a particular search was appropriately conducted toward the legitimate objective. The human factor can change the appropriateness of any search. Regardless of the courts' approval of a specific procedure or specific piece of equipment, an individual who steps outside the bounds of the procedure or the intended use of the equipment may still invalidate the search. Training and experience are critical to the effective and legal use of aircraft passenger screening.

The basic administrative search exception that has been extended to airports, however, is specifically limited to the search for objects that are a threat to the airport or aircraft. Other contraband, including drugs and currency, are technically not the appropriate goal of the search. However, no matter how narrowly a device or procedure is tailored to detecting safety-related concerns, other information will still be obtained in the process. The search procedure in use, therefore, may yet be acceptable for the confiscation of other contraband, if the additional information is acquired inadvertently. When the information is sought specifically, however, and no concurrent safety rationale is given, the search no longer falls under the exception. A much-discussed topic is the illegal transportation of narcotics. It must be remembered that a plane cannot easily be hijacked by waving a bag of marijuana at the pilot. Nor will a briefcase filled with cash convince most pilots to divert an aircraft. It begs the question whether airport security needs to be searching for these objects. It also raises an inquiry over the legality of police paying airport security officers, who are already underpaid, to inform on potential drug smugglers.

The fine point of this debate is whether information on a non-threat object is obtained in the course of the strict search for threat objects or whether action has been taken in the course of the search to broaden the scope to include a search for non-threat but illegal or suspicious objects. For example, invasive searches are authorized only of persons who repeatedly set off metal detector alarms. Security personnel in some cases may even conduct an "intimate search" of such persons until the suspicion is dispelled.[12] In *U.S. v. Roman-Marcon*, the defendant passed through a magnetometer and, as he passed, the machine alarmed. Instead of remaining at the checkpoint for further screening, he kept walking. He was detained by a police officer, patted down, and packages of narcotics were found. However, the search was initiated because of an alarm from a metal detector. Since metal is the prime indication of a weapon, which can be an effective instrument with which to hijack an aircraft, the search fell within the administrative search exception to the Fourth Amendment requirements. Generally, where there is an indication of the presence of metal, the security personnel may frisk the individual.

## THE STOP AND FRISK EXCEPTION

A stop and frisk exception to the Fourth Amendment requirement for a search warrant occurs when an officer or another authority has a reasonable suspicion that another person is a threat. In the context of airport passenger screening, reasonable suspicion might be that the subject fits the profile of a typical hijacker, that the screener observed something unusual or that a metal detector alarmed. Again quoting the decision in *Terry*, a warrantless search was deemed reasonable when "a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger."[13] Courts since that time have also analyzed the reasonableness of searches based on profiles. It would seem that current law would allow a stop and frisk if an individual fits a narrow class of suspicious persons who are part of a "selectee" class search.

However, such procedures are subject to rigorous judicial scrutiny. A case in point occurred in 1997, in Florida. An off-duty police officer, working for the Miami-Dade county police, pulled over a car on the Florida turnpike. The police testified that the car was pulled over because it had changed lanes without properly signaling. In the course of the stop, a fight broke out. At trial, the accused, Aaron Campbell, alleged that the officers had really used a drug courier profile to make the decision to stop him. The judge agreed.[14]

In essence, the court determined that the officers had stopped Campbell not because they had a reasonable suspicion that he had broken a law but because they had a "mere suspicion" based on the drug courier profile. Such profiling has adamant supporters on both sides. In a legal stop and frisk, law enforcement officers may briefly detain a person they reasonably believe to be suspicious, and if they believe the person to be armed, proceed to pat down or frisk that person's outer clothing.[15]

Again, it must be remembered this case law is directed at government officers, whether they are local, state, or national, and not private security employees such as contract airport security employees. The question of a "passenger" can be stopped and frisked has opened up a whole new set of case law. This too may change in light of the airport screening function becoming the purview of federal employees.

## THE INDIVIDUAL STOP AND FRISK SEARCH

In the famous case of *Terry v. Ohio*, the Supreme Court ruled that a policeman based on his own instincts and suspicions and on the need to protect himself and others may conduct a limited search for weapons without a warrant or probable cause if there is reason to believe that a crime has been committed.[16] The case involved a detective named McFadden who had observed two men in downtown Cleveland acting, according to him, suspiciously. According to testimony by the officer, the men would walk past a certain store, look in, and stop at a nearby street corner and confer. They proceeded to meet again at another street corner where an additional man joined the group, which included Terry. The officer detained the group and frisked them. He located two handguns The men were charged with carrying concealed weapons and convicted.

*Terry v. Ohio* holds that only a limited search for weapons is allowed in the absence of probable cause where the search is not incident to an arrest. The search can be permissible only if a reasonable, prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger. The rationale, as it pertains to airports and aircraft, is that the slight infringement upon individual rights should be balanced against the overwhelming need to stop hijacking.

Overall, the judicial system has refrained from placing restrictions on officers' ability to make stops. The court has basically agreed that officers do have street experience and must be given leeway to use it. In *United States v. Cortez*, the Court supported an officer's discretion to stop an individual by holding that reasonable suspicion should be based on the "totality of the circumstances," which may include inferences and deductions made by a trained officer.[17] Subsequently, the general climate of danger following the repeated hijackings of U.S. air carrier flights was determined to be reason enough for searching all airline passengers. *U.S. v. Epperson*[18] and Section 202 of the Air Transportation Security Act of 1974, required a preboarding search of all passengers and their carry-on baggage for weapons and explosives, pursuant to regulations. The passing of a human passenger through a magnetometer is just such a search. The invasion of privacy constituted by a measuring of the distortion of magnetic waves around the body is so minimal as to be considered administrative. Stopping and frisking moves the level of intrusion up a notch. The search must now be reasonably related in scope to the circumstance that made the original intrusion justified in the first place.

## THE SELECTEE CLASS STOP AND FRISK SEARCH

In contrast to the individualized stop and frisk search, the selectee class category of the stop and frisk search approach requires the identification of small groups of people singled out for additional scrutiny. The suspicion needs only to establish probability, not certainty, and it can be established from the totality of the circumstances. However, to prevent abuse, the attributes in the profile must be relevant to the threat being averted. In *U.S. v. Sokolow*, the defendant was stopped at the Honolulu airport by agents who knew the following: (1) he had paid $2,100 for two airplane tickets from a roll of $20 bills; (2) he traveled under a name that did not match the name associated with the telephone number he provided the airline; (3) his original destination was Miami; (4) he stayed in Miami for only 20 hours; (5) he appeared nervous during the trip; and (6) he checked none of his baggage. The court reasoned that these facts amounted to reasonable suspicion, and the majority opinion concluded that "reasonable suspicion" was a level of suspicion considerably less than proof of wrongdoing by a preponderance of the evidence.[19]

The court upheld, in essence, the agent's belief that the defendant's behavior was consistent with the DEA's drug courier profile, but stated that a court sitting to determine the existence of reasonable suspicion must require the agent to articulate the factors leading to that conclusion, whether they are part of a profile or not. This decision seems to set a precedent for airport passenger profiling of potential terrorists. Further decisions, however, will be required to settle the issue.

## THE CONSENT EXCEPTION

Another exception to the Fourth Amendment prohibition against unreasonable searches and seizures is evidenced by the rules relating to consensual searches. When passengers freely and voluntarily give consent to a security search, they surrender their privacy interests, and the issue of potential violations of 4th Amendment rights is moot. *Schneckloth v. Bustamente* on the other hand, if the travelers had an expectation of privacy, any consent would have to knowingly be waived in order for the consent exception to come into play.

In *Schneckloth v. Bustamente*, a police officer stopped a car containing several men when he observed that one headlight and the license plate light were nonfunctioning. When the driver could not produce a license, the officer asked a passenger, who claimed he was the vehicle owner's brother, if he (the officer) could search the car. The passenger replied, "Sure, go ahead." Stolen checks were found under a seat, leading to charges against the car passenger Bustamente, whose motion to suppress the evidence at trial was denied. His conviction was affirmed on appeal but the 9th Circuit Court of Appeals set aside the district court's order. The precise question became, what must the state prove to demonstrate that consent was voluntarily given? The court issued a very narrow decision.[20]

It held that when a subject of a search is not in custody and the State attempts to justify a search on the basis of his consent, the Fourth and Fourteenth Amendments require certain conditions to be met, namely, that the State demonstrates that the consent was in fact voluntarily given and not the result of duress or coercion, express or implied. Voluntariness is a question of fact to be determined from all the circumstances, and while the subject's knowledge of a right to refuse is a factor to be taken into account, the prosecution is not required to demonstrate such knowledge as a prerequisite to establishing voluntary consent.

As early as 1973, the consent exception to the Fourth Amendment requirement, in the context of airport searches, had been litigated. If the nature of the established screening process is such that the attendant circumstances will establish nothing more than acquiescence to apparent lawful authority, some authorities have ruled that there is no real consent.[21] One case went so far as to say that it could hardly be considered voluntary consent when the passenger's only alternative was to forego the flight.[22]

Once again, the central issue revolves around the concept that airline employees, in compliance with government regulations, conduct these searches. As already discussed, some legal authorities contend that these "warrantless," nonarrest searches are legal because private persons administer them. Nonetheless, these searches have been conducted because a federal agency has required them. Adding to the mix, in the future the federally trained federal employees will conduct the searches. Section 108.9 of Federal Aviation Regulation 10811 requires each certificate holder to "conduct screening under a security program . . . to prevent or deter the carriage aboard aircraft of any explosive, incendiary, or deadly or dangerous weapon on or about each individual's person or accessible property and the carriage of any explosive or incendiary in checked baggage." A passenger can not legally board an aircraft unless the airlines conduct a search of the passenger's person and possessions.

An on-point case was *United States v. Lopez*,[23] which was decided before the 100 percent screening rules came into effect in 1973. Regardless of this, it contains some interesting and applicable language. The government in this case argued that the posting of signs advising that passengers and baggage were subject to search was tantamount to "implied consent." The court disagreed and even pointedly commented that consent to a search involves the relinquishment of fundamental constitutional rights and that consent cannot be lightly inferred. In *U.S. v. Lopez*, that involved the seizure of narcotics. The judge wrote, "Nor can the government properly argue that it can condition the exercise of the defendant's constitutional right to travel on the voluntary relinquishment of his Fourth Amendment rights."[24] The court extended its reasoning by providing that airport searches were not justified as searches incident to arrest either. It is also interesting that the judge referred to air travel as some sort of "constitutional right." Of course, a thorough search of the U.S. Constitution fails to reveal such an explicit right.

Two questions regarding the consent exception remain unanswered:

1. At what point do passengers give consent?
2. To what precisely are passengers consenting?

As stated, some legal scholars argue that it can hardly be considered voluntary consent when a passenger's alternative to submission is foregoing the flight. The 9th Circuit court in *U.S. v. Davis*, as early as 1973, also confronted this issue.[25] The Davis court did not specifically hold that consent to an additional search could be withdrawn after an inconclusive scan if the passenger agrees not to board the plane. Nor did it determine at what point in the boarding process a passenger might decide not to fly and thereby withdraw implied consent. Basically, the judge simply believed that the defense argument failed because the passenger did voluntarily consent, at least to the initial search.

The law regarding the consensual search of baggage and one's person by police officers has remained fairly constant over the years. Recent case law, as in *U.S. v. Favela*, upheld the concept that police officers can approach and question passengers without the officers' conduct constituting a seizure.[26] The officers had approached the defendant after observing her walk back and forth from a gate to a gift shop at the Kansas City airport. The officers asked if they could search her bag and she consented. Nothing was discovered. She was requested to pull her shirt tightly around her waist when the officers observed a bulge. One officer asked to touch the bulge and she consented to the touching as well. She was placed under arrest. A search incident to arrest uncovered 1.2 kilograms of methamphetamine. The case was distinguished from *U.S. v. Eustaquio*, which involved the nonconsensual touching of a bulge in the defendant's clothing, without reasonable suspicion, which was determined to have violated her Fourth Amendment rights.[27] The defendant had argued that the officer lacked the reasonable suspicion necessary to justify a nonconsensual investigative search. The court reasoned that the issue need not be addressed because in this case there was not even a seizure for Fourth Amendment purposes.

Another twist to the voluntariness matter or consent question is the power relationship between the security individual and the passenger, who may be a person of color. That persons of color are subjected to a disproportionate amount of police security is hardly in doubt. This is especially prevalent in the context of ordinary stops; even when increased security has no objective foundation, it often results in an actual search. As regards traffic stops, Justice O'Connor stated in a dissenting opinion to *U.S. v. Eustaquio* that "As the recent debate over racial profiling demonstrates all too clearly, a relatively minor traffic infraction may often serve as an excuse for stopping and harassing an individual."[28] Such traffic stops can be analogized to stops in airports. Demonstrating whether or not a particular airport security or police officer has acted on race-based motivation is problematic at best. So much racial bias is subtle and difficult to prove, and it can even be subconscious. The concept was highlighted when after September 11, two rabbis praying in an aircraft

were removed from the aircraft to be searched, presumably when a passenger assumed they were speaking Arabic and acting suspiciously.

Once the passenger is singled out for whatever reason, she or he is often asked to consent to a search. Many courts are leaning toward requiring a law enforcement officer to have at least an articulable suspicion before even asking for consent to search. The officer often intimidates people, especially those of color. They do not completely understand their right to just say no. Even if the police do have some suspicion, the inherently coercive nature of the police a citizen encounters, especially in airports, and the difficulty in proving free and voluntary consent may require additional safeguards. One court in Hawaii has even suggested a Miranda-like warning such as advising the individual of the following:

1. The individual is free to leave and need not give consent;
2. If consent is given, that any contraband found during the search will be used to prosecute; and
3. That consent may be withdrawn at any time.[29]

The courts will certainly continue to evaluate whether passengers have truly consented to searches in airports and whether the consent they give is voluntary. In the aftermath of September 11, passengers seemed particularly willing to consent to be searched. This attitude may well already be fading.

## OTHER EXCEPTIONS TO FOURTH AMENDMENT REQUIREMENTS

### Border Searches

At a national border, a border search is a superficial search or inspection conducted without a warrant or probable cause of persons, vehicles, and property entering the United States. The Supreme Court in *Martinez v. Fuerte* upheld border searches as inherently reasonable under the Constitution.[30] All persons entering the United States are subject to search for the simple reason that they are entering the sovereign territory of the United States. The border area is defined as any place that is the functional equivalent of the border, whether it is the first airport where the plane lands or any established inspection station near a border. Additionally, a U.S. Customs official is allowed to stop, search, and examine any person an officer suspects to be in possession of any type of contraband whatsoever.

Specifically, in *U.S. v. Ramsey*, the court upheld a customs inspection of mail entering the United States, which by regulation does not extend to reading the correspondence. The mail can be searched for prohibited items, including explosives and weapons. In *Ramsey*, the court stressed:

1. That the search was constitutional under the long-standing rule generally applicable to border searches, namely, that such searches are considered to be reasonable

by the single fact that the person or item in question had entered the United States from outside; and

2. That the lower court was wrong in concluding a warrant would be needed as to mail.

The lower court in *Ramsey* had excluded the evidence because it did not meet the "exigent circumstances test" for permitting searching without warrants. The Supreme Court, however, reversed this decision and determined that the border search exception is not based on the doctrine of exigent circumstances at all. As for nonroutine border inspections, the standards are quite different. Lower courts have generally held that a "real suspicion" is needed for a strip search and a "clear indication" of the presence of some sort of contraband for a body cavity search to be acceptable. U.S. Customs has often been criticized for abusing this investigative tool.[31]

### Exigent Circumstances

Searches under exigent circumstances also constitute an exception and are conducted to prevent physical harm to officers or other persons and the fruits of them are perfectly admissible, as was ruled in *U.S. v Sarkissian*.[32] Certain situations may clearly justify a search of something without triggering the Fourth Amendment. According to the Legal Counsel Division of the FBI, there are three threats that provide that justification.[33] They include clear dangers to life, of escape, and of the removal or destruction of evidence. The requirement for searches under exigent circumstances was first recognized by the U.S. Supreme Court in *Warden v. Hayden*.[34]

The court approved the search of a residence conducted without a warrant, which followed a report that an armed robber had fled into a specific building. The courts, using very interesting language, extended the idea even further in *Mincey v. Arizona*.[35] The Supreme Court held that "the 4th Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others."[36] Emergency searches, therefore, seem to be permissible when conducted by the police without a warrant on the basis of some immediate and overriding need, such as police safety. Employing this logic, airport police officers, airport security officers, and the public are certainly gravely endangered if a fellow passenger has a gun or an explosive device. How that device becomes apparent to the authorities is what is at issue. In essence, it is apparent when it is reasonable for the officer to assume that a threat exists.

## REASONABLENESS

Much has been written about the concept of reasonableness. Law enforcement personnel and security professionals use searches and seizures to locate and collect evidence needed to convict individuals suspected of crimes and to control access to aircraft. Each of these searches must be reasonable. Courts,

lawyers, police, and security officials have agonized over the precise meaning of this term. In *Mapp v. Ohio*, the Supreme Court found that the police did not exercise reasonable judgment in their enthusiastic seizure of alleged pornographic materials without a warrant.[37] On the other hand, the same actions, with a valid warrant, would probably have resulted in a conviction upheld by the courts.[38]

In airports, the reasonableness of a search must be weighed against the level of the threat. High threat situations, such as existed during the Persian Gulf War and after September 11, change the degree of acceptable intrusiveness of airport searches. However, there are limits to intrusiveness. In *U.S. v. Afanador*, customs officials, acting on an informer's tip, stopped two airline attendants in Miami after arriving from Columbia, a known drug source country.[39] Despite finding no contraband in the luggage, the agents insisted on a strip search, even though the informant's tip had only pertained to one individual. The court decided that the strip search of the second flight attendant was just too intrusive based on the totality of the circumstances.

Another case involved a Drug Enforcement Agency (DEA) agent who stopped a traveler in the Atlanta airport. The passenger had arrived from Fort Lauderdale, a city the agent considered a principal source of cocaine. The suspect apparently arrived early when law enforcement activity is diminished and appeared to be concealing the fact he was traveling with someone else; in addition, he possessed only some carry-on luggage. In *Reid v. Georgia*, the Supreme Court held that "the agent could not, as a matter of law reasonably suspect the petitioner of criminal activity on the basis of these observed circumstances."[40] The Court went on to note that its members' experience with drug agents makes them wonder if there exists any city in the world that a DEA agent would not characterize as a known source of narcotics. These cases support the contention that courts will set limits on police and airport searches when they believe the authorities have simply gone too far.

## PROBABLE CAUSE

This concept of reasonableness is linked to probable cause, and probable cause is another term that has been meticulously dissected and reconstructed by the courts. In essence, the Supreme Court has ruled that any arrest or seizure is unreasonable unless it is supported by probable cause.[41] The burden of probable cause requires more than mere suspicion. The officer concerned must know of facts and circumstances that would reasonably lead to "the belief that an offense has been or is being committed."[42]

If no probable cause existed when a police officer took a certain action, it cannot be retroactively applied. Information to support probable cause can be acquired in a number of ways. First, personal observation permits police officers to use their personal training, experience, expertise, and instinct to infer probable cause from situations that may or may not be obviously criminal. Second, information collected from witnesses, victims, and informants,

so long as it is reliable, can be used to support probable cause. Third, physical evidence, such as a gun or knife in plain view inside an x-ray machine, may provide officers with sufficient credence to support probable cause. Finally, probable cause clearly exists where the police actually see a person committing a crime by concealing some sort of weapon or contraband.

On top of all this, recent case law has held that a judicial determination of probable cause must be made within 48 hours after an arrest, even if this period is over a weekend.[43] The conclusions of the courts as to what exactly constitutes probable cause are often difficult to apply in an airport setting. Airport security officers, whether police or private, are expected to make split-second decisions on probable cause. This is required regardless of the fact that the courts will dissect the decisions with a fine tooth comb, using all the time in the world needed to do so. When an officer has overstepped what the courts consider reasonable, they are quick to implement the exclusionary rule.

## THE EXCLUSIONARY RULE

The judiciary's most effective tool in regulating the activity of law enforcement officers is the exclusionary rule, which prohibits the use of illegally seized evidence in court. According to the rule, any evidence obtained by an unreasonable search or seizure is inadmissible against a defendant at trial.[44] Furthermore, any physical or verbal evidence police acquire by using illegally obtained evidence is known as the fruit of the poisonous tree and is also inadmissible.

The exclusionary rule forces the police to gather evidence properly. If they abuse the mandates of the Fourth Amendment, they are unlikely to get a conviction. Critics of the rule argue that it permits guilty people to go free because of simple carelessness or innocent errors. Consequently, the courts have carved out several exceptions to the rule.

## THE LEGAL AUTHORITY OF PRIVATE PERSONS TO SEARCH

The exclusionary rule applies to all evidence presented in federal court as per the decision in *Weeks v. U.S.*[45] The case held that where federal officers have made an "unreasonable" and consequently illegal search and seizure, the evidence obtained is not admissible in a federal court proceeding. However, in *Wolf v. Colorado*, it was decided that the *Weeks* ruling was not to be applied to illegally seized federal evidence offered in a state court.[46] Consequently, the first of many "illegal state searches" was admissible in federal proceedings. As evidenced by the case of *Lustig v. U.S.*, the courts were inclined to admit evidence illegally seized by state officers in federal court. The court had, for some reason, not readily accepted that "The crux of that doctrine is that a search is a search by a federal official if he had a hand in it; it is not a search by a federal official if evidence secured by state authorities is turned over to the authorities on a silver platter."[47]

For approximately 50 years after the original *Weeks* ruling, state courts continued to allow illegally obtained evidence, and federal courts could admit evidence that had illegally been obtained by state officers. This practice came to be known as the "silver platter doctrine" because each conviction was handed to the prosecution on a silver platter. The only times when the procedure was discouraged was when police actions were so extreme that they shocked the conscience of the court.

For many years, however, the silver platter doctrine was acceptable law. It meant that a search by a federal official offered even if the officer had a hand in collecting the evidence did not technically constitute a search by a federal official. If the evidence secured by the state authorities was turned over to the authorities "on a silver platter," it was still admissible. The Supreme Court in the decision in *Mapp v. Ohio* finally eliminated this procedure. Whereas the Supreme Court had previously been hesitant to apply the Fourth Amendment in state courts, *Mapp* signaled a new willingness to apply the Fourth Amendment to both federal and state law enforcement officers.

Earlier, in *Elkins v. U.S.*,[48] the Supreme Court had laid the foundation that evidence illegally obtained by state offices and subsequently provided to federal agents would not be admissible in federal court as per the due process clause of the Fourteenth Amendment. This was further refined in *Mapp*, where the court reasoned that the prohibitions of the Fourth Amendment were fully applicable to the states under the amendment's due process clause, making illegal searches equally inadmissible in any court.

The court was first convinced in cases where, as already mentioned, police actions were so extreme that they shocked the conscience of the court. The standard was created in *Rochin v. California*.[49] In the Rochin case, the police entered the home of Mr. Rochin, without a warrant, and testified that they saw him place what they suspected to be narcotics in his mouth. They transported him to a hospital and had his stomach pumped. Some morphine was recovered, and he was subsequently convicted of possession of illegal drugs. The Supreme Court overturned his conviction. They concluded that the police officers had gone too far and had violated the defendant's constitutional right for protection against unreasonable searches. Earlier, the courts had made a huge distinction between state officers and federal officers. Today, they make a distinction between officers of a government entity and private security officers. It remains to be seen whether that differentiation will survive, especially when the "private security officers" are federal employees.

It should be noted at this point that as regards airport searches, which are in essence still considered private citizen searches, the courts first recognized and analyzed the issue in a landmark case as early as the 1920s in *Burdeau v. McDowell*.[50] The court specifically held that searches by private persons are separate and distinct from searches conducted under state authority. The Fourth Amendment was intended as a restraint upon the activities of sovereign authority, and it was not intended to be a limitation upon anyone other than governmental agencies. Individuals have other means of redress against

those who may have illegally taken private property as part of an administrative search. This particular reasoning was reinforced again 40 years later. Individuals can sue using the law of torts as a remedy.

In *People v. Superior Court of Los Angeles*, the court reiterated that there are no state standards for "search and seizure" by a private citizen who is not acting as an agent of the state or other governmental unit.[51] The court subsequently reasoned that "therefore acquisition of property by a private citizen from another person cannot be deemed reasonable or unreasonable." Exactly who today is considered a government agent or is acting in essence as or in the shoes of a government agent is still to be adequately defined by the courts, an issue that again is becoming more and more complicated by the assumption of such duties by the TSA.

## NONVIOLENT THREATS?

Generally, security is concerned with detecting weapons, explosives, and other dangerous materials. When security personnel do suspect such a risk, they usually call in the appropriate government agency or military personnel to handle the risks of a bomb or other dangerous device. This type of search is easily distinguishable from the normal "suspect" search due to the potential threat to the public. Arguably it could be held to be a private search, since the carrier initiated it. Additionally, it could be considered a lawful police search under the exigent searches exemption to the Fourth Amendment rules.

However, the search for other "nonviolent threats" has also occupied the courts. In *U.S. v. Pryba*, a United Airlines supervisor had authorized a package to be opened because of "peculiar circumstances" surrounding the receipt of the shipment.[52] Basically, the "peculiar circumstances" consisted of the fact that the shipper was nervous; he evaded questions on the actual contents of the package and admitted that the return address on the package was nonexistent. It must be remembered that this incident took place in 1970. The airline employee was arguably just being cautious, since the airlines were being held to the standard of exercising due diligence in uncovering explosives. When the package was opened without a warrant, the contents turned out to be films of alleged hard-core pornography, which were turned over to the FBI. The search was considered legal.

Other examples of closer judicial scrutiny was exhibited in *Wolflow v. U.S.*, where police participation at the request of the carrier was at issue once again in a case involving the "nonviolent" contents of certain suitcases checked for carriage.[53] The ticket agent accepted two "overweight" suitcases for a flight scheduled to fly between Los Angeles and Las Vegas. The agent testified that he held them off the flight based solely on the excessive weight of the two suitcases. The agent's superior, for whatever reason, called a Los Angeles policeman to witness the opening of the bags. The contents revealed 3,500 watch movements that the airline turned over to customs agents. This 1968 case upheld the admissibility of the fruits of the search as falling within the exemption created by

*Burdeau v. McDowell.*[54] However, it is unclear in what way the weight of baggage actually accepted for shipment is suspicious in and of itself.

Earlier the courts had bolstered once again the concept that law enforcement agents must secure a warrant whenever reasonable. The judges categorically restated the basic idea of unreasonable searches when they said, "It is a cardinal rule that, in seizing goods and articles, law enforcement agents must secure and use search warrants whenever reasonably practicable." This rule rests upon the desirability of having the magistrate rather than police officers determine when search and seizures are permissible and what limitations should be placed upon such activities, as was decided in *Trupiano v. U.S.*[55] Overall, airline agents now leave the contraband exposed so that law enforcement can visibly see the contraband and are not forced to reopen the luggage, which would necessitate the acquisition of a warrant.

Therefore, the courts have sought to rule on searches in which the airline agent locates contraband and summons the police. Is the police activity with respect to the same object a separate search subject to Fourth Amendment constraints? In *U.S. v. Jacobsen*,[56] Federal Express employees opened a damaged box. They discovered newspapers covering a tube. After the tube was cut open they observed plastic bags of white powder. They immediately summoned the federal authorities. However, prior to the federal agent's arrival, the airline employees had put the plastic bags back into the tube, and the tube and newspapers back into the box. They did keep the box open. The federal officer reopened the box and exposed the smaller bags of white powder. He field tested the contents on the spot and determined the white powder to be cocaine.

Justice Stevens concluded that the agent's actions were not a significant expansion of the earlier private search and concluded that subsequently no warrant was required. He stated in *U. S. v. Jacobsen*, "Respondents could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents." The agent's viewing of what a private party had freely made available for his inspection did not violate the law. It remains unclear as to whether the suggestion that the owner of the container had no legitimate expectation of privacy in its contents and that government agents in opening that container without a warrant on the strength of information provided by a private party would not violate the law.

The subject of joint operations between private security, the airlines, and/or law enforcement personnel remains blurred and is generally decided on a case by case basis. In a very early case during prohibition, *Byars v. U.S.*, a federal agent who had been invited to accompany a state officer participated in a search that turned up counterfeit strip stamps of the kind used on whiskey bottled in bond.[57] The court ruled that such joint operations need to strictly follow Fourth Amendment protections and therefore held the contents of the baggage inadmissible.

In summary, in *Burdeau v. McDonell* the exclusionary rule was characterized "as a restraint upon the activities of sovereign authority and not a limitation upon other than governmental agencies,"[58] and on this basis courts have declined to exclude evidence in criminal cases when obtained by private persons. However, the Fourth Amendment becomes applicable when a private officer or citizen is acting as an instrument of government agents. Whether a private individual has been encouraged to cross the line is determined by a "totality of the circumstances" test. Circumstances to consider include the motive of the private security officer or airline agent; any compensation or other benefit the private individual receives from the government; and the advice, direction, and participation of the government agent. This test would therefore apply to airline security officers who receive a bonus for discovering certain kinds of contraband and who may be receiving bribes from law enforcement officers to inform them of suspicious activity.

Certain circumstances can jeopardize an individual's status as a private airport security guard or simply a private citizen. Of particular concern is the moonlighting of off-duty police officers. In *People v. Tarantino*, the court resolved that a police officer working during his off-duty hours as a security guard is still a deputized police officer.[59] In *Tarantino*, the court concluded that *Burdeau* was inapplicable. The court distinguished the case by recognizing that an officer employed by the district attorney and paid with public funds as part of his regular daytime employment obtained the evidence.

## ADMINISTRATIVE SCREENING SEARCHES AT AIRPORTS

As repeatedly mentioned, the concept of police participation in private searches takes on a whole new aspect when combined with the idea of searches conducted by federal employees. Much has been written about the idea that airport security officers are not agents of the state and that they are in essence private citizens. However, they would never be stationed at airports searching baggage unless mandated by federal regulation. The government and the airlines consider the threat real; they have regulated the equipment used in the searches and have made it obligatory that airport operators and airline carriers maintain and implement stringent search procedures precluding the introduction of dangerous weapons and materials onto airplanes and into airplane terminals.

Section 108.9 of Federal Aviation Regulation 10811 required each certificate holder (those entities approved by the FAA to operate as airlines) to conduct screening under a security program. Such people must prevent or deter, by appropriate procedures approved by the FAA, the carriage aboard airplanes of any explosive, incendiary, or deadly or dangerous weapon on or about each individual's person or accessible property and the carriage of any explosive or incendiary in checked baggage. An assistant attorney general of the United States testified before Congress in 1973 that even though private employees

of airlines are doing the search, it is indisputable that they are ordered to do so by the federal government. This issue is again amplified by the transfer of private security jobs to federal employees.

Cases prior to the mandatory 100 percent screening of all passengers and baggage requirement explain the concept. In *U.S. v. Lopez*, discussed earlier, the courts were critical of airline employee violations of civil rights of those being screened in airport searches.[60] The case involved a narcotics seizure and turned on the issue of consent. Government attorneys contended that because airport officials had posted signs advising passengers that they and their baggage were subject to search, they could search on that basis alone. The idea of "implied consent" is not a new one but is based on some stringent requirements.

*Lopez* was one of the first airport search cases to raise the issue of consent by prior written notification. The idea that simply posting signs advising that passengers and baggage were subject to search was tantamount to "implied consent" neglects to recognize that the passenger is not free to leave if contraband is suspected or that access to air transportation is effectively denied. Everyone knows that to actually reach the aircraft or gate concourse each passenger, visitor, crewmember, or vendor must submit to a search of his or her person and effects. Early cases were extremely critical of the concept. Most courts have consistently held that consent to a search involves the relinquishment of fundamental constitutional rights and that this consent should not be lightly inferred. In fact in *U.S. v. Meulener*, a passenger opened a suitcase only after he was ordered to do so by the marshal at a time when he was not free to leave or to avoid the search.[61] The court therefore concluded that, under these particular circumstances, the search was inherently coercive.

*U.S. v. Blalock*, another earlier case, discussed the requirement of an "intelligent consent," which implies that the subject of the search must have been aware of his/her rights.[62] The logical extension of this reasoning was that for an intelligent consent to be present, it could only embrace the waiver of a known right. In other words, if individuals are not aware of the fact that they have a right; it is difficult to conclude that they knowingly waived it. Remember, again, that this case was decided prior to the 100 percent screening requirement. Second, note that *Lopez* also did not support the contention that airport searches were justified on the basis that they are searches incident to arrest. The simple fact that a search discovers evidence of a violation of a law does not render the search justifiable. The end does not justify the means. A police search conducted in violation of the Constitution is not made lawful just because the police find something illegal.

Returning to the discussion relating to *Terry v. Ohio*, legal scholars have also sought to use the concept of probable cause to warrant an airport search. *Terry* was the first case to recognize the need for police officers to search individuals for the sheer need of protecting themselves and in the interest of public safety. The *Terry* court reasoned, "A police officer may in appropriate circumstances and in an appropriate manner approach a person for purposes

of investigating possible criminal behavior even though there is no probable cause to make an arrest." The court, however, made it perfectly clear that the police officer's conduct must be limited in scope and be reasonable. So what constitutes probable cause? Officers have used everything from a magnetometer alert to an individual fitting a specific profile.

The *Terry* court also commented on whether or not mere government observation constitutes a search regulated by the Fourth Amendment. The court concluded that the decision rests on whether or not the defendant had a legitimate expectation of privacy in the place or thing searched.[63] This kind of rationale has also been used to substantiate the legality of canine searches.

*United States v. Place*, decided in 1983, ruled that the warrantless use of a canine does not violate the Fourth Amendment, because the sniff of a dog only discloses the presence or absence of drugs or explosive residue.[64] The dog cannot reveal a plethora of unlimited information about the items or person searched. The logic is based on the concept that a defendant has no legitimate expectation of privacy for drugs, explosives, or other contraband. Some legal analysts have extended this logic to reach the conclusion that more sophisticated and precision-oriented search equipment at airports may be free of the Fourth Amendment concerns of the past. The *Place* court concluded that the canine search was not very intrusive and also did not expose the person to much embarrassment or inconvenience.

The courts have relied heavily on determining just how intrusive the search is. There are competing values at play. Certainly, the courts have recognized the need to maintain public safety. As the courts and public further understand the continuing need for stringent security measures, the more likely the courts will justify the newer, less intrusive means of airport searching. As early as 1971, in *Barrett v. Kunzig*, the judges supported the government's substantial interest in conducting a cursory inspection at federal buildings, determining that the intrusion outweighed the personal inconvenience suffered by the individual.[65] Such searches have now become commonplace. Further supporting the idea that "some" government observation does not even rise to the level of a search, the court ruled in *Barrett v. Kunzig*, "The term search has been used by plaintiffs. To the extent that term is applied to more than a casual visual inspection, it has no meaning and is without foundation in this record."[66]

The courts have applied the above reasoning to magnetometers at airports. They have once again weighed the minimal invasion of personal privacy and the reasonableness of the security search in the light of the known risks. As early as 1972, the court in *U.S. v. Epperson* simply and concisely analyzed the legality of a search by the use of a magnetometer.[67] The growing need to combat terrorism was self-evident. Consequently, the court expressed the view that "the danger is so well known, the government interest so overwhelming and the invasion of privacy so minimal, that the warrant requirement is excused by exigent national circumstances." The court was quick to recognize that the public viewed the searches as a welcome reassurance of safety to passengers traveling domestically and abroad. Specifically the court stated,

The reasonableness of any search must be determined by balancing the governmental increases in searching against the invasion of privacy, which the search entails. . . . It is clear to us that to innocent passengers the use of the magnetometer to detect metal on those boarding is not a resented intrusion on privacy, but, instead, a welcome reassurance of safety. Such a search is more than reasonable; it is a compelling necessity to protect essential air commerce and the lives of passengers.

The court considered the use of magnetometers perfectly legal right from their initial operation. It is worthwhile to point out that the Constitution does not forbid all searches, just those that are unreasonable. The reasoning applied to magnetometers was soon also applied to X-ray machines searching carry-on baggage at airports. X-ray machines are minimally intrusive of privacy and are also minimally embarrassing, if at all, to passengers. This is true at least with regard to the machines currently in use.

Soon, however, the court in *U.S. v. Henry* differentiated between the X-ray scan and the magnetometer search.[68] The judges resolved that the X-ray scan was a more intrusive search than the magnetometer and that both were subject to Fourth Amendment controls. At the time they also recognized that if passengers had wanted, they could have decided to avoid the X-raying of their carry-on baggage by merely consigning any baggage they did not want searched to the baggage compartment. The magnetometer does not provide such an option, in that passengers can not ship themselves via the baggage compartment. A different set of circumstances is introduced when the only way to avoid search is not to fly. With the advent of 100 percent screening of checked baggage, this will become moot.

## PASSENGERS' RIGHT TO TERMINATE A SEARCH

According to many legal analysts, passengers are deemed to have given consent when they place their bags on the conveyer belt for luggage screening.[69] The judge's decision includes the following: "Those passengers placing luggage on an x-ray machine's conveyer belt for airline travel at a secured boarding area gave implied consent to a visual inspection and limited hand search of their luggage even if the x-ray scan is inconclusive in determining whether the luggage contains weapons or other dangerous objects."[70]

From a security officer's perspective, if passengers were allowed to withdraw after setting off the security system, the deterrent effect of the security system would be undermined. It may even be reasonable to argue that there is no guarantee that they might not return and be more successful later in getting through the security check.

Implicit consent derives much of its justification from the fact that it is a privacy invasion that free society is willing to tolerate as long as the scope of the search is limited to discovering weapons or explosives and is limited in a manner that produces negligible social stigma. It appears the law is still somewhat unsettled. In *U.S. v. DeAngelo*, a traveler submitted his briefcase

for search.[71] The security officer noticed an opaque object, which could not readily be identified. The traveler was advised that his bag would have to be manually searched. The passenger protested the further search of his briefcase and said he would prefer not to take the flight. He was not afforded that option, and narcotics were ultimately found.

The court believed that the circumstances were sufficiently suspicious to cause a reasonably prudent man to conclude the defendant might endanger security officers and passengers. Later in the opinion, the judge specifically stated that "allowing him to withdraw his luggage when the x-ray raised the suspicions of the security officers would frustrate the regulation's purpose of deterring hijacking." *De Angelo* was decided before *U.S. v. Pulido Baqerizo*, in which the court extended the earlier decision. The opinion in *Pulido Baqerizo* added the concept that placing luggage on the X-ray machine conveyor machine automatically provides implied consent not only to scan but also to conduct a manual search if deemed by security personnel to be necessary.

The idea that potential passengers may avoid the search by electing not to fly is somewhat losing favor. Even though there certainly exists no constitutional right to fly, there has been some softening of the hard-core position that passengers have indeed consented to searches in order to fly, but only when the search is directly related to the safety of the flying public. As stated before, marijuana or counterfeit money do not have the ability to bring an aircraft down or provide the means to hijack it.

In the course of litigating these issues, some passengers and later defendants have more vigorously sought to avoid being searched. *U.S. v. Herzburn* clearly involved a more determined and forceful attempt by a passenger to terminate the search.[72] The defendant had placed a shoulder bag on the conveyor belt and the examiner observed a large dark mass on the bottom of the bag. The defendant insisted he did not want the bag searched further, but the airport security officer reached into the bag. At this point, the defendant exclaimed, "I don't want to fly," grabbed the bag, and retreated to the nearest exit. Later the bag was searched after a dog alerted its handlers as to the possibility of prohibited items and the authorities obtained a warrant. The court opinion referred to the *Skipwith* case discussed earlier and restated that an unimpeded exit would diminish the risk to skyjackers and increase attempts to hijack planes.

## THE WAR ON DRUGS

Continuously, airline officials have attempted to reiterate the fact that the airlines are not in the law enforcement business. They have repeatedly argued that the carrier's only legal obligation is to locate weapons. On occasion the courts, in frustration, have gone further. Certainly, procedures for handling attempts to smuggle contraband, when discovered by the airlines, need to be addressed. Criminal activity cannot just be overlooked. Difficult issues arise, however, in determining just how far the airlines need to go to fulfill their duty to every citizen to maintain a safe and lawful atmosphere at airports and

aboard aircraft. These difficult situations are passed along by the airlines to the security officials, who are expected to understand and interpret the law in every situation and to conduct themselves accordingly in every instance. Of course, constant correct decision making constitutes a tall order as attorneys and judges alike struggle with these issues.

In 1973, the federal courts were becoming distressed over the amounts of illegal drugs being smuggled into the United States on commercial carriers. Consequently, in a U.S. district court, in Brooklyn, New York, a judge ordered the U.S. attorney to seize a Braniff DC8. The aircraft, which had carried three persons smuggling drugs from South America, was technically used in the illegal transportation of controlled substances. The federal government had already passed laws to combat the increasing influx of drugs into the United States by statutes that provided for the actual confiscation of vehicles used in transporting narcotics. This well-known law, however, had not previously been enforced against commercial carriers. The seizure in this instance did get the attention of the airlines.

This particular federal action prompted carriers to reexamine corporate policy regarding contraband items. The original legislation, permitting federal agents to confiscate boats and small aircraft, was passed in 1986. It also imposes stiff penalties on the owners and operators of aircraft found to be involved in smuggling or in other fraudulent activities. The legislation was intended to take away the smugglers' means of transporting the illegal goods as well as the tangible results of extremely profitable drug businesses. However, the airlines had not considered themselves subject to this law.

They based their interpretation of the law on theories argued in other case law. Some state courts had reasoned that a common carrier aircraft should not be seized in connection with drugs unless the carrier had been negligent in locating the contraband. Generally, the cases agreed that the carrier was not responsible for drugs found on passengers, in their luggage or in cargo found to be properly manifested, unless the carrier had knowledge of the violation or was "grossly negligent" in preventing or discovering it. Other judges concluded that the aircraft could not be seized and forfeited unless the aircraft's owner, its pilot, or any other employee knew or through the exercise of the "highest degree of diligence" could have known that the contraband was aboard.

It is well-accepted law that no carrier is required to embark upon a full-scale law enforcement effort to discover contraband. The carrier must take steps to ensure that proscribed articles are not knowingly transported. Extraordinary measures to identify contraband items are not required, but just what constitutes reasonable measures will continue to be litigated. Airlines are not often able to analyze or guess what courts will determine to be sufficient effort to locate contraband on an air carrier. Judges are usually willing to permit searches in the name of airport security, citing a special need that benefits all of the traveling public. Extending police power to search, simply for drugs, has not been authorized and will not likely be authorized in the future.

## PASSENGER RIGHTS

Additionally, airport security officials that go beyond what the courts consider reasonable searches are subject to legislation, passed in 1976, that authorizes a person deprived of any constitutional right as a result of state action to bring civil suit against the person who deprived him/her of that right.[73] Even though neither the airlines nor airport security officials have yet to be considered to be engaged in "state action," they have repeatedly been sued for allegedly violating a passengers' constitutional rights.

Clearly, not ignoring contraband is very different than actively searching for it. As discussed previously, the issues are once again fogged when the airlines refuse to cooperate. Sometimes law enforcement officers continue to pursue passenger screening with airline employees as paid informants, without the knowledge of the carrier. When airport security personnel literally have a police officer standing over their shoulder and are encouraged to engage in a search that the officer would not be permitted to effectuate, the courts will raise a red flag and exclude any evidence of contraband found. Airline security officials must not encourage employees to engage in this activity and when discovered it must be stopped. Otherwise, the airlines and contract security officials will be ratifying the conduct of the informants and the courts will not look kindly on the activity. Such conduct could result in the carrier being sued.

One of the most recent cases in this area tried to answer the question, "Can law enforcement authorities use airport security inspections to look for contraband that is unrelated to safety?" The U.S. Court of Appeals for the 9th Circuit, in *United States v. $125,570 Currency*,[74] analyzed the actions of Bonnie Boswella, a flight terminal security officer at the Seattle International Airport, when she noticed a dark mass in a briefcase. On January 5, 1987, Wayne G. Campbell put his locked briefcase on the airport X-ray scanner. After noticing the dark mass, Officer Boswella asked Campbell to open the briefcase. At first he was reluctant but agreed to open it in a private area behind a screen. Karen Kangas, another airport security officer, searched through the briefcase and located a huge sum of money. After inquiring as to Campbell's destination, security released him. Ms. Kangas called Steve Symms, a U.S. Customs Service officer, and informed him about the briefcase and its contents. In addition, Customs was provided with a description of Mr. Campbell. Consequently, for their efforts, they received a reward of $250 for locating currency over $10,000. Later, Mr. Campbell arrived in Los Angeles, where two DEA agents met him. During questioning he admitted that he had about $130,000 in his briefcase, but that the money belonged to a friend of his who had hired him to ransom a stolen painting.

The two DEA agents confiscated the briefcase. They advised Mr. Campbell that he was free to go but he decided to accompany the agents to the DEA office. At the office, the agents asked Campbell to open the briefcase. If he refused, he was told, they would simply obtain a search warrant and open it in any

case. Mr. Campbell therefore opened the briefcase and a significant amount of money was discovered as well as large number of cigarette-rolling papers and a receipt from a Seattle hotel. On the following day, a drug detection dog alerted its handlers as to the possibility of prohibited items when brought into contact with the money; indicating that drugs had come into contact with the currency. As per administrative procedures, the United States filed a civil forfeiture action pursuant to the currency. In response, Mr. Campbell filed a claim to suppress the evidence uncovered by the search. The district court denied the motion to suppress and ruled the currency was rightfully subject to forfeiture, a decision that was later appealed to the 9th Circuit Court of Appeals.

The judge, Alex Koziniske, was concerned with two issues. He considered the idea that the flight terminal security officers were looking more carefully for currency in carry-on baggage because of the potential $250 reward, rather than concentrating on searching for items relating to air safety. The second issue the judge considered was whether Mr. Campbell had in actuality voluntarily consented to the search at the airport, because his expectation of privacy was waived only as it related to the search for weapons or explosives. The judge ruled that the search at the airport had not been conducted within the narrowly construed objectives permitting airport searches solely to ensure airline and airport security. The judge reversed the lower court ruling and vacated the order of forfeiture. Basically, the judge had reasoned that the Air Transportation Act of 1974 requiring all passengers and carry-on property to be screened by security does not extend an exception to the Fourth Amendment to search for contraband or currency.

## NEW LAW IN THE AREA OF SEARCHES

In a departure from recent rulings supportive of police in drug interdiction efforts, the U.S. Supreme Court in *Indianapolis v. Redmond* has held that the use of roadblocks designated to uncover ordinary criminal activities like drug trafficking are unconstitutional.[75] The decision stems from a situation in which police stopped a motorist at a roadblock in a high drug crime area. The man was arrested after police discovered drugs in the car. The motorist challenged the arrest, arguing that there was no probable cause for the search.

In the decision, the court distinguished between roadblocks used to deter drunken driving and illegal immigration from those used to check for random criminal activity. While the previous roadblocks carry implications for public safety and immigration, the latter searches were reasoned to amount to an unreasonable search under the Fourth Amendment. Specifically, Justice Sandra Day O'Connor stated, "We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing." The case evidenced the scrutiny by the court in distinguishing between searches that serve a public safety purpose, like airport searches, and searches specifically conducted in order to detect criminal activity unequivocally unrelated to public safety.

Earlier caught in a fire of controversy over "racial profiling," in 1999, the U.S. Customs Service began imposing limits on its screening of airline passengers to intercept illicit drug shipments. The service has implemented rules that prohibit agents from detaining airline travelers suspected of drug smuggling for more than four hours without the specific approval of a federal magistrate. The policy guidelines also require customs officers to notify an attorney or friend of the passenger, if asked, if the passenger is detained for longer than two hours. In cases where no drugs are discovered, the agents must also assist the passenger in resuming his/her journey.

The high technology crime landscape is another area of expanding law. Experts are closely watching a pending racketeering case against Nicodemo S. Scarfo. FBI agents used a warrant to break into his place of business and put either a program or some sort of "electronic bug" into his computer. According to Scarfo's lawyer, the procedure enables law enforcement to capture every keystroke made on a user's computer.[76] Using a system called TEMPEST, the FBI has the means to recreate a picture on a computer screen from its electromagnetic energy. Another program, called DCS 1000, enables investigators to follow a suspect's Web browsing and e-mail.

As discussed in the federal court case in New Jersey (on appeal), Mr. Scarfo was using a publicly available software program named Pretty Good Privacy, which is a free-encryption program that is usable for e-mail and files. The FBI wanted the password to those files ostensibly so they could collect information on gambling and loan-sharking operations. The government argues that what they did does not rise to the level of a wiretap. Mark Rausch, former head of the Department of Justice's computer crime section, has said, "You really need to understand at what point it captured things, and how it got it back to the government, in order to figure out what the Fourth Amendment concerns are."[77] The defendant's motion to suppress this evidence was denied.[78]

Permitting law enforcement to peek into computers is the wave of the future. Providing such a tool to airport security personnel would enable them to snoop into the computers of passengers and possibly detect information on potential terrorist activity. However, civil libertarians and the courts will likely heavily scrutinize this kind of exploratory investigation.

## NEW TECHNOLOGIES AND THE LAW

Sometimes, new technologies change everything. The use by drug enforcement officials and law enforcement in general of forward-looking infrared devices or FLIR is one of those innovations. Law enforcement has used the equipment, often mounted on helicopters, not only to assist ground law enforcement during dangerous chases but also to establish evidence of indoor marijuana cultivation. The device detects differences in the surface temperature of objects, and can detect the huge amount of heat radiated by the high-intensity grow lights that are needed to successfully grow marijuana indoors.

The constitutionality of the use of FLIR has been upheld on several occasions. A circuit court, in the case of *U.S. v. Pinson*, believed that the defendant

had no legitimate expectation of privacy in the heat emanating from his house.[79] The court took into account the fact that the only information acquired by the FLIR was data. The 8th Circuit developed a two-pronged test for determining what constitutes an expectation of privacy. A legitimate expectation of privacy is considered to exist where "the individual manifests a subjective expectation of privacy in the object of the challenged search and society is willing to recognize that subjective expectation as reasonable." The Supreme Court, however, ruled in 2006 that special heat-seeking devices require a warrant if they are to be used in the search for homegrown marijuana plants; changing the legal landscape completely.

The courts have analogized the expectation of privacy argument to the use of canines and also the placement of garbage left on the curb. These situations have been thought not to have a reasonable expectation of privacy attached to them. In the case of the garbage, it's left out to be taken away. In the case of the dogs, the Court compared the dogs to FLIR, claiming that the dogs merely sniffed the odor emanating from the bags. The court also specifically stated that "none of the interests which form the basis for the need for the protection of a residence, namely the intimacy, personal autonomy, and privacy associated with a home, are threatened by thermal imagery."[80] Consequently, FLIR could easily be utilized for airfield security without much concern about constitutional challenges.

As is common in the law, other courts have disagreed. The 5th Circuit Court, in *U.S. v. Ishmael*, reasoned that FLIR cannot tell the difference between legal heat and heat being used to grow marijuana.[81] For that matter, even the excessive heat radiated from grow lights could be being used to grow basil or a host of other legal plants. They therefore reached the conclusion that FLIR is more intrusive than a dog. Additionally, the dog's sense of smell is clearly not as technologically precise as FLIR, which can detect miniscule heat graduations. Reviewers of both arguments have tended to continue to support the concept that dog-sniffing, FLIR, and garbage searches are all fair game for law enforcement as investigative techniques. Dogs and FLIR especially both involve sense-enhancing equipment. The degree of detectability is really not an issue.

Other technological innovations have presented additional court reviewable topics. U.S. Customs officials at six U.S. airports are currently using a body search X-ray to examine drug-smuggling suspects. The system basically sees through clothes. Specifically, passengers who cause customs officials to become suspicious are required to choose between a pat-down search or standing in front of a machine that arguably renders an image of the suspect naked.

Customs officials "had hoped that the new technology would help quiet a controversy over the agency's searches, which civil libertarians contend focus too much on minority passengers. A hands-off approach, customs officials reasoned, would seem less intrusive."[82] However, the technology is so good it reveals just about everything. In other words, airport security officials might

be able to view a little more than the average citizen is personally inclined to show to a stranger. Modesty has nothing to do with the carriage of weapons. Pulsed radar scanners, which pretty much produce an image of an individual's naked body, are clearly intrusive.

In summary, the courts currently do not require a physical intrusion in order to determine that a search has taken place. However, how much of an intrusion, what degree of expectation of privacy is involved, and how reasonable the search is will all play into any future court analysis. The problem evolving is that as technology improves, it becomes easier to characterize information as exposed, because technology can now expose it. By systematic practice, passengers have been conditioned to expect some sort of search. Just how intrusive a search is permissible is still the question to be litigated fully.

## CONCLUSIONS

Admittedly, the law is a complicated matrix of sometimes conflicting legislation, policies, and opinions. However, every security official, whether a state agency employee or a privately employed individual, should have a basic understanding of the Fourth Amendment and how it applies to airport searches. Since the Fourth Amendment is currently only applicable when a state agent is conducting the search, private security must be careful not to wander into discretionary authority that rightfully belongs to the police. Whether contract airport security personnel continue to fall into the nonstate agent category has so far generally been decided in the negative. However, the distinctions between private and public "policing" are blurring and it will remain to be seen if this decision persists. The water becomes even murkier when the airport security officer is an off-duty police officer or a federal employee.

The Fourth Amendment also protects passengers only against unreasonable searches and seizures, not against all searches. Additionally, just what is considered reasonable is often defined in terms of how serious the threat is conceived to be. During the Persian Gulf War, the threat was accepted as being significantly higher than normal, and the public and the courts were willing to adjust the expectations of privacy. This acceptance was clearly expanded again after September 11, 2001. Another issue pertains to how much privacy a passenger expects to receive at an airport. Passengers expect to be searched for dangerous weapons and explosives because that is the public policy function of the search. Therefore, it may be perfectly acceptable to have passengers screened by a metal detector and their carry-on luggage scanned. Having them literally undress in front of an X-ray machine may result in a different conclusion. The courts, consequently, will likely continue to evaluate the extent of the permissible intrusion. Advances in technology will likely strain the courts' patience with the airlines' wish for speed versus the level of intrusion.

There are outright exceptions to the Fourth Amendment, including administrative searches, border searches, and consent searches. Generally, the

judiciary has concluded that passengers do consent to airport searches but the judiciary also seems to accept that they are administrative in nature and serve a distinct public need. If the courts believe that security has gone too far, the exclusionary rule may come into play. It is meant to keep the state, via its police function, at an appropriate distance from individual rights. If the state chooses arbitrarily to overstep its bounds, the rule will deny it a conviction against the perpetrator of the alleged crime. According to many criminologists, the rule has proved an effective deterrent, but the rule has also attracted much criticism. It is difficult to know just how many police officers or federal agents have restrained their conduct fearing the implications of the exclusionary rule. Consequently, some exceptions have been carved out. Most importantly, the good faith exception and the exigent circumstance exception are the most frequently utilized. Whatever the ultimate decision of the courts regarding a particular search or procedure, the public's attitude toward the search will play a large part in determining its acceptability.

The reasonableness and extent of that attitude from the public can become strained even in today's tense environment. The perception that it is unreasonable to search "little old ladies" while "suspicious characters" are permitted to board unhindered will continue to pose a challenge to security officials. Additionally, any legal search can quickly become illegal when security goes outside the boundaries of reasonableness. The allegation of the selection of only "good-looking" flight attendants for pat-down searches at Sky Harbor Airport in Phoenix is a good example. Most people do not mind being searched in order to feel more secure when they fly. However, when the searches provide neither security nor a sense of security, they lose their public safety purpose and the support of the traveling public.

## NOTES

1. *Harris v. United States*, 376 U.S. 643 (1961): 649.
2. "American Profile of John Walker Lindh," *BBC News*, news.bbc.co.uk/1/hi/world/americas/1779455.stm.
3. U.S. Constitution, Art. I, Sec. 4, Clause 6.
4. *U.S. v. Morgan*, 774 F.2d 1215 (6th Cir. 1985).
5. *U.S. v. Ross*, 32 F.3d 1411, 1413 (9th Cir.), quoting *U.S. v. Davis*, 482 F.2d 893, 904 (9th Cir. 1973).
6. *Terry v. Ohio*, 392 U.S. 1 (1968).
7. *Veronia School District 47J v. Acton*, 115 S.Ct. 2386 (1995).
8. *Veronia School District 47J v. Acton*, 2392.
9. *Veronia School District 47J v. Acton*, 2388.
10. *U.S. v. Skipwith*, 482 F.2d 1272 (1973).
11. *U.S. v. $124,570 U.S.Currency*, 164 F. 3d 462 (9th Cir., 1989).
12. *U.S. v. Roman-Marcon*, 832 F. Supp. 24 (1993).
13. *Terry v. Ohio*, 27.
14. "Jury's Mixed Verdict in Cop Trial," *UPI Online*, April 3, 1998, www.upi.com.
15. Karen M. Hess and Henry M. Wrobleski, *Police Operations Theory and Practice* (St. Paul, MN: West Publishing Co., 1997), 122.

16. *Terry v. Ohio*, 392 U.S. 1 (1968).
17. *U.S. v. Cortez*, 449 U.S. 418 (1981).
18. *U.S. v. Epperson*, 454 F.2d 769 (4th Cir. 1972).
19. *U.S. v. Sokolow*, 490 U.S. 1, 109 S.Ct. 1581 (1989).
20. *Schneckloth v. Bustamente*, 93 S.Ct. 2014 (1973); 412 U.S. 218.
21. *U.S. v. Ruiz-Estrella*, 481 F.2d 723 (2nd Cir. 1973).
22. *U.S. v. Albarado*, 495 F. 2d 799 (2nd Cir. 1974).
23. *U.S. v. Lopez*, 328 F. Supp. 1077 (1971).
24. *U.S. v. Lopez*, 76F.3d 133a (1969).
25. *U.S. v. Lopez*, 482 F.2nd 893,
26. *U.S. v. Favela*, 247 F.3d 838, 2001,
27. *U.S. v. Eustaquio*, 198 R.3d 1068 (8th Cir. 1999).
28. *Atwater v. Lago Vista*, 121 S.Ct. 1536: 1567 (2001).
29. *State v. Kearns*, 867 P.2nd 903 (1994).
30. *Martinez v. Fuerte*, 428 U.S. 543 (1976).
31. *U.S. v. Ramsey*, 431 U.S. 606, 97 S.Ct. 1972 (1977).
32. *U.S. v Sarkissian*, 841 F.2nd 959 (9th Cir. 1988).
33. John Gales Sauls, "Emergency Searches of Premises," Part I, *FBI Law Enforcement Bulletin*, March 1987, 23.
34. *Warden v. Hayden*, 387 U.S. 284 (1967).
35. *Mincey v. Arizona*, 437 U.S. 385 (1978).
36. *Mincey v. Arizona*, 392.
37. *Mapp v. Ohio*, 367 U.S. 643 (1961).
38. *Mapp v Ohio* also held that the prohibitions of the Fourth Amendment were fully applicable to the states under the Amendment's due process clause; evidence obtained by illegal searches by state or federal officers was admissible in state court.
39. *U.S. v. Afanador*, 567 F2d. 1325 (5th Cir. 1978).
40. *Reid v. Georgia*, 448 U.S. 438, 100 S.Ct. 2752 (1980): 441.
41. *Michigan v. Summers*, 452 U.S. 692 (1981).
42. *Brinegar v. U.S.*, 338 U.S. 160 (1949).
43. *County of Riverside v. McLaughlin* (1991); Rolando V. Del Carmen, *Criminal Procedure for Law Enforcement Personnel* (Monterey, CA., Brooks/Cole Publishing, 1987), 63.
44. *U.S. v Leon*, 468 U.S. 897 (1984).
45. *Weeks v. U.S.*, 232 U.S. 383 (1914).
46. *Wolf v. Colorado*, 338 U.S. 25 (1949).
47. *Lustig v. U.S.*, 338 U.S. 74: 79.
48. *Elkins v. U.S.*, 364 U.S. 206 (1960).
49. *Rochin v. California*, 342 U.S. 165 (1952).
50. *Burdeau v. McDowell*, 245 U.S. 465, 41 S.Ct. 574 (1921).
51. *People v. Superior Court of Los Angeles*, 449 v. P.2nd 230, 74 Cal. Reporter 294 (1974).
52. *U.S. v. Pryba*, 312 F. Supp. 466 (1970).
53. *Wolflow v. U.S.*, 391 F.2nd 61 (1968).
54. *Burdeau v. McDowell*, 256 U.S. 465, 41 S.Ct. 574 (1921).
55. *Trupiano v. U.S.*, 68 S. Ct. 1229, 334 U.S. 699 (1948).
56. *U.S. v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2nd 85 (1984).
57. *Byars v. U.S.*, 47 S.Ct. 248 (1927).
58. *Burdeau v. McDonell*, 256 U.S. 465 (1921).

59. *People v. Tarantino*, 45 Cal. 2nd 590, 290 P.2nd 505 (1955).
60. *U.S. v. Lopez*, 328 F. Supp. 1077 (1971).
61. *U.S. v. Meulener*, 351 F. Supp. 1284 (1974).
62. *U.S. v. Blalock*, 255 F. Supp. 268 (1966).
63. *Terry v. Ohio*, 392 U.S. 1 (1968): 9.
64. *United States v. Place*, 462 U.S. 696, 707.
65. *Barrett v. Kunzig*, 331 F. Supp. 266 (1971).
66. *Barrett v. Kunzig*, 331 F. Supp. 272 (1971).
67. *U.S. v. Epperson*, 454 F.2d 769 (1972).
68. *U.S. v. Henry*, 615 F.2d 1223 (9th Cir. 1980).
69. *U.S. v. Pulido-Baquerizo*, 800 F.2nd 899 (1986).
70. *U.S. v. Pulido-Baquerizo*, 800 F.2nd 902 (1986).
71. *U.S. v. DeAngelo*, 584 F.2d 496 (4th Cir. 1979).
72. *U.S. v. Herzburn*, 723 F.2d 773 (11th Cir. 1984).
73. 42 USC Section (1983).
74. *United States v. $125,570 Currency*, 873 F 2nd 1240 (9th Cir. 1989).
75. *Indianapolis v. Redmond*, 531 U.S. 32, 121 S.Ct. 497 (2000).
76. *U.S. v. Scarfo*, 263 F.3rd 80 (3rd Cir. 2001).
77. Associated Press, "FBI's Electronic Snooping Headed for Court Test," *Star Tribune*, Minneapolis, MN, July 29, 2001, A13.
78. *U.S. v. Scarfo*, 180 F. Supp. 2nd 572 (2001).
79. *U.S. v. Pinson*, 24 F3d 1056 (8th Cir. 1994).
80. In *U.S. v. Pinson*.
81. *U.S. v. Ishmael*, 843 F. Supp. 205, affirmed 48 F.3d 850 (1995).
82. Michael Allen, "Are These X-Rays Too Revealing? Targeting Drug Smugglers. Airport Screening Device Sees Right through Clothes," *Wall Street Journal*, Thursday, March 2, 2000, B1, B4.

# CHAPTER 4

# Aviation Security and Response Management

*Kathleen Sweet*

The tragic events of September 11, 2001, brought about many changes in the way airports execute security procedures. However, recent changes are even more significant than those that took place over the last five years. A comparison of the time when airport security was nonexistent to the tedious process that it is today reveals the impact that air travel has on the American way of life.

Air travel has become an essential element in the way people live, and it must be protected and secured. According to the Department of Homeland Security, 730 million people travel on passenger jets every year.[1] Security procedures have become a rite of passage. Passengers pass through a doorframe-like metal detector that beeps when anything, from loose change to a belt buckle, passes through it. Passengers place carefully packed belongings on a conveyer belt that pulls the bags into a dark tunnel to be X-rayed and inspected. Passengers may even be required to remove shoes, socks, and jackets and even be restricted in the amount of liquid they can carry on board.

But there was a time, only 35 years ago, when passengers could walk straight from the ticket counter to the terminal and onto the plane without being stopped. Considering the airport security measures in practice today, it is hard to believe that in 1972 there were no aviation security precautions in effect at all.

Aviation security has become one of the most important and controversial aspects of travel. Nonetheless, since the 1950s, the need for aviation security has repeatedly necessitated the expansion of the security infrastructure. The first recorded hijacking occurred in 1930, when Peruvian rebels hijacked a mail plane for use in dropping propaganda leaflets on Lima.[2] Twenty years

later, Jack Graham committed one of the first criminal acts on an aircraft in the United States. In 1955, he sought to collect on an insurance policy on his mother and literally planted a bomb in her luggage. After succeeding in killing all 44 on board, he was later captured and sentenced to death.

## NATIONAL REGULATIONS

A U.S. task force developed an airline passenger preboarding screening system to deter hijackers as early as 1978. The screening system combined a behavioral profile with a metal-detecting device to identify persons who could be potential hijackers, but the system has not kept pace with the changes that have occurred.[3] National regulatory bodies have differing security requirements, making it difficult for passengers to understand the rules and to prepare to comply with those rules when abroad. An agreed-upon international standard in which the security requirements for aviation are met and passengers understand the process would have real benefits at airports. Airport security procedures differ by country and, in some cases, the regulation applied or the interpretation of the regulation differ even from airport to airport within a country. There are also clear differences in passengers' levels of awareness of requirements based on nationality and passenger type.[4]

For example, U.S. nationals, who are typically well aware of the security requirements at a home airport, routinely take off shoes and belts. When traveling from an airport outside the United States, it is not uncommon to see U.S. passengers remove these items for X-ray screening; even when this action is not requested or required of them. It does not affect the delivery of security but it does extend the processing time per passenger, adding both preparation time and move-away time after passing through security.

The differences in airport passenger security are particularly evident at hub airports where there is a high frequency of international passengers. The lack of uniformity in international procedures contributes to a reduction in passenger throughput rates. Confusion as well as increased conversation with screening officers due to "unfamiliar" screening demands or unnecessary preparation at the X-ray in feed further extends the screening process and therefore the waiting times for other passengers.

## PREBOARDING SCREENING

The preboarding passenger screening process was made statutory with the enactment of Public Law 93–366. This law added Section 315 to the Federal Aviation Act of 1958, stating, "The Administrator shall prescribe or continue in effect reasonable regulations requiring that all passengers and all property intended to be carried in the aircraft cabin in air transportation or intrastate air transportation be screened by weapon-detecting procedures or facilities employed or operated by employees or agents of the air carrier, intrastate air carrier, or foreign air carrier prior to boarding the

aircraft for such transportation."[5] Additionally, Section 108.9(a) of Federal Aviation Regulation 10811 states that every air carrier certified by the Civil Aeronautic Board (passenger or public charter operations) is "required to conduct screening under a security program," shall use the procedures included, and the facilities as well as the equipment described, in [the Federal Aviation Administration] approved security program to prevent or deter the carriage aboard airplanes of any explosive, incendiary, or deadly or dangerous weapon on or about each individual person or accessible property, and the carriage of any explosive or incendiary in checked baggage or certain restricted airport areas.[6]

The amendments also addressed law enforcement and civil aviation security by ensuring that only those persons who are authorized to carry firearms are permitted to carry them aboard an aircraft or into certain restricted airport areas. The first airport screening devices used, referred to as magnetometers, began as a retrofit from the machinery used in the logging industry to prevent nails (metal) from severely damaging saws.[7] Later, the bombing of Pan Am flight 103 resulted in the concept of passenger baggage reconciliation and another new method of passenger and baggage screening; requiring airlines to match the passenger to the checked baggage.

## SEPTEMBER 11 CHANGES

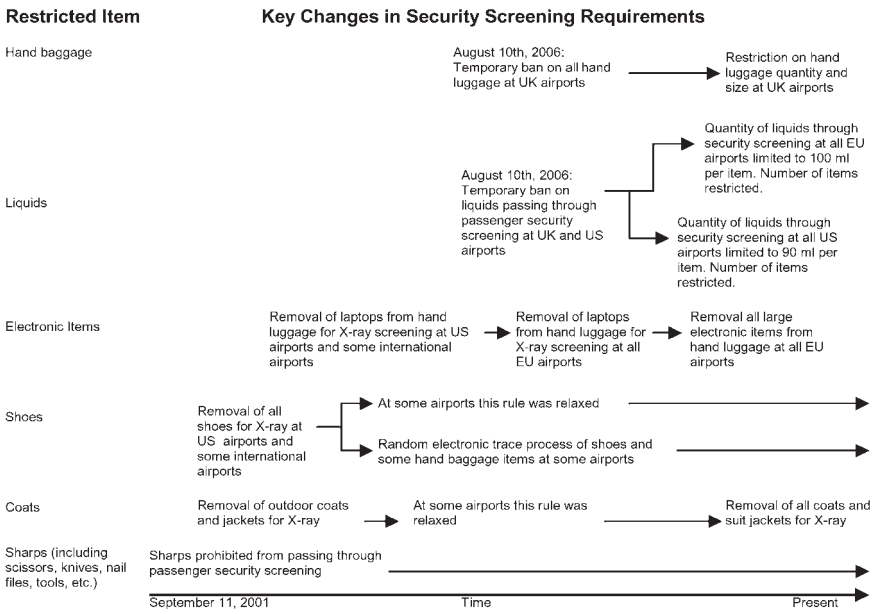
On September 11, 2001, a series of coordinated terrorist attacks resulted in tumultuous changes in processing passengers. An overview of key developments over the past five years demonstrates how quickly the requirements have evolved (see Figure 4.1).

Terrorists used the actual aircraft as the weapon, intentionally crashing commercial airliners into the north and south towers of the World Trade Center. A third aircraft hit the Pentagon and a fourth aircraft crashed into a field outside of Somerset, Pennsylvania, after passengers attempted to retake the plane. It has been speculated that the intended target was in Washington, DC. The attack resulted in 2996 people confirmed killed, along with the 19 hijackers.

To examine the security deficiencies pre–September 11 and the ways they were exploited, Congress created the National Commission on Terrorist Attacks upon the United States,[8] commonly known as the 9/11 Commission, which strongly recommended government supervision of airline screening.

Prior to September 11, aviation security was a joint venture. The FAA was responsible for the safety and security of aircraft and maintained direct oversight of screening operations, yet it employed fewer than 900 special agents to oversee the operations at 429 commercial airports. The airlines were responsible for passenger screening. When Congress enacted the Aviation and Transportation Security Act (ATSA), authority was transferred from the FAA and the airlines to the Transportation Security Administration (TSA).[9] The ATSA, Public Law 107–071, created the Transportation Security Administration, and

**Figure 4.1**
**Response Management and Aviation Security**




although TSA was initially placed in the Department of Transportation, the Homeland Security Act, Public Law 107–296, later moved TSA under the authority of the newly formed Department of Homeland Security (DHS).[10]

Currently, TSA screeners are over 60,000 strong and screen virtually all passengers and checked baggage.[11] Public Law 107–071 also mandated that TSA protect all commercial aircraft by November 19, 2002. New measures included the hardening of cockpit doors and the overhauling of the Federal Air Marshal (FAM) Program.

TSA was additionally encouraged to create and evaluate other programs that might provide supplementary layers of security. Subsequently, the Federal Flight Deck Officer (FFDO) Program allowed the arming of specially trained pilots. Mandates to implement checked baggage and screening procedures,[12] screening all checked baggage with explosive detection systems, the implementation of risk-based objectives, air cargo screening, and improvements in screening technology were all authorized for rapid completion but were all given extended deadlines before they were ultimately completed.[13]

ATSA also provided for a pilot program, known as the PP5, to be established one year after ATSA was signed into law. This provision permitted screening at participating airports to be performed by employees of qualified private screening companies, with oversight from federal authorities. Private companies involved in the pilot program work under TSA supervision and hire personnel using the guidelines that TSA uses for its own screeners. TSA provides the training materials and instruction for all the private screeners, and they are held to

the same standards and mandates as the federal screeners. The airports initially selected for participation in PP5 included San Francisco International Airport, Kansas City International Airport, Greater Rochester International Airport (in New York State), Jackson Hole Airport, and Tupelo Regional Airport.

Fifteen months after the inception of the PP5, BearingPoint, a private assessment firm under the direction of TSA, began an evaluation of the performance level of the PP5 participants. The independent evaluation made the following determinations:

- *Security effectiveness:* There was no evidence that any of the PP5 airports performed below the level of federal airports.
- *Cost:* The cost to perform the screening function at the five airports was similar to the estimated cost of federally conducted security operations at the same airport.
- *Customer service and stakeholder impact:* Data indicated that customer satisfaction at the Category X and I airports was mixed. For the other airports, there was insufficient data to draw any conclusions. However, a qualitative survey of stakeholders revealed no significant difference between privately and federally screened airports.[14]

This encouraging evaluation permitted TSA officials to continue the PP5 pilot program as a permanent program, now referred to as the screening partnership program (SPP) or the "opt-out" program. The SPP program was based on operational experience from the PP5 program; it outlined a cost-effective, seamless transition to an SPP environment. The five airports originally selected to use private screeners have already renewed the original contracts for private screening. Some private screening contractors have also expressed an interest in expanding operations further, to include additional airports once others are allowed to opt out of the federal screening program. For example, Covenant Aviation Security has been renewed at San Francisco International airport as a preferred contractor, and managers have used the relationship to collaborate on further security measures, such as the installation and current use of closed circuit television systems to monitor security lines, rotate screeners, and minimize wait times.[15]

## THE PATRIOT ACT: IMPLICATIONS FOR AIRPORT SECURITY

Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, also known as the USA PATRIOT Act.[16] This act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. Additionally, the secretary of the treasury is vested with regulatory powers to combat corruption in U.S. financial institutions for foreign money-laundering purposes. The act seeks to close our borders to foreign terrorists and to detain and remove those within our borders. Furthermore, it creates new crimes, new penalties, and new procedural

efficiencies for use against domestic and international terrorists. Although the act is not without safeguards, critics contend that some of its provisions go too far. Although it grants many of the enhancements sought by the Department of Justice, others are concerned that it does not go far enough.

One subtle point in the act establishes minimum new customer identification standards and record keeping and recommends an effective means to verify the identity of foreign customers. In September 2003, President Bush issued Homeland Security Presidential Directive 6 (HSPD-6), establishing a Terrorist Screening Center (TSC) to consolidate the government's approach to terrorist screening.[17]

The Transportation Security Administration has interpreted the act's guidance and proposed all passengers boarding flights be screened against the consolidated terrorist screening database (TSDB) maintained by the U.S. government prior to the flight's departure.[18] TSA introduced Secure Flight in August 2004, shortly after the agency abandoned plans for its predecessor, the second generation Computer Assisted Passenger Prescreening System (CAPPS II). CAPPS II would have examined commercial and government databases to assess the risk posed by each passenger: green for minimal threat, yellow for those deserving of heightened security, and red for those who, judged to pose an acute danger, would be referred to law enforcement for possible arrest.

CAPPS II was scheduled for a test run in the spring of 2003 using passenger data provided by Delta Airlines. One citizen, Bill Scannell, who promoted a boycott of Delta Airlines, wrote, "The idea of citizens having to undergo a background investigation that includes personal banking information and a credit check simply to travel in his or her own country is invasive and un-American. The CAPPS II system goes far beyond what any thinking citizen of this country should consider reasonable."[19] Following a public outcry, Delta refused to provide the data and the test run was delayed indefinitely. Ultimately, in the summer of 2004, TSA abandoned CAPPS II, due in part to privacy and security concerns that could not be resolved.

One finding of the 9/11 Commission Report states that the "improved use of 'no-fly' and 'automatic selectee' lists should not be delayed while the argument about a successor to CAPPS continues."[20] TSA will also build a "random" element into the new program to protect against those who might seek to reverse engineer the system. Secure Flight will automate the vast majority of watch list comparisons; will allow TSA to apply more consistent procedures where automated resolution of potential matches is not possible; and will allow for more consistent response procedures at airports for those passengers identified as potential matches.

Prohibitive costs, long security lines, and questionable effectiveness in preventing attacks have impeded passenger screening initiatives. Significant infrastructure changes have been made at several airports to accommodate new screening devices, and passengers have been subjected to long lines in airport lobbies awaiting screening. Passenger screening system designs must consider the potential impact of cost, space, throughput, and effectiveness.

## AIRPORT POLICING

Since September 11, proper airport policing also has become a significant issue including the following concerns: controlling the entry and exit of people in an airport; ensuring security in and around aircraft, taxiways, and runways; and maintaining a visible presence throughout the airport terminals and passenger areas. Procedures for allowing the entry of personnel and vehicles into the airport perimeter, where access to runways and aircraft are easily attained, have been improved, but more training for police officers in the unique airport environment is warranted.

## THE FEDERAL AIR MARSHAL PROGRAM

Federal Aviation Administration (FAA) Order 1650.6 formerly governed the program, which had been authorized in the Federal Aviation Act of 1958, the Anti-Hijacking Act of 1947, and the International Security and Development Cooperation Act of 1985 (Public Law 99–83). The program was intended to establish a covert, armed security force capable of rapid deployment. The precursor of the Federal Air Marshal Program, formerly known as the Sky Marshal Program, was announced in a Department of Treasury news release dated as long ago as October 1970.

When the perceived need for armed agents first arose, former Secretary of the Treasury David M. Kennedy and Secretary of Transportation John A. Vople were responding to President Nixon's call in September 1970 for armed personnel on U.S. commercial flights. The original members were a temporary force recruited from the Customs Bureau, the FAA, the FBI, the CIA, and the military. Eventually a permanent force of 1,500 civilians was established.

Unfortunately, the original Sky Marshal Program proved to be ineffective. The program clearly enjoyed some success but proved incapable of stopping the continuing attempts to hijack aircraft. Early on, the director of civil aviation security for the Department of Transportation, Lt. Gen. Benjamin O. Davis (USAF, Ret.), recognized the need to switch primary security efforts from the aircraft to the ground.[21] Time would prove that even aircraft with both an FBI agent and a sky marshal on board were not immune from incident.

Once the aircraft is in flight, the hijackers are already on board and the presence of agents has done little to deter hijacking attempts. It was therefore determined fairly early on that the better security solution was preventive in nature and better pursued on the ground. Prevention of access to the airport or aircraft was and remains a crucial key to safety. Apparently, that lesson will have to be relearned.

The airlines also considered the coverage in the original Sky Marshal Program too sparse and feared a midair shoot-out. The debate over the Sky Marshal Program raged for years. The FAA responded to complaints from the air carriers by charging that the airlines were preoccupied with efforts not to inconvenience the passengers instead of focusing on safety. When

mandatory 100 percent passenger screening came into force in 1972 in deterring hijacking, the need for airborne law enforcement agents seemed to lose support. Eventually the program fell into disrepair. The number of active agents was reduced to as little as three dozen prior to September 2001. The government is now considering a revitalized training program as key to the success of an upgraded federal air marshal program.

Currently, the FAMs aboard aircraft are some of the best marksmen in the world. They are highly trained, and their firearms training currency requirements are some of the most stringent in law enforcement, in spite of the fact that recent reductions in training have been criticized. The "Certified Protection Professional" certification program (American Society for Industrial Security) has been acknowledged by TSA as the only "security management designation" that will be recognized on the application form for new air marshals. Other certifications include sworn civilian law enforcement agent, emergency medical technician, private pilot and licensed attorney. The FAM Program and continues to provide extra security aboard high-risk routes with renewed vigor since September 11, though with less than enthusiastic support from the airlines and professional pilot associations. The agents are deputized as special deputy U.S. marshals.

The program received a great deal of attention after the hijacking of TWA Flight 847 on June 14, 1985. Captain Testrake and his crew were hijacked and the media plastered photographs of the event all over the world, indicating to the terrorists that the media and the public could not get enough of it. In response to the dramatic events relating to Flight 847, the FAA drafted and implemented Federal Aviation Regulation 108.14, which required scheduled carriers and public charter operators to carry federal marshals on a priority basis, without charge, even if it required bumping a paying customer. The new regulation also corrected a gap in the regulations, which had not provided for the deadheading of agents, that is, how do they get back home after completing a working flight in one direction only.

The Federal Air Marshal Program currently has its training facility and airline security research facility located at the Williams J. Hughes Airport and it now falls under the purview of the Transportation Security Administration.[22] Using a wall full of computer-generated maps, TSA tracks the flight path of each flight with an air marshal on board, and supporting documents indicate the travel schedule of each marshal. The TSA currently employs 45,000 people and is financed with a $4 billion supplemental spending bill from Congress.[23]

The agents receive special training and regularly travel on U.S. air carriers on high-risk routes. They are among the very few people who are authorized to carry firearms on board aircraft and use them if necessary. Additionally, as federal agents, they are permitted to make arrests without a warrant when certain felony offenses against the United States can be reasonably shown to have been committed or to be in the process of being committed. Today, the FAM Program is just one of the tools used by air carriers, airport security officials,

and law enforcement agents in combating the threats to civil aviation. The FAM agents continue to fly millions of miles a year, blending into the crowd of other passengers unbeknownst to a vast majority of them.

However, the debate is back. Rep John Sweeney (R, NY) a member of the House Appropriations Subcommittee, has been quoted as saying, "We need to start seeing some results that are equal to the huge investment that we're making."[24] The program always seems to gain attention and support after a significant event. Administrations use the public's fear to support the need for the air marshals, but after the hullabaloo dies down, their practical usefulness, aside from a perception of safety on the part of the traveling public, dims considerably.

The program has changed considerably over the years. As long ago as the 1970s, administrators recognized that the program was one tool in the airport security toolbox but not the definitive solution to airport security. Before September 11, 2001, the program had a $4 million budget and about 33 armed officers who flew on international flights. A year after September 11, thousands of marshals and a budget of over a billion dollars have not resulted in concrete proof that the marshals have foiled a single hijacking attempt. The mere fact that an officer is on board does not mean the aircraft will not be hijacked or destroyed.

A major problem is that it is logistically impossible to have an officer on every flight. It is even impossible to have an officer on every aircraft considered to be at some higher risk. In an attempt to cover more aircraft, the program rushed to hire marshals. However, in the rush to grow the agency got ahead of itself. Marshals have complained that poor scheduling, inadequate training, insufficient supervision, and cutbacks in marksmanship training have hampered the force. At one point the agency was hiring approximately 800 marshals a month. The administration of such a process carries its own problems. The question arises, therefore, as to whether the public is getting sufficient protection, considering the cost.

Most recently, the American government has sought to force European airlines to have similarly trained law enforcement personnel on board aircraft destined for the United States. French and British pilots literally revolted over the demand. The effectiveness of the problem is clearly in question and the costs are astronomical. The inability of intelligence officials to accurately designate which fights are truly "high-risk," in conjunction with the fact that marshals simply can not be placed on all flights, brings the program into question.[25] In fact, the hit-and-miss security benefit appears similar to the statistical likelihood of whether the plane will be hit by an asteroid. The program arguably provides the perception of protection instead of real protection. The presence of marshals is really not going to prevent a terrorist attempt, because the terrorists neither know which flights will have them aboard nor in reality care. The hijacking and subsequent media attention are goals in and of themselves.

The issue came to the forefront once again when U.S. intelligence claimed to have uncovered plans for a September 11–style incident. As a result, 10

U.S.-bound flights were grounded during the 2003/2004 end-of-year holidays. An informant tipped off authorities the weekend before Christmas that Islamic extremists intended to hijack flights operated by British Airways, Air France, and Aero Mexico, possibly with the intention of attempting to crash them into nuclear power plants.

## RAPID CHANGES WORLDWIDE

In 2006, in a sign of the times, the security level was raised to "critical" at all United Kingdom airports at a moment's notice. There was no advance warning, no prior discussion of measures with airport operators, ground handlers, and airlines, and no time to prepare equipment, staff, and signs. Hand baggage was prohibited, and passengers were permitted to carry only a wallet and passport through security screening; all other items had to be processed as hold baggage. Additionally, every passenger had to be hand searched. In the ensuing chaos, thousands of passengers missed flights, some airlines cancelled up to a quarter of the scheduled flights, and thousands of bags were left stranded. At the main United Kingdom airports, the check-in concourses and curbs filled with queuing passengers and, of course, passengers suffered enormous uncertainty and anxiety.

As the security position changed over subsequent weeks, the requirements were gradually relaxed. First it was acceptable to carry one small bag containing no liquids; then the bag size increased but still no liquids were allowed; later one bag with limited liquids was permitted per passenger.[26] The United States has continued mandating these requirements, though many European airports do not.

In an unpredictable global security environment, the only certainty in aviation security is that there will be change, changing security requirements and changing technologies. Every change adds complexity to the passenger security screening process. Layer upon layer of change, often without engineering the process, impacts the rate of throughput and productivity of the entire operation. The operation becomes slower, more lanes need to be provided, and the conflict over the use of space in terminals and the time spent in lines intensifies.

There are two change-related areas that contribute to this effect: With the introduction of each new regulation, and therefore a change in processing, a change in the performance of the screening lane can be expected. A typical example involves the European Union (EU) requirement to remove all jackets and coats prior to passing through the walk-through metal detector (WTMD). This raises the number of items per passenger passing through the screening process by at least 0.5 of an item at peak time in most terminals. Given that one of the limiters of the screening process is the number of items or images that the X-ray machine can view in each hour, an increase from, say, 1.5 images to 2 images per passenger makes a notable difference. Another effect of the new requirement is that the process of collecting items after

screening and moving away from the lane takes more time, and there is an additional half an item per passenger on the out feed conveyor (postscreening). The process constantly needs to be reengineered.

## PLANNED INTEGRATION AND IMPROVED COMMUNICATION

In the typical security screening process, the limiting factor should be, in most cases, the X-ray machine. However, in reality, the ability to get passengers prepared for the process is the actual limiter. To apply a manufacturing analogy, raw material is arriving unprepared at the start of the production line, so the line is idle while the material is being prepared for the process. In most cases where there is excess demand for production, an idle line is more costly than ensuring that material is well prepared and available in consistency with the capacity of the line. Thus, the increased preparation demands of the new Transportation Security Administration and European Union aviation security regulations, requiring the removal of coats and electronic items from cases for screening as well as restricting the carriage of liquids, will exacerbate this problem if simply added on to the existing process.

To prevent this from happening, an airport operator should identify the most appropriate approach to integrating process modifications and quantify its effect on production rates for the full security process and passenger waiting times. The more effective and thorough the preparation of the passenger, the greater the probability that the passenger will not set off the alarm unnecessarily, for example, by failing to clear metal items from pockets. Taking actions to minimize the number of items to be scanned per passenger will maximize the available capacity of the X-ray machine. Ensuring that the collection area is a suitable size will enable the perfect number of passengers to collect their belongings and with them move away, ensuring that the production line does not need to stop while collections are completed. Improved communication with passengers to increase their awareness of preparation requirements should form part of any optimal solution.

As passenger demand grows and process complexity increases, it may be suggested that passenger security screening, in its current form, has a limited life.[27] This leads us to consider what the security requirements of the aviation industry will be in the future: whether it will be enough to secure passengers as they cross the landside-airside divide at airports, and whether the existing processes will be capable of handling the volumes of passengers and the threat identification demands of the future.

## INTERNATIONALIZATION OF THE PASSENGER SECURITY SCREENING PROCESS

The idea of setting international standards—regulating the setup, equipment, processes, and rules for airport passenger security screening operations

worldwide—is an idea whose time has come. Such a development would reduce passenger uncertainty; it would be clear what is required of each individual at every airport visited. Additionally, there would be confidence that transit passengers and baggage have been through recognized security checks at the airport of origin, perhaps eliminating the need to screen them again. Recent developments in aviation security have made some progress toward achieving cross-border standards. However, even in these recent changes, variations still exist: EU regulations allow a maximum of 100 ml per liquid container; the U.S. maximum is 90 ml. Achieving global standardization would be a major undertaking. Agreement from all nations, definition of the optimal screening process, funding and implementation worldwide, and the establishment and maintenance of international controls are just some of the obstacles that the regulating body would face.

## PROHIBITING HAND LUGGAGE

One way to reduce the risk of threat and to reduce the task of screening would be to prohibit hand baggage, permitting passengers to carry only essential items—wallet and travel documents—as in the United Kingdom on August 10, 2006. This is a most contentious issue. It raises the question of airport and airline customer service. Can a long-haul passenger really be expected to travel for 24 hours without personal items, except for those that can be bought airside? Would a frequent short-haul business traveler be prepared to regularly endure the traditional processing and waiting time required to check in baggage? Or would alternative methods of short-haul transportation be sought, during which the passenger can work on her/his laptop and is not inconvenienced by having to wait for baggage on arrival?

On the other hand, many passengers would argue that if the baggage handling system was reliable, safe from damage and risk of loss, and baggage delivery was quick at destination, there would be far less need to carry hand baggage. One day in the future, the entire airport may be a completely secure area, with the help of powerful technologies able to "control" people and activities seamlessly at the main point of entry to the airport. It may eliminate a screening-related line, removing the need for passengers to take off coats and shoes and have items screened individually. This will not be available for some years. For now, making the process effective, efficient, and customer friendly continues to present an opportunity to the global aviation community.

## CONCLUSION

The pace of change to passenger security screening processing has been unprecedented in the twenty-first century century. Each instance of change creates a capacity imbalance in the sequence of processes making up the passenger screening "production line." It is reasonable to suggest that if the frequency of change continues, passenger security screening in its current

form may exceed its boundaries in terms of handling passenger volumes and meeting threat identification demands. International screening standards, new detection technologies, and the creation of a completely "sterile" airport are some of the options that may be considered. All of these take time and investment to endorse and implement. Until that time comes, there are clear opportunities for airport operators to better manage the integration of new requirements by understanding their effects on the end-to-end process and rebalancing appropriately.

## NOTES

1. Transportation Security Administration, *TSA Screening Program Optimizing Passenger Through-Put at Security Screening, 2006* (Washington, DC: GPO, 2006), 1, hereafter TSA.

2. J.U.S. Rudderman, Centennial of Flight Commission, *Aviation Security*, http://www.centennialofflight.gov/essay/Government_Role/security/POL18.htm.

3. H. Reighard and J. Dailey, *Task Force on Deterrence of Air Piracy* (Washington, DC: FAA Office of Aviation Medicine, 1978), 27.

4. *Aviation Security, National Commission on Terrorists' Attacks on the United States*, May 22, 2003, http://www.9/11Commission.com.

5. *Federal Aviation Act of 1958.*

6. Ibid.

7. A. Wu, *The History of Airport Screening*, http://www.savvytraveler.publicradio.org.

8. Public Law 10 7-306 (2002).

9. 9/11 Commission Staff, *Aviation Security System and the 9/11 Attacks, Staff Statement No. 3*, 2004, http://www.911commission.gov/staff_statements/staff_statement_3.pdf.

10. D. Fonda and S. B. Donnelly, *Bumps in the Sky*, October 26, 2003, http://www.time.com/time/magazine/article/0,9171,526469–2,00.html.

11. U. S. Government Accountability Office, *Transportation Security: Post–September 11 Initiatives and Long Term Challenges* (GAO-03–616T), 2003, http://www.gao.gov.

12. U.S. Government Accountability Office, *Aviation Security: Transportation Security Administration Has Made Progress in Managing a Federal Screening Workforce and Ensuring Security at U.S. Airports, but Challenges Remain*, 2004 (GAO-06–597T), http://www.gao.gov.

13. S. Res. 1447 (2001); 160 Cong. Rec. 8341.

14. Airports are categorized according to the amount of cargo and passengers they handle. X are the biggest airports whereas I are smaller. BearingPoint, *Private Screening Operations Performance Evaluation Report*, April 16, 2004, http:// www.tsa.gov/assets/pdf/Summary_Report.pdf.

15. S. K. Goo, *Airport Screeners' New Guard: Private Security Firms Want to Replace Government in 2005*, http://www.washingtonpost.com.

16. Public Law 108–334, October 18, 2004, 118 Stat. 1303.

17. *Homeland Security Presidential Directive/HSPD-6, Subject* (Washington, DC: GPO, 2003).

18. Transportation Security Administration, TSA Web site, June 2007, http://www.tsa.gov/what_we_do/layers/secureflight/editorial_1716.shtm.

19. Mark Skertic, "Passenger List Review May Add To Flight Time," *Chicago Tribune*, August 17, 2006.

20. *Report of the National Commission on Terrorist Attacks upon the United States (9/11 Commission Report)* (Washington, DC: Government Printing Office, 2004).

21. Mimi Hall, *Report Caatalogues Problems in Air Marshals Service*, August 30, 2004, http://www.usatoday.com/news/washington/2004–08–30-marshals-misconduct_x.htm.

22. TSA: 49 CFR Chapter 12, Part 1544.223.

23. TSA, *Federal Air Marshals—Mission Focused*, 2006, http://www.tsa.gov/lawenforcement/people/index.shtm.

24. *CNN*, CNN.com, May 8, 2002.

25. "TSA Response to the House Committee on the Judiciary Draft Report: *In Plane Sight: Lack of Anonymity at the Federal Air Marshal Service Compromises Aviation and National Security*," *ABC News*, April 6, 2006, http://abcnews.go.com/images/WNT/air_marshal_extract.pdf/.

26. JP International Aviation Security, *International Aviation Security*, May 23, 2004, http://www.jp-ias.co.uk/aviation-security-management-personnel.html.

27. Ibid.

# CHAPTER 5

# General Aviation Security in the United States: Challenges and Responses

*James Jay Carafano*

Air security in the United States since September 11, 2001, has overwhelmingly focused on commercial aviation and passenger airlines in particular. Flying over American skies every day, however, are many thousands of small airplanes, many of them owned and operated by individuals. General aviation is an industry that involves 5,288 community airports in the United States, employs 1.3 million people, and totals just over 1 percent of GDP.[1] In addition, there are approximately 219,000 general aviation aircraft in the United States, comprising 77 percent of all U.S. air traffic.[2] General aviation is important to the economy and it is growing.

Implementing a common-sense and practical security system for this dynamic, decentralized, and diversified sector of the U.S. transportation network, in a manner that provides reasonable security but does not threaten the enormous advantages of a growing general aviation sector, is no easy task. There are several obstacles that have to be overcome.

*Americans do not understand.* Despite the fact that the general aviation industry encompasses over three-quarters of all air travel, average Americans know little about a part of the U.S. transportation system that includes everything from test aircraft to cargo transport, gliders, and even crop dusting and parachuting, all of which fit within the general aviation sector.

Because Americans know so little about the general aviation domain, security incidents or concerns could well engender significant but unwarranted anxiety, in much the same way that the general lack of public knowledge about maritime affairs contributed to the unjustified uproar over the 2006 proposed sale of some U.S. port facilities to a foreign-based company.[3] Thus, educating the public on the sector, its value to the economy, and the real risks and concerns associated with general aviation is the first necessity.

*One size does not fit all.* The sheer size and diversity of the general aviation sector makes it difficult to craft a single comprehensive security policy that would address the diverse components of the industry. There are over 200,000 general aviation aircraft registered in the United States. Ninety percent of these are powered by single-piston engines and have a short travel range. They weigh and hold about the same amount of cargo as a Honda Civic.[4] On the other hand, 10 percent are medium-size jets that weigh over 12,500 pounds and are usually chartered for business travel. Some have intercontinental range.

Airfields and airports that service general aviation exhibit a similar diversity. Among the more than 19,000 landing facilities that service general aviation, some have grass runways and are located in the wilderness, while others are fully functioning international airports in large cities.[5] In addition, the airports are scattered throughout the United States, including Alaska and the Hawaiian islands. Because there is no standard size, shape, or function of a general aviation airport, it is difficult to devise a one-size-fits-all set of security standards.

Likewise, transportation patterns are diverse and fluid. Aircraft flights range from the occasional pleasure or hobby flight to the more frequent chartered activity of corporate business jets. Depending on the size, speed, and destination of the aircraft, they may need to file formal flight plans or simply radio in to the control tower when they reach their final destination. This makes it virtually impossible to track the majority of aircraft when they are in transit. The single characteristic that all general aviation flights share is that, unlike commercial flights, they are scheduled on demand.

*Comprehending the threat.* The 9/11 Commission recognized the inherent vulnerabilities to general aviation (GA) when it discovered that several of the September 11 hijackers had used private flight schools to train for the attacks. The commission concluded that "[m]ajor vulnerabilities still exist in . . . general aviation security."[6] It is highly unlikely, however, that a general aviation incident would be anything like a September 11–style suicide attack. Most general aviation aircraft would make poor weapon platforms. The majority are too light and slow to cause significant damage to people or infrastructure. For example, a fully loaded Cessna 172 weighs 2,400 lbs and carries 56 gallons of fuel. A Boeing 767, such as one of the aircraft used in the September 11 attacks, can weigh more than 400,000 lbs and carry 25,000 gallons of fuel.[7] Most general aircraft could cause only a fraction of the amount of damage that a large commercial airliner could cause. The recent crash of Yankees' pitcher Cory Lidle into a Manhattan building shows that small aircraft don't cause significant damage to buildings or the people inside them. The only people to die in the crash were Lidle and his instructor on board the aircraft.[8]

Even an aircraft packed with explosives would have modest potential as an air-delivered weapon. Most critical infrastructure is resilient enough to withstand such attacks. For example, nuclear power plants are designed to survive the accidental crash of a commercial airliner.[9]

Another often overstated threat in the realm of general aviation is that crop dusters can be used to dispense biological or chemical weapons. This concern originated with the 9/11 Commission, when it discovered that Mohammad Atta, the lead hijacker in the attacks, was looking into crop dusters in the months prior to September 11. While the threat seemed plausible in the aftermath of the attacks, subsequent investigations cast doubt on the practicality of the plot. Crop dusters have to fly very slowly and low to the ground to disperse their contents. In addition to these factors, crop dusters are designed to have a limited coverage area. The mechanism installed on the belly of the aircraft does not have a very wide range, in order to avoid excess chemical dispersion or overcoverage. Often, pilots will have to fly over the same field several times to ensure that the crops have had proper exposure.

In addition, experts doubt the feasibility of employing general aviation aircraft as biological weapons dispensers. Conventional sprayers on crop dusters or air tankers that are used to fight forest fires, for example, would probably not be very effective at dispensing biological agents. Mechanical stresses in the spraying system might also kill or inactivate a large percentage of the particles, by some estimates up to 99 percent.[10] Nor could crop sprayers carry sufficient volumes to carry out a significant chemical attack.

## FOCUSING ON THE RIGHT PROBLEM

The most worrisome threat from general aviation comes from using aircraft as a transportation platform—a means to convey "bad things" or "bad people." General aviation is a private means to haul cargo in a short amount of time over a long distance. In general aviation, the security standards for travelers, particularly passengers, is much more lax than for commercial airliners. While private pilots have their identities and credentials checked on a regular basis, passengers may not be screened, even when they fly internationally. On domestic flights, cargo is virtually never inspected.

Drug smuggling demonstrates the potential to exploit the general aviation sector for illicit activity. For years, small private planes have been used to transport narcotics from South America to Mexico and the United States. In fact, for many years the most popular means to transport cocaine from Colombia to Mexico was private aircraft. In 1975, only two years after President Nixon declared the "war on drugs," Colombian officials made the largest narcotics seizure in history, seizing over 600 kilograms of cocaine from a private aircraft.[11]

In addition to the transport of illicit material, general aviation can be an effective means to smuggle people. With thousands of landing facilities in the United States plus innumerable fields, open spaces, and roads that could serve as impromptu landing sites, there exist endless locations to deliver passengers covertly.

General aviation aircraft are seldom stolen. According to statistics from the Aviation Crime Prevention Institute, only eight general aviation aircraft were

stolen in 2006.[12] Private planes are valuable assets, and the individuals who own them take every precaution to protect their planes. For example, even a 30-year-old single-piston plane can be worth up to $40,000. The security precautions that pilots take every day have also helped prevent the theft of more aircraft. Additionally, general aviation planes are almost never hijacked. Most of them are flown for personal use and the pilots know who their passengers are, because most of the time they are friends and family. Even in the case of chartered business flights, aviation companies go through strenuous measures to ensure the identity of their passengers. Overall, unlike commercial pilots, general aviation pilots know is flying with them before they get in the cockpit.

Thus, it is more likely that any smuggling involving general aviation would be part of a criminal or terrorist conspiracy involving the pilot, the passengers, or some aspect of the general aviation services industry.

## PRINCIPLES OF GENERAL AVIATION SECURITY

Crafting the right solutions for making the skies safer and maintaining a vibrant general aviation sector that has room to grow and innovate requires principled proposals that address the threat in the most efficient and cost-effective manner.

*Eschew "silver bullet" solutions.* Because of the enormity and diversity of the general aviation sector, there is no single measure that can adequately address security concerns.

*Adopt a layered approach.* The best approach will be one that incorporates layers of security. General aviation security requires different layers of protection at different stages. For example, security measures at flight schools, hangars, and airports should be streamlined to provide a fail-safe approach to giving pilots access to the skies. The best way to stop the illicit exploitation of general aviation is to keep malicious actors out of the cockpit.

*Employ a menu of measures.* If a security program works for corporate business jets, it doesn't necessary follow that it would be effective for small Cessna planes or hobby aircraft. Programs must be tailored to different types of aircraft, airfields, and aviation services.

*Establish a reasonable role for the private sector.* Security activities should be dictated by a comprehensive assessment of risks. Washington, not the private sector, is responsible for preventing terrorist acts through intelligence gathering, early warning, and counterterrorism efforts. The private sector is responsible for taking reasonable antiterrorism precautions in much the same way as society expects it to take reasonable safety and environmental precautions.

The government has a role in defining what is "reasonable" and facilitating information sharing. A model public-private regime for the aviation industry would (1) define what is reasonable through clear performance measures, (2) create transparency and the means to measure performance, (3) establish

ways for the market to reward good behavior, and (4) ensure that any "fix" does not cripple the economic viability of the aviation industry.

## THE STATE OF SECURITY

Some of the U.S. security measures that have been established since September 11 reflect principled security. Others do not. One of the first security improvements implemented by the private sector is the "Airport Watch" program. Airport Watch is a joint venture between the private and government communities, and was cofounded by the Aircraft Owners and Pilots Association (AOPA) and the Transportation Security Administration (TSA). This partnership resulted in an elaborate program resembling a "neighborhood watch" at thousands of local airports nationwide. This network includes over 650,000 pilots, who serve as eyes and ears for observing and reporting suspicious activity. Airport Watch relies on local pilots and airport officials to report information to state and local law enforcement agencies. The Airport Watch program includes warning signs for airports, informational literature, and a training video to teach pilots and airport employees how to enhance security at their airports. To date, this program has prevented theft and airport break-ins at airports in Kansas, Missouri, Ohio, Georgia, Arkansas, and Minnesota.[13] Initiatives like Airport Watch are important because they provide a decentralized network for reporting security threats. Making the everyday pilot the eyes and ears at his airport provides an additional layer of security on the ground. It is also cheaper than training thousands more government security officers and deploying them at airports around the country. Airport Watch is successful because it turns the everyday pilot into a security asset at the disposal of local, state, and federal law enforcement.

After September 11, the private sector worked with the FAA and TSA to make flight training a more transparent and secure process. The first step was advanced screening of pilot databases against the TSA threat watch lists. This regulation was adopted into law on January 24, 2003, with the sponsorship of the TSA and FAA, and means that individuals who show up on TSA watch lists can have their certificates suspended or revoked. While this improvement is not completely interoperable, it is certainly a good first step.

Another security measure created by many private flight schools applies to foreigners training for pilot certificates. Now, all foreign nationals applying for flight training will be subject to a Department of Justice background check before entering their training programs. A more stringent screening process is in place for foreigners wanting to learn to fly jet aircraft over 12,500 lbs. This rule is dubbed by experts as the "twelve-five rule" and was introduced into law as part of the FAA renewal legislation (HR 2215) in 2002. In addition, in January 2005, the Vision 100—Century of Aviation Reauthorization Act (PL 108–176) was introduced, requiring that flight school instructors be trained in "suspicious circumstances and activities of individuals enrolling or attending a flight school."[14] On the domestic end, U.S. student pilots must show a government issued photo ID card to verify their identity before enrolling in

flight school. In addition, many flight schools require instructors to be present anytime a student pilot is on the tarmac or near training aircraft.

The TSA also published the *General Aviation Security Guidelines/Information Publication*, which provides municipalities, owners, and operators in charge of general aviation airports with a set of federally endorsed recommendations to enhance security.[15] Just as it does for major commercial airports, the TSA issues and spreads security advisories to GA airports, giving them a summary of relevant facts on security that are designed to increase security awareness. In terms of airport infrastructure security, on June 15, 2006, the TSA issued the *Recommended Security Guidelines for Airport Planning, Design and Construction.*[16] This document contains security guidelines on airport layout, security screening, emergency response, access control, and communications.

In addition, the TSA is currently working on the General Aviation Vulnerability Identification Self Assessment Tool (GA-VISAT). GA-VISAT is a comprehensive, Web-based airport risk assessment tool, available online via an authorized account. The program consists of a series of pull-down menus and check boxes that provide a virtual check list for airport security. At the end of the lists, the program scores the results and gives the user a "target attractiveness" score. The score will also explain the social, political, and economic impacts of improvements to security tailored to a specific airport. GA-VISAT is currently in its testing phase and should be available to GA airport personnel in the forseeable future.

Less meaningful to promoting aviation security was the Air Defense Identification Zone (ADIZ) established after September 11. The ADIZ represents a 30-mile nautical ring around the Washington, DC, greater metropolitan area and has proved to be more of a burden than an asset. The measure prevents private pilots from having reasonable access to DC airspace. In addition, the ADIZ costs an estimated $11 million dollars per year.[17] For all that cost and inconvenience there is arguably very little security benefit. A small plane intent on covertly entering the district's airspace could likely evade detection and reach its target before it could be effectively intercepted.

After September 11, general aviation was also banned from Ronald Reagan Washington National Airport. In order to restore access to the area, the TSA established a "gateway" program. General aviation flights into Washington resumed in October 2005. In order to fly into Reagan National Airport, aircraft must first fly through predesignated gateway airports and meet strict requirements including the following:

- Pilots must be prescreened;
- Flight plans and crew manifests must be submitted 24 hours in advance;
- Aircraft, crew, baggage, and passengers must be screened;
- An armed law enforcement officer, certified by the TSA, must accompany flights with passengers.

Facilities already serving as gateway airports include Seattle-Tacoma in Washington, Boston Logan in Massachusetts, Houston Hobby in Texas, White Plains and LaGuardia in New York, Chicago Midway in Illinois, Minneapolis/St. Paul in Minnesota, West Palm Beach in Florida, San Francisco in California, Teterboro Airport in New Jersey, Philadelphia in Pennsylvania, and Lexington in Kentucky. Airports to be added include Dallas/Love Field Airport, Memphis International Airport, and Milwaukee's General Mitchell International Airport. The costs associated with the gateway program place significant burdens on general aviation. The TSA requires operators to pay for security screening and background checks plus the onboard security officer. The procedures remain too expensive and complex for average general aviation aircraft.

## OPTIONS FOR THE FUTURE

While some practical and reasonable measures have been taken, other requirements, particularly with regard to security in the Washington area, require refinement. In addition, more attention needs to be given to how to prevent a recurrence of the post–September 11 period when aviation was indiscriminately suspended in the wake of the attacks on New York and Washington. The suspension created as many problems as it solved. Many specialized emergency responder groups, such as urban search and rescue teams, for example, could not quickly deploy to the World Trade Center flight because commercial and general aviation flights were grounded. Improving the layers of general aviation security might include the following initiatives:

*Eliminating the post–September 11 ADIZ in the Washington, DC, area.* Instead, the FAA should require general aviation to comply with the more limited Flight Restricted Zone (FRZ), which was in place before September 11 as the standard no-fly procedure over critical infrastructure in Washington, DC. In the event of an emergency or special circumstance, the government should have the right to resurrect the ADIZ as part of the protocol for a National Security Special Event (NSSE), as was the case with the Republican National Convention in 2004.

*Making the gateway program more flexible.* The "Maryland Three," the three general aviation airports (College Park Airport, Potomac Airfield, and Washington Executive/Hyde Field) within the current ADIZ should be made more accessible to the general public, providing a realistic alternative for noncommercial general aviation flights that cannot afford the security costs of landing at Reagan National Airport. In addition, the TSA should consider more flexible and cost-effective options for implementing the gateway program, including eliminating the requirement for a law enforcement officer to accompany each flight.

*Establishing a trusted pilot program.* This program would be vital in preventing general aviation from shutting down completely in the event of another terrorist attack or natural disaster. A trusted pilot program with certification for first responders, for example, would ensure that such people are always granted access to the air to response to emergencies that might shut down U.S. airspace. This program would

also speed up customs inspections for trusted pilots when they reenter American airspace from abroad. In addition, a trusted pilot program should allow credentialed general aviation pilots easier access to the Baltimore/DC airspace, as well as to the "Maryland Three."

*Focus on an interoperable database for registered aircraft and airmen*. With the numerous databases already in place between the Department of Transportation, TSA, FAA, and private sector, interoperability is the key to interagency security cooperation. Making the same databases and watch lists available to everyone in the GA sector will ensure that pilots and flight students are checked against every source of information before they are allowed in the sky. A database organized like the current driver's license databases at the state level would allow the federal government to do a systematic analysis of all U.S.-registered aircraft. It would also allow the government to look at a pilot's history in terms of flight time and possible illegal activity. Finally, interoperability is essential to integrating the FAA and DOJ databases so that background checks on foreign and domestic flight students can be completed in a timely manner.

*Establish secure credentials for pilot certificates and credentials*. National standards for these credentials and for "breeder" documents (such as birth certificates) required to obtain pilot credentials should be similar to those for driver's licenses established under the REAL ID Act.[18]

*Build up the Department of Homeland Security aviation law enforcement capacity*. The Department of Defense currently protects U.S. airspace. This is an expensive and inefficient use of high-performance aircraft that are not optimized for domestic air security missions, such as interdicting hijacked and stolen planes and guarding restricted airspace. The long-term investment strategy should look to building up appropriate civilian law enforcement capabilities in the Coast Guard and Customs and Border Protection (CBP) and getting the Defense Department out of the domestic air security business.

Both CBP and the Coast Guard face daunting modernization challenges, particularly concerning their modest and overworked aircraft fleets. For example, the Coast Guard's fleet is old, expensive to operate and maintain, and poorly suited for some homeland security missions. Deepwater was to be funded at $330 million (in 1998 dollars) in the first year and $530 million (in constant dollars) per year in the following budgets, but no annual budget before FY 2004 matched the required rate of investment.[19] Meanwhile, the Coast Guard's increased operational tempo and expanded mission requirements since September 11 have been wearing out the fleet faster than anticipated and putting the modernization program even farther behind schedule.

*Integrate Coast Guard modernization and the Secure Border Initiative*. Preventing the illegal crossing of U.S. land and sea borders by general aviation aircraft will be an imperative in the years ahead. Both CBP's Secure Border Initiative (SBI) and the modernization of U.S. Coast Guard aviation assets could potentially play an important role in air security along the border. Securing the borders will require more than an investment in land border assets. It will also require strengthening sea and air borders. The Coast Guard plays a central role in immigration control along the U.S. coasts. Thus, its modernization program should be a priority component of the Secure Border Initiative, and Congress should fully fund Coast Guard modernization programs to enhance homeland security.[20]

*Adapt new technology*. GPS units are becoming more commonplace in general aviation aircraft. Congress and the administration should promote the voluntary adoption of GPS throughout the general aviation sector. The more widespread use of GPS will provide greater situational awareness of aviation activities, enhancing both public safety and law enforcement.

The improvement of general aviation security should be part of the national effort to make the skies safer.[21] Much has been done since September 11 to establish security measures that are appropriate for the threat. More can be done, however, to ensure that general aviation remains a vibrant industry and a secure one.

## NOTES

1. *Our Economy: A Critical Sector of the US Economy*. Aircraft Owners and Pilots Association. http://www.gaservingamerica.com/our_economy/economy.htm (8 March 2007).

2. Transportation Security Administration, Aviation Security Advisory Committee Working Group, "Report of the Aviation Security Advisory Committee Working Group on General Aviation Airports Security" (Washington, DC: TSA, October 1, 2003), 2.

3. James Jay Carafano and Alane Kochems, *Security and the Sale of Port Facilities: Facts and Recommendations WebMemo #997*, February 22, 2006, www.heritage.org/Research/HomelandDefense/wm997.cfm.

4. Aviation Security Advisory Committee Working Group, "Report," 2.

5. U.S. Department of Homeland Security, *Report to Congress on General Aviation Security: In Accordance with the FY 2006 DHS Appropriations Act* (P.L. 109–90), May 2006, 2.

6. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: W. W. Norton), 391.

7. Aircraft Owners and Pilots Association, *General Aviation and Homeland Security*, security brief by AOPA, March 29, 2007, http://www.aopa.org/wahtsnew/newsitems/2002/020621_homeland_security.html.

8. James Fallows, "The Cory Lidle Crash in New York City," *The Atlantic Online*, *Atlantic Monthly* March 20, 2007, http://www.theatlantic.com/doc/200610u/lidle-crash/2.

9. Robert M. Jefferson, "Nuclear Security: General Aviation is Not a Threat," May 16, 2002, 1.

10. Seth W. Carus, *Bioterrorism and Biocrimes. The Illicit Use of Biological Agents in the 20th Century* (Washington, DC: Center for Counterproliferation Research, National Defense University, 1998), 24.

11. *Timeline: America's War on Drugs*, *NPR*, June 17, 2004, http://www.npr.org/templates/story/story.php?storyId=9252490.

12. Aviation Crime Prevention Institute, Inc., *Stolen Aircraft Statistics*, October 25, 2006, www.acpi.org.

13. GA Serving America, "Airport and Aircraft Safety," *General Aviation Security*, March 30, 2007, http://www.gaservingamerica.com/Airport-Security2.htm.

14. Aviation Security Advisory Committee Working Group, "Report," 4–5.

15. Transportation Security Administration, *General Aviation Security Guidelines/Information Publication* (Washington, DC: TSA, 2002).

16. Transportation Security Administration, *Recommended Security Guidelines for Airport Planning, Design and Construction* (Washington, DC: TSA, 2006).

17. Aircraft Owners and Pilots Association, *Operation ADIZ*, February 2, 2002, http://www.aopa.org/adizalert/.

18. James Jay Carafano, *Making REAL ID A Reality—Concerns, Challenges, Choices, Solutions (Testimony #9999)*, September 29, 2003, www.heritage.org/Research/HomelandDefense/tst050807.cfm.

19. Deepwater is the name of the program to modernize the Coast Guard's fleet with newer ships and the latest technology.

20. James Jay Carafano, *Coast Guard Modernization Is Integral to the Success of the Secure Border Initiative, Executive Memorandum #1009*, August 7, 2006, www.heritage.org/Research/HomelandDefense/em1009.cfm.

21. James Jay Carafano, *America Needs a Security Strategy for Safer Skies, Executive Memorandum #996*, March 21, 2006, www.heritage.org/Research/NationalSecurity/em996.cfm.

# CHAPTER 6

# The Airport Retailing Business and the Impact of Updated Security Measures: The European Perspective

*David Jarach and Fulvio Fassone*

> Terrorists do have something in common with airlines after all: they both operate internationally.
>
> —Rod Eddington, then-CEO of British Airways, speaking in Washington in early 2004 at the end of an extraordinary few weeks of security alerts on the North Atlantic

Airports play a pivotal role today in the development of local territories, acting as main gateways for both incoming and outgoing business and tourism, thus promoting international exposure and supporting the globalization of companies. Airports are increasing their economic return on investment by accelerating the pace of offering "non-aviation-related" activities, of which retailing is the main one. Actually, a distinctive and rather innovative non-aviation-related value proposition has become a major factor for passengers choosing an airport, most definitely in the case of various airports competing for passengers' attention in overlapping catchment areas.

This positive scenario has been threatened by recent terrorist attacks, from the September 11 events to the more recent events in London during August 2006, where terrorists were planning multiple explosions on a number of transatlantic flights. These attacks and threats have brought about much stricter security measures that have impacted the non-aviation, retailing-based formula, for example, limiting the quantity and nature of purchases, such as liquids. Some of these rules have been relaxed over time, but others are still in place. What effect the rules have and even whether there is any real threat is questionable.

This chapter first explores the value proposition of airport enterprise as it has evolved, with the growth of the "commercial airport" philosophy linked to the need to support long-term infrastructural investments with cash flow originating from non-aviation-related business. Second, it explores in depth the most recent security measures taken at airports with regard to liquid products like perfumes, cosmetics, and drinks that are the core of airport retailing. This analysis has a European perspective, given the expertise of the two authors and the direct link between what happened just after the August 10, 2006, London terrorist events and what is happening today.

## THE ECONOMIC VALUE OF AIRPORTS: TOWARD A NEW DEFINITION OF THE BUSINESS MODEL OF AIRPORT ENTERPRISES

Airports are an essential part of the air transport system. They play a vital role not only within the macro environment of transportation but also in the process of increasing the quality of life in their regional economies and directly participating in creating wealth. They can thus be considered as leading players in regard to the economic, productive, tourist, and commercial upgrading of a territory, thanks to the "multiplier effect" in the number of business transactions they may stimulate.

Born from aerodromes, mostly military ones, in the post–World War II era, airports have thus become conduits for business and tourism. Currently, not only do they offer the businessperson an efficient means of transport to clients' bases far away, but they constitute commercial hubs for an area, employing thousands of people in their operation.

Historically, flight and inherently aviation-related activities, like the number of destinations served and number of flights offered, have been at the very heart of what an airport is and why passengers go to it. For these customers, airports represent physical structures, some more or less spacious and comfortable than others, in which they have to spend a certain amount of time to allow for the processing of technical requirements related to the "flight experience." Typical examples are check-in procedures for passengers and their baggage, passage through security inspections for accessing airside areas, and time spent waiting at boarding gates.

This traditional view, combined with stagnant airport managerial approaches, leads, however, to a broad underestimation of the relevance of a vast category of ancillary activities that can be carried out inside both terminal buildings and airport boundaries. These activities may be included in the category of non-aviation-related activities, like commercial services (airport retailing), tourism services, congressional services, logistics and property management services, and consulting services.[1] These may, in fact, play a significant role in complementing and supporting the primary service of the airport infrastructure and become a major source of airport revenues. Moreover, it's very clear that the airport environment, when exploited in a creative way,

may become a location with unique features not only for shopping but also for many other types of services like logistics and real estate services.

Thus, widening the view of the non-aviation-related business to include other sources of activity can be a good stimulus for creativity and innovation by proactive airport management. In this sense, the non-aviation-related business unit grows to include all sources of activity by acknowledging a different concept of airport service and value proposition, where the only limit may be ascribed to space constraints and inefficient project designs inside the airport complex.

## IMPLEMENTING THE NON-AVIATION-RELATED REVENUE DRIVER: TOWARD THE "COMMERCIAL AIRPORT" PHILOSOPHY

Compared with most other industries, airports enjoy unique opportunities for gaining extra profit from non-aviation operations, thanks to a high degree of strategic control, primarily in the form of "customer ownership." In other words, airports have a customer base that any high-street retailer would willingly exchange body parts for; furthermore, these customers are a captive audience. This happens because airport customers are forced to spend a good deal of time within the terminal walls due to the range and profile of operations to be undertaken in an airport infrastructure before boarding a flight.

Air passengers will often arrive at the terminal building well before the scheduled departure time, especially if flying to sunshine destinations with a charter carrier and submitting to a series of operational necessities and security controls. Also, passengers' meeters and greeters will be waiting for a long time at the airport, especially when incoming or departing flights have been delayed, while employees of the various players in the value chain will spend most of their day working inside the airport perimeter and will look for a variety of service propositions to satisfy their primary needs. Eventually, citizens inside the airport's catchment area may stay in the terminal building for long periods of time to help justify the trip from downtown, especially when the airport's value proposition looks innovative and unique compared with neighboring outlets.

The relatively long duration of a customer's stay within the "shopping mall with runways" may have a direct and positive impact on the average income of each shopping outlet and service provider hosted in the terminal, as customers may choose to spend some of their spare time shopping. But, in such growing hypercompetitive contexts, the magnitude and quality of the non-aviation-related formula may become a catalyst for competitive supremacy over other players. For instance, in the Middle East scenario, non-aviation-related activities have become travelers' primary element of choice between the various airport sites competing in an overlapping catchment area, most definitely in the case of hub-related travel patterns.

Singapore airport is famous throughout the world for its own unconventional and innovative package. Travelers may pass their time before boarding not only shopping in the various arcades of the complex but also relaxing near an artificial lake surrounded by orchids. Choosing between a long list of bars and pubs, it's possible to have a drink while listening to a violinist within an environment of tropical palms and reproductions of past civil airliners. Children may play their favorite videogame in a dedicated area, while film lovers will find a movie theater and sport fans a sports arena. There is also a fitness centre close to the Transit Hotel at Terminal 1, where you can also have a sauna or relax in a Jacuzzi. Some best-in-class examples are clearly visible in the European scenario as well, as in Copenhagen, Amsterdam, Vienna, and London. For all these players, non-aviation activities are vital elements in their global operations, not only in delivering the experience the customer wants but also in providing the revenue needed to support any long-term investment programs. In contrast, the historical "hop on, hop off" view that is pervasive in U.S. airports has prevented the growth of significant non-aviation-related business, although the non-aviation phenomenon had its early roots in America when two Americans, Charles Feeney and Robert Miller, opened the Duty Free Corporation in Hong Kong in 1960.

We can clearly see that proactive airport infrastructures have been evolving from a purely mono- or multimodal logistical medium into more sophisticated market entities that may be described as "multipoint service-provider firms," in which most of the profit (as opposed to the loss) contribution comes from non-aviation-related activities.

There has of course been September 11, 2001, a cataclysmic event that threatened to derail not only the world's economy but also the whole genre of flight. What it has meant is a complete rethinking of the security arrangements within airport structure and management. Human nature being what it is, the response has been to turn the negative into a positive. Passengers need services while they are in a "hold" situation, and one way of paying for increased security costs is to expand the earnings coming from commercial revenues. The August 10, 2006, London events, however, led to a different result when the local authorities responded by strictly reinforcing security measures that had a direct impact on airport retailing sales.

## NEW SECURITY MEASURES AFTER THE AUGUST 10, 2006, LONDON EVENTS

In fact, the August 10, 2006, London events showed once again that after September 11, air passengers and aircraft unfortunately remained high-priority targets for terrorists. Only successful intelligence-gathering and effective operations by the United Kingdom police and security services prevented a potentially devastating terrorist incident that would have shot down up to 12 U.S. and UK aircraft flying over the Atlantic.

United Kingdom officials were also very quick to introduce strict, upgraded security measures at all UK airports immediately after the new terrorist threat, which imposed significant restrictions on passengers' bags and personal items.

However, these heightened security measures proved to be very detrimental to airport commercial and retail operations, since they were absolutely unprecedented in their magnitude and scope. The restrictions on taking liquids and gels on board all European Union and extra-European Union flights departing from Europe, preventing the retailers' customary "gate delivery" sales, clearly precluded significant purchases of duty-free liquor, perfume, and cosmetics.

In fact, airport airside duty-free and retailing outlets have always been one of the most heavily inspected sectors in the world. For instance:

- Dutiable goods pass through an official, customs-regulated bonded warehouse system;
- Goods are screened as they go airside into the stores;
- Retail staff working airside are security screened by the relevant authority in each country and are screened every time they go airside; and
- Sophisticated electronic point of sale (EPOS) and IT systems record detailed sales information.

Nevertheless, the United Kingdom authorities immediately activated a new set of heightened security measures that apparently were to remain in place indefinitely. The impact on all the airport retailing activities in Europe was immediate. No one—not airports, nor airlines, nor retailers, yet alone the industry's trade associations—was prepared for the new measures. Featured below is a press release from the United Kingdom Department of Transport mentioning the kind of new security measures set in place by the United Kingdom authorities beginning August 14, 2006.

**Effective from August 14, 2006**

Following the Joint Terrorism Analysis Centre's decision to change the UK threat level from Critical to Severe, the following aviation security measures will apply at all UK airports with immediate effect.

These arrangements apply to all passengers starting their journey at a UK airport and to those transferring from international flights at a UK airport.

*Each passenger is permitted to carry ONE item of cabin baggage through the airport security search point.* The dimensions of this item must not exceed: a maximum length of 45 cm, width of 35 cm and depth of 16 cm (17.7" × 13.7" × 6.2" approx) (including wheels, handles, side pockets etc.). Other bags, such as handbags, may be carried within the single item of cabin baggage. All items carried by passengers will be x-ray screened.

*No liquids of any type are permitted* through the airport security search point, other than the following items:

- Essential medicines in liquid form sufficient and essential for the flight (e.g. diabetic kit), as long as verified as authentic
- Baby milk and liquid baby food (the contents of each bottle or jar must be tasted by the accompanying passenger).

NOTE: The definition of liquids *includes gels*, *pastes*, *lotions*, *liquid/solid mixtures and the contents of pressurised containers*, e.g. toothpaste, hair gel, drinks, soups, syrups, perfume, deodorant, shaving foam, aerosols, etc.

To help their progress through search points, passengers are encouraged not to include items capable of containing liquids (e.g. bottles, flasks, tubes, cans, plastic containers etc.) in their cabin baggage.

All laptops and large electrical items (e.g. large hairdryer) must be removed from the bag and placed in a tray so that such items neither obscure nor are obscured by the bag.

Pushchairs and walking aids are permitted but must be x-ray screened. Wheelchairs are permitted but must be thoroughly searched.

In addition to the above, passengers boarding flights to the USA and items they are carrying, including those acquired after the central screening point, will be subjected to secondary search at the gate. Any liquids discovered will be removed from the passenger.

The Department for Transport will work closely with operators to introduce these new arrangements, seeking to keep disruption to passengers to a minimum. The Department will keep these measures under review.

If passengers have any questions on their travel arrangements or security in place at airports they should contact the airport or their airline.[2]

Ten days after the August 10 event, the picture with regard to security measures in Europe was really confusing. On August 20, the ETRC (European Travel Retail Council) organized a meeting at Amsterdam's Schiphol Airport with the duty free and travel retail industry key players, in order to create and coordinate a lobby front and therefore put into action a strong reaction toward these new security measures.

At that stage, ETRC formally launched a campaign to persuade all EU member state governments, industry national associations, and ultimately the U.S. Homeland Security/TSA to accept and adopt a system based on the use of a sealed bag. In principle, this would permit the continuation of sales to U.S.-bound passengers departing non-U.S. airports and would enable passengers to receive goods at their gates.

ETRC said in a press statement:

Meeting in Amsterdam . . . , representatives from all sectors of the travel retail industry moved quickly to address the need for enhanced security on flights from European airports to US destinations. The industry agreed that the temporary use of the "sealed bag" measure would enhance security without unnecessarily hindering airside retail. We believe that our recommended actions can provide the most practical and effective solution to the need for more security in airports at this time. With the "sealed bag" measure, the industry can extend its secure supply chain from the point of sale to the final destination.

This security measure would use durable, transparent plastic bags provided by airport retailers for U.S.-bound flights and for all flights to the United Kingdom, Israel, and certain other destinations, and it would permit passengers to carry their purchases as hand baggage on board aircraft. Purchased items would be placed in these bags and sealed by airside retail staff at the point of sale, enabling passengers to take them from the store and onto the aircraft. The sealed bags could be easily inspected by security officers at any point between when passengers leave the store and when they finally board their planes.

After the August 10 event, a set of significant, related decisions were made in order to improve procedures at screening checkpoints. These deal with

a requirement to separately screen complex electronic equipment, including portable computers, in order to update the screeners' ability to detect dangerous items. In addition, an agreement in principle was reached on parameters for common European standards on screening equipment, including a phased introduction of higher-performance equipment.

At the beginning of September 2006, ETRC President Frank O'Connell sent a letter on these topics to the European Commission (EC) vice president, Jacques Barrot:

I am writing to you on behalf of the European travel retail industry to express our serious concerns regarding proposed new security measures at European airports.

The European Commission is finalizing a proposal for new security measures, which includes restrictions on passengers bringing liquids, gels and pastes onboard aircraft. This proposal is expected to set out two prospective solutions for securing liquids, gels and pastes purchased by passengers from airside retail outlets that are situated after police and immigration controls but before the security restricted area. These solutions are for (a) purchases of liquids, gels and pastes to be delivered to passengers preparing to board aircraft in the security restricted area, or (b) purchases of liquids, gels and pastes to be sealed in tamper-evident bags at the point of sale.

The European travel retail industry has serious reservations about the practicality and costs of delivering passenger purchases of liquids into the security restricted area of airports. Following the events of 10 August, "gate delivery" of liquid purchases was introduced for US-bound flights at a number of European airports. Gate delivery, even on a limited scale, has proven to be a major logistical challenge, enormously costly and very unpopular with the traveling public. Problems encountered have already forced London Heathrow airport to cease this practice.

The airside retail outlets of many European airports including Roissy-CDG 1, Frankfurt, Schiphol, Brussels, Athens and Vienna are situated outside security restricted areas. The size and complexity of these and other European airports, and the costs involved, make delivering liquid purchases into security restricted areas an unworkable solution.

The use of tamper-evident bags can effectively secure liquids, gels and pastes purchased from airside retail outlets and can close any perceived "security gap" between airside sales of liquids from outlets situated before security restricted areas. The European travel retail industry has since 10 August advocated for such a solution to enhance the security of these products purchased at airside retail outlets

The industry is encouraged by the consensus amongst EU Member States that new security measures must not unnecessarily hinder airport shopping and appreciates the cooperative approach of the European Commission to date in preparing the new security measures proposal.

The European Travel Retail Council calls on the European Commission to remove any reference in its forthcoming proposals to delivery of purchases into security restricted areas as a means of enhancing security at European airports and encourages instead the Commission to clearly support the proposed tamper-evident bag solution.

Yours sincerely,
Frank O'Connell
President
European Travel Retail Council

Similar letters were also sent from ETRC national associations to the transportation ministers of all European states and to the European Commission national representatives.

On September 28, a committee of the 27-member EU Regulatory Committee for Aviation Security (AVSEC), in preparation for a European Commission meeting on October 12, agreed to a set of proposals to the commission that came very close to meeting ETRC concerns:

- Liquids, gels and pastes purchased from retail outlets beyond the point where boarding passes are controlled will not be affected by any new security measure. This means that separate rules are NOT required for the Schiphol, Brussels, Paris CDG2 type airports. *Passengers will be able to shop as normal in all airside shops;*
- Goods bought by transfer passengers or by passengers on the outward leg of a same-day return journey should be placed in sealed bags which will be recognized as secure within all EU (and EEA) airports, and therefore will not be treated as part of the new personal landside to airside liquid allowance, *thereby allowing transfer and same-day return passengers to shop as normal at airside retail stores for liquor and perfume etc.* This will apply to passengers from EU & EEA (Norway, Switzerland, Iceland etc.) airports only. This applies therefore to a passenger flying Heathrow–Copenhagen–Heathrow, for example, but only if the trip takes place on the same day; but it does NOT apply to a passenger flying, for example, Karachi–Amsterdam–-Dublin where the goods would be confiscated in Amsterdam because they were not bought at an EU/EEA airport;
- Personal liquid limits for passengers to take landside to airside will be 100 ml per individual object with a maximum of what can be fitted into a one-liter transparent bag (20 cm x 20 cm) to be presented at security screening;
- All these measures will be subject to six-monthly reviews by the AVSEC committee.

This decision was formally included in EU Regulation 1546/2006 and formally entered into force 20 days later, on November 6, 2006.

## NEXT STEP: IT'S A LONG WAY TO COME BACK TO NORMALITY

### The Supply Chain

Key to the tamper-evident bag system is airside retail's existing supply chain. As has been said, airside retail is the most heavily regulated retail sector in the world and it is also among the most secure.

Over the last three decades, the European airside retail sector has worked with suppliers and distributors to put into place a safe and secure supply chain running from the manufacturers of goods for airside retail to the retail outlet at the airport. The majority of goods sold at airside retail outlets, whether within the security restricted area (SRA) or airside prior to the SRA, are common to both the domestic and travel retail markets. These goods are manufactured without knowledge of their final retail destination, which ensures a random selectivity at distribution points for the majority of goods sold from

airside retail outlets. Where goods are manufactured exclusively for travel retail, separate security provisions are put in place prior to distribution. All goods destined for airside retail are dispatched under strict loading procedures, which include the sealing and scanning of bulk packages, the sealing of trucks and containers used to transport products, and detailed manifest checks to ensure that only what is dispatched is delivered. The selected forwarding companies used by manufacturers are required to institute rigorous security procedures for the delivery of goods for airside retail to customs-regulated bonded warehouses. These bonded warehouses have secure perimeters and are guarded under CCTV surveillance 24 hours a day. Permanent and temporary staff at these warehouses are subject to background screening by government authorities.

Only goods ordered by airside retail outlets are allowed into these warehouses, and all goods received must arrive sealed and with documentation detailing the passage of these goods from the manufacturer to the warehouse. Retail staff access to and from these warehouses is strictly regulated, and personnel are generally prohibited from bringing items from outside into a bonded warehouse. The bonded warehouses are subject to inspection by customs and police authorities, while warehouse staff are subject to random security checks.

The movement of goods from bonded warehouses to airside retail outlets is again tightly controlled. Goods are transported in locked metal cages with detailed inventory documentation. All goods, for sale through airside retail outlets whether before or within the SRA, are subject to inspections and security checks before they are prepared for sale in retail outlets. Once it arrives at airside retail outlets, each consignment of goods must be registered and signed for by authorized retail managers.

All retail staff members working in airside retail outlets are subject to background screening by government authorities. These staff members and all sales representatives of companies providing goods for sale at airside retail outlets are required to carry special identification and are screened by security agents each time they go airside in the airport. Every sale of a good at an airside retail outlet is captured on sophisticated electronic point-of-sale systems, which record passenger flight details, time and date of purchase, name of retail salesperson, and full description of items bought. These processes and back-office IT systems also ensure that full stock inventory controls are in place and all purchases are referenced against carefully recorded inventories.

### The Tamper-Evident Bag

The second element of the system is the specially designed bag to be used by passengers to carry liquids, gels and pastes purchased at an airside retail outlet prior to the SRA.

These bags are largely transparent and made from durable plastic. The bags are to be sealed by the retail sales assistant using a special strong adhesive strip or other means. Once the bag is sealed, the contents of the bags cannot

be accessed without visible damage to the bag. Sealed bags cannot be resealed. The bags have reinforced handles and are easily and safely portable, even when containing heavier items.

The surface area of the tamper-evident bags will prominently display a notice to customers that as part of new European Union (EU) security restrictions, airside retailers are required to seal liquid purchases in these bags. This notice will instruct customers not to open the sealed bag until they have reached their final destination. It is proposed to have the following messages on all bags:

*Side One: EU REGULATION*

Not to be opened until final destination reached

*Side Two: EU REGULATION*

Passengers transferring to another flight or returning home same day—opening or tampering with this sealed bag may result in confiscation at security check

Passengers not returning same day need to check liquid/gel items over 100ml into Hold Baggage

The bags will also have a retailer or airport brand of an agreed-upon size printed on the surface area, which will also facilitate the identification of purchases. The tamper-evident bags will be provided only to departing passengers in possession of a valid boarding card and purchasing liquids, gels, and pastes from airside retail outlets. Relevant items purchased will be placed in the bags by airport retail staff. The passenger's sales receipt/invoice for the items purchased will be placed in the bag and secured to face outward so as to be clearly readable. Retail staff will then seal the bag. The sales receipt/invoice, which will be visible to anyone examining the bag, will clearly display in an easily readable format the date and time of purchase, the quantity, and other details of items purchased.

At the point of sale, passengers will also be verbally instructed by retail staff not to open the tamper-evident bag until they reach their final destination.

At the screening point, and at subsequent screening points throughout the transit passenger's journey, security agents will be easily able to visually examine the contents of sealed bags with the sales receipt/invoice inside. Any tampering with bags will be clearly visible to security agents. Once on board the aircraft, the sealed tamper-evident bags can be easily stowed like other hand baggage in overhead bins or beneath the seat in front of the passenger.

## Benefits of the Tamper-Evident Bag System

The tamper-evident bag system provides an effective and efficient means of extending airside retail's existing safe and secure supply chain to the passenger's final destination. Purchases of liquids, gels, and pastes from airside retail outlets within the SRA have already been recognized as secure. The use of tamper-evident bags in this security program ensures extra security for liquids, gels, and pastes purchased from airside retail outlets before the

security restricted area while dispelling any need for the gate delivery of liquid purchases at European airports, which has proven inefficient, costly, and unpopular with passengers.

Mutual recognition of the-tamper evident bag system between airports will allow transfer passengers and those returning the same day to continue to enjoy airport shopping. Using the tamper-evident bags, transit passengers will be able to securely transport liquid purchases on to their final destination without exceeding the limits on liquids, gels, and pastes in their hand baggage.

### Communication with Passengers

Airport security management will be giving information to passengers concerning new requirements on carrying liquids, while retailers will put a simple message across in local media, in advertising, and as signage at airport parking lots, as people check in.

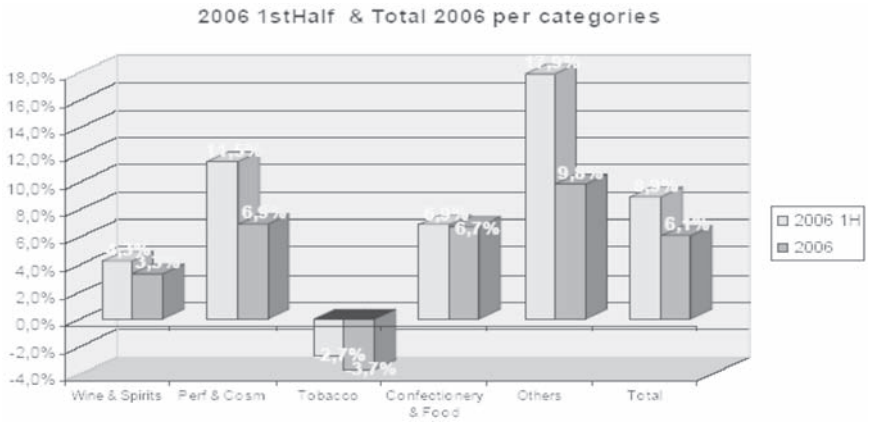
The message will be as follows: "all passengers can shop as normal once past boarding card/immigration controls. Any questions will be answered by sales staff." It's pretty certain that some very detailed information and training for all retail managers and sales staff will have to be provided for some years, in order to ensure that everybody involved in the business fully understands the new regulations, with whatever extra expenses are entailed.

### The Economic Impact on Airport Retailing Business of New Security Measures

In the first half of 2006, the growth of the European airport retailing sector sales sector increased 8.9 percent over the previous year. On the other hand, the second part of 2006 showed a more modest +6.1 percent. Perfumery and cosmetics showed an 11.5 percent increase in 2005 in the first half and a +6.9 percent increase in the second half, with spirits and wine performing at +.3% in the first half and +3.3% in the second half. Figures 6.1 and 6.2 give evidence from ETRC data.

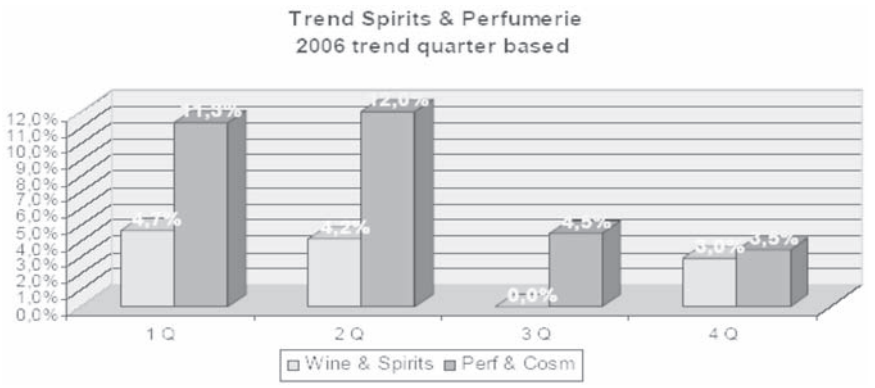
The wine and spirits and perfumery area showed negative growth in the first and second quarters of 2006 if matched with data referring to an EU air traffic growth of 6 percent year over year (YOY). However, it is not only liquids sales that have been deeply affected by the security measures. In fact, confusion in terms of communicating new rules and caused by a different implementation in each EU state member created a general negative consumer reaction. Confectionery and food but also clothes and accessories, electronics, jewelry, and watches showed slow growth in the second half of the year All these conditions meant a loss of sales in the duty-free and travel retail business in 2006 of at least US$300 million, most of it in the last four months of that year. As the average royalty fee that retailers usually pay to airport authorities is close to 30 percent of net sales, in the last four months of 2006, airports lost US$90 million worth of income. Moreover, airport authorities also had to bear increased security costs in terms of staff and technology.

**Figure 6.1**
**Impact of New Security Measures: 1st Half 2006 and Total 2006, Per Categories**




*Source:* Data from members of European Travel Retail Center (ETRC).

**Figure 6.2**
**Impact of New Security Measures: Trend in Spirits and Perfumery, 2006, Quarter Based**




*Source:* Data from members of European Travel Retail Center (ETRC).

## NEW ISSUES: NON-EU FLIGHTS AND PASSENGERS TRANSFERRING THROUGH EUROPEAN AIRPORTS

Another important issue arising at the beginning of 2007 was that passengers from non-EU airports transferring through European airports and carrying liquid/gel purchases had major problems at security screening, as

the regulations in relation to the acceptability and recognition of sealed bags apply only to EU airports and products sold on board EU airlines. ETRC promptly alerted colleagues in the Middle East, Asia, and the Far East, because these problems could pose a serious threat to sales. To make this happen governments need to recognize that a balance has to be struck between the sale of certain products and security risks. This begins with agreement on global recognition and standardization among the EU, the United States, and Canada on the security of duty-free and travel retail liquid, gel, and paste products and the tamper-evident bag security program.

With this mutual recognition setting a precedent, airports worldwide will need to adopt EU standards for overall airport security management, particularly practices relating to the supply chain for duty-free goods and airport staff screening. Airports must apply for formal recognition by the EU and the United States of their compliance with these standards, with this recognition established through bilateral agreements between the airport's host country and the EU and United States. ETRC's goal is to build a critical mass of bilateral agreements, which will pave the way for a global solution to the transfer passenger problem through harmonized global regulations.

On March 23, 2007, the International Civil Aviation Organization (ICAO) issued guideline recommendations to its 189 member airports for the specifications of tamper-evident bags plus proposed security principles for retail liquid, aerosol, and gel items for airport retailers and manufacturers involved in that practice and business.[3]

While these guidelines carry no obligation on the part of any country to comply with them, they are expected to be widely adopted, as most ICAO guidelines are for international airports.

The new guidelines contain one or two "optional additions" to existing practice, such as the inclusion of a security device—meaning a hidden graphic—inside the bag and a colored logo on the outside as a further means of recognition.

Section five of the guidelines is of particular significance, as it outlines the proposed security principles for retail liquid, aerosol, and gel items for airport retailers and manufacturers. These guidelines say that all liquids, gels, and aerosols (LAGs) should be handled in accordance with ICAO's recommendations contained in state letter AS 8/11–06/100 dated December 1, 2006.[4]

Introducing national regulations restricting liquids in hand baggage and the use of tamper-evident bags, does not, however, solve the transfer passenger problem for airports and airport retailers. Passengers arriving from a third country and transferring at EU airports will only be able to take sealed ttamper-evident bags through security points if the EU

- Recognizes the security of airports in the country of origin;
- Recognizes the security of the airport retail supply chain in the country of origin; and

- Formalizes mutual recognition of security standards in a bilateral agreement with the country of origin.

This is the second step for airports and airport retailers. If third countries can agree to mutual recognition of airport security standards and security procedures for the airport retail supply chain, airport retailers in those countries will be able to sell to EU-bound transfer passengers and solve the transfer passenger problem where it is most acute.

A strategic plan was prepared to deal with this difficult and confusing situation, which advanced European and U.S.-EU problems to global status.

ETRC moved strongly at this time with regard to this problems and the relevant steps were as follows:

- Prepare a "base protocol" including airport security standards for liquids restrictions, appropriate staff control and validation, and agreed-upon security standards for retail supply chains, based upon the simple principle that they must recognize the secure nature of the chain including the "known concept," which allows security personnel to easily verify the products, drafted by the European Commission, including elements regarding the tamper-evident sealed bag; and
- Propose this protocol from the European Commission be imposed on significant non-EU states with major traffic flows into Europe.

After many contacts between ETRC and the EC Transport Directorate, the latter decided to seek a mandate (permission) from the Transport Council (all 27 member states) to conclude agreements with third country groups.

Although this process could take a long time, the fact that the European Commission embarked upon the process sent a strong signal of the need to have bilateral agreements with third countries. In the case of the United States, it appears that there was no need for a mandate, due to the open skies agreement.

As of April–May 2007 there has been significant progress in attempts to forge a solution to the current passenger transfer problem. The European Commission has come forward with a new approach, which will allow liquids bought in airport duty-free shops from certain third countries and in approved tamper-evident bags to be recognized as secure by security screening at EU airports. The aviation security committee gave the European Commission approval to come forward with a legislative proposal for approval at their meeting on May.

In brief, this new proposal will allow the EU to create a list of approved countries based upon certain strict criteria. The criteria have yet to be finalized, but obviously inclusion on this list will require the full application of both ICAO state letters. We understand that countries that do not recognize EU competence on aviation issues may be barred from this list, but we are awaiting confirmation of this.

The European Commission has never taken such an approach to an international problem before, so it remains to be seen how long it will take for countries to be approved following the adoption of the proposal. This was a major step forward and one that, if adopted, will provide a solution to many of

our problems. There is still much ground to be covered before that becomes a reality, and as always, the details of the proposal may reveal some unexpected problems.

On May 30, the European Commission presented a new proposal to AVSEC. This regulation, once approved by the member states, will allow the EU to recognize the security of liquid, gel, and paste products purchased from airport shops in selected third countries. This recognition will be dependent upon airports in those selected third countries adopting the ICAO guidelines on restricting liquids in hand baggage and having in place duty-free supply chain security standards and procedures comparable to those at EU airports.

This recognition will allow passengers departing approved airports to transfer at EU airports with their duty-free liquids sealed in standardized and easily identified security tamper-evident bags, as specified by ICAO. Following approval of the regulation, the commission will assess and unilaterally extend recognition to third countries and airports on a priority basis and in the expectation that these third countries will extend reciprocal recognition to purchases from EU airport shops.

The approval and adoption of the commission's unilateral recognition proposal marks a major step forward in solving the transfer passenger problem and safeguarding the global duty-free market.

The European Commission has made clear that the proposal was a direct result of extraordinary political pressure brought to bear on the institution and member states by a broad alliance of industry stakeholders and the European Parliament.

However, the unilateral recognition proposal is not the end of industry efforts to safeguard the global duty-free market. Further steps would include the following:

A. Maximize the number of third countries/airports receiving EU recognition;
B. Make the recognition process as simple as possible; and
C. Prevent ICAO from setting additional standards and provisions, especially for tamper-evident bags.

Maximizing the number of third countries receiving recognition was actually the most critical issue in relieving the current pressures on non-EU airport retailers who are unable to sell to EU-bound transfer passengers and safeguarding future sales to departing EU passengers transferring in third countries.

At the end of this long process of responding to the situation after August 10 in terms of sales and economic results, in October 2007, Singapore became the first country to be approved under Regulation (EC) 915/2007, following the EC's decision to "recognize" that security at Singapore's Changi Airport met ICAO standards. This means that passengers arriving from Singapore will no longer have to forfeit their duty-free liquid at EU airport security checkpoints when connecting with another flight.

After Singapore, the EC confirmed that four more countries had formally given notice of application for mutual airport security recognition. The new applicants are Armenia, Canada, Macedonia, and Malaysia, and they join other countries that are already known to have applied, including Argentina, Australia, Croatia, Dubai, Israel, and Mauritius. However, U.S. airports, after a long discussion time between the EC and TSA, still have unsolved problems. Of particular interest among the new applicants is the position of Canada, which is seen as having an influence on the future when it comes to U.S. policy related to mutual security recognition.

## CONCLUSIONS

As of the beginning of 2008, ETRC continues to work strongly on policies supporting the duty-free and travel retail business. A positive result in 2007 in terms of European airports' retailing sales—a significant recovery in the first nine months of that year—meant that all initiatives proceeded in the right direction, at the same time providing a safer environment for the security of all passenger travelers.

The August 10 events have clearly shown that the best outcome in terms of responses and strategies can only be achieved through a continuing dialogue and strict cooperation between institutional bodies, like the European Commission, and representatives of all areas of industry involved in the process. ETRC definitely played a pivotal role in this process by successfully leveraging the interests of its associates. The right lobbying action and the strong support of all ETRC national association members in the first phase and the positive response of all organizations in various geographical areas in the second, but not less crucial, phase show that we need to learn to react differently in order to arrive at the right answers, to combat the negative forces that can strongly influence our social and economic situation.

## NOTES

1. For a broad explanation of these activities, see David Jarach, *Airport Marketing* (London: Ashgate, 2005).

2. U.S. Department of Transportation, "New Security Measures," August 14, 2006, http://www.uktransport.co.uk.

3. International Civil Aviation Organization, "Recommendations of Temper-Evident Bags," ICAO, May 23, 2007, www.icao.int.

4. International Civil Aviation Organization, "Recommendations on LAGs," ICAO, December 1, 2006, www.icao.int.

# CHAPTER 7

# Passenger Screening

*Mark B. Salter*

Passenger screening is a key component of civil aviation security and is subject to the same pressures of technological innovation, limited space, efficiency, efficacy, and customer service. It is the most important osmotic barrier, or filter, in the aviation security system: Individuals move from a public space to a "sterile" space, which then allows them access to terminal and aircraft. Because the vast majority of illegal interventions in civil aviation have been committed by individuals (rather than remotely with explosives), passenger screening is an important filter in the task of separating off the safe from the dangerous. Screeners themselves are hired, trained, and managed as part of the overall security architecture of the airport and civil aviation system. One of the dominant policy debates within the field of transportation security is the question of the federalization or privatization of the screening workforce.[1] In this overview, we will address three areas of passenger screening: what is screened, where passengers are screened, and how passengers are screened.

## SCREENING FOR WHAT OR FOR WHOM?

Aviation security is largely reactive: criminals and terrorists are faster innovators than government; police and civil aviation bureaucracies are more conservative in their policies. After wide-scale terror attacks on jetliners in the 1970s, X-ray arches were introduced at the gates to airplanes. After attacks on airports themselves, passenger screening was moved to centralized choke points. After intelligence about gels and liquids was received, new regulations were put in place.

The primary focus of passenger screening has been on screening for prohibited items, rather than for suspect individuals.[2] Passenger screening

follows one of two models: individual travelers are screened either differentially according to risk or behavioral profiles (an investigatory model) or with the same procedures regardless of individual characteristics (a screening model). This represents a fundamental difference—either passengers are treated according to their risk profile or they are treated precisely the same regardless of risk. This section will examine the origin and importance of the prohibited items list, the recent trends toward behavioral profiling, and the importance of identity management.

### Objects and the PIL

Following the conservative trend in security measures, passenger screening traditionally focuses on the detection of prohibited items in sterile areas and aircraft. The International Civil Aviation Organization (ICAO) issues a recommended Prohibited Items List (PIL), which is updated according to the advice of the Aviation Security (AVSEC) panel of experts and the International Explosives Technical Commission. This is supplemented with a list of "dangerous goods," such as explosives, corrosive or flammable chemicals, dangerous biological agents, radioactive material, toxic waste, and so forth, that are also prohibited. The PIL contains a number of categories and varies by national standard. The standard ICAO list includes firearms and other weapons (guns, bows, toy guns); pointed, edged, sharp objects (swords, axes, ice skates, scissors); blunt instruments (baseball bats, clubs, sports equipment); explosive or flammable substances (aerosols, detonators, grenades, ammunition); toxic chemicals (acid, mercury, chlorine, fire extinguishers, mace, poisons); and other potentially dangerous items (corkscrews, hypodermic needles, knitting needles, razor blades).

The PIL grows with new additions, new intelligence, and new fears. It changes as new threats emerge and old ones fade away. The inclusion of liquids and gels, for example, has continued, even after the specific threat has vanished. Has there been an attack on civil aviation by knitting needles or a safety razor? This is an example of risk management within the sector. Threats are gauged by the frequency of breach and the potential impact of failure to detect.[3] In short, the cost of a false positive (the detection of a nonthreatening item) is always cheaper than the potential impact of a false negative (the nondetection of a threatening item).[4] It is only when cumulative false positives create unacceptable delays in the system that the screening process is modified.

An extensive PIL makes up for the lack of a clear ability to determine and detect dangerous individuals, by attempting to remove intentionality from the screening process. It does not matter if your ax or pistol is benign, the risk posed by the item is too great, and the item itself is prohibited. As a result, we know that "terrorists fly all the time"—and in a significant way, this does not pose a problem for the civil aviation sector as such (although it may pose problems for national security and intelligence agencies). If terrorists and criminals fly without prohibited items, then the integrity of the system

is secured. At least, such is the calculation. This is undermined by the institutional dynamic of illegal behavior: if we accept that terrorists and criminals are better and faster entrepreneurs than governments are regulators, then a system based on items can only be driven by failure. An item appears on the list because of a dangerous use (or because of a reasonable guess by a security official). Any PIL will always be incomplete and lacking in imagination.

## INTENTIONS, BEHAVIOR, AND PROFILES

The items on the list are for the most part benign unless used with malice—but bad intentions are notoriously difficult to gauge. In fact, we would argue that it is virtually impossible to find out what intention lurks in the heart or mind of a potential criminal or terrorist, at least with current technology. The face-to-face interrogation of individuals (did you pack this bag yourself, where are you traveling, and so forth) is, consequently, a crucial supplement to physical screening. As a result, some aviation security officials are moving toward a screening process that entails the evaluation of behavior or risk profiling. In these cases, while intention cannot be gauged or guaranteed, there is an assumption that behavioral cues and or criminal/terrorist profiles can aid screeners in facilitating the process for the vast majority of unproblematic passengers and help them focus their scarce technological and human resources on "risky" individuals. The possibility of determining the intentions of travelers is far beyond the horizon, although a great deal of technological and psychological research is currently dedicated to this project. Research into individual brain imaging, the quantification of the physiological markers of stress in large groups, and the development of integrated surveillance systems are all ongoing.

Two models of profiling are becoming more widely used in aviation passenger screening: behavioral profiling and risk profiling. Behavioral profiling sets out a training and policy framework for the evaluation of individuals within the airport environment. The American Transportation Security Administration has been piloting a program called "Screening Passengers by Observation Techniques," which utilizes this kind of profiling.[5] This is often called the Israeli method of security screening, since it has been in use at Ben Gurion airport and other checkpoints for a number of years.[6] Cultural sensitivity is necessary within this context, since body language can have radically different meanings within different cultural systems: the amount of direct eye contact with persons in authority and the amount of personal space maintained between individuals vary wildly. Within this context, however, behavioral profiling has the potential to focus on an individual and his/her actions. For example, a recent article reported that after the installation of a CCTV system at Geneva airport, police officers discovered that the typical thief in the arrivals area did not fit the "typical" pattern: rather, it was individuals who were dapper and well-dressed who stole the most luggage.[7] As Redick argues, "The science of profiling was developed from the processes of narrowing a

list of suspects by identifying areas of interaction of numerous generalizations belonging to all suspects. Profiling, which relies solely on race, ethnicity, religion, or national origin in selecting which individuals to subject to routine or spontaneous investigatory activities, is inappropriate. Scientific profiling utilizes mathematical probabilities without relying on race as a major factor in the analysis."[8] The case of Raed Jarrar is illustrative: a human rights activist returning from a workshop was traveling on Jet Blue, wearing a T-shirt which read, in Arabic and English, "We will not be silent." Passengers, airport security, and airline employees asked Jarrar to cover up his T-shirt, on the basis that going to an airport with a T-shirt in Arabic script is "like wearing a T-shirt that reads 'I am a robber' and going to a bank."[9] Scientific profiling has the ability to check the pervasive impact of stereotypes.

Risk profiling assumes that the majority of terror attacks or criminal acts of intervention are committed by the most obvious suspects, although that profile will change according to national context. Two types of data are included in this assessment: incident data, regarding the particular profile of the flight, and individual data, based on the particular individual. The system is alert for the "typical" pattern of terror or criminal flights and for particular individuals or profiles. As a typology of hijacking in the past 10 years indicates, the threat may often be difficult to predict. Miller demonstrates that the majority of unprepared hijackings were nonterrorist in nature, whereas the majority of terrorist hijackers were affiliated with a political organization.[10] Predicting from this data which national or ethnic profiles might be subject to greater scrutiny, however, is fraught: international hijackers "comprised more than 20 different nationalities."[11] Profiling according to risk categories or behavior, especially in an environment that is structured by human rights obligations and civil liberties groups, must be done with great care.[12]

## IDENTITY MANAGEMENT AND DOCUMENT MANAGEMENT

Passengers cannot prove their identity absolutely and without doubt, especially within the constraints of time and efficiency at the screening point, the airline check-in counter, or the international border. With various documents, however, passengers can prove the isomorphism between the identity we claim, our government records, and our body. Passports, and other national identity documents, make the strongest claim for identity and security: the application process is more stringent than for other kinds of identity cards, the legal status of citizenship and often the prima facie authority to travel is proven through nationality and visas, and the history of previous travels is recorded.[13] There has been a global push for improvement in the integrity of passport documents, standards that are also set by ICAO. Starting with the development of the machine readable passport and subsequently machine readable travel documents, ICAO has established a nonbinding global norm for passports that details format, security measures, and some minimal

technological standards. Passports themselves are issued nationally, and so ICAO's standards are not uniformly implemented. One of the challenges to border, immigration, and intelligence agencies is the lack of uniformity in passports and the data they contain. This question is not simply one of the ability of a state to control population flows, but as airlines and airports are increasingly required to police migrants through carrier sanctions, the integrity of a global identity system becomes an important issue for actors throughout the civil aviation sector.

The passport, in itself, is no guarantee of safety. Richard Reid, the attempted shoe bomber, carried an entirely authentic passport. Passengers and documents must be connected to intelligence for there to be any integrity to the civil aviation security system. As more and more states move toward using some kind of no-fly or watch list, secure identity documents will become more important. The Computer-Assisted Passenger Profiling System (CAPPS), the now-defunct CAPPS II, and the prospective Secure Flight programs in the United States are automated risk evaluation systems.[14] Using information from policing, immigration, and intelligence agencies, as well as embedded data from the Passenger Name Record (PNR) or Advanced Passenger Information (API), the system attempts to rank the risk of an individual. The risk score is then translated into different levels of security screening. One of the concerns of these competing watch lists is that there is no reconciliation of various national databases, and it is completely unclear how "false positives" (falsely suspected individuals) might enjoy unrestricted travel.

A single global identity management system would pose its own problems and concerns. In terms of contemporary and future passenger screening, travel documents are important for identity and security management. The proliferation of standards, formats, and data makes passenger screening by identity extremely difficult. As a consequence, passenger security has taken a risk approach that attempts to discriminate between known, low-risk travelers and unknown, high-risk travelers.

## DELOCALIZATION, SELF-SERVICE, AND FAST TRACKS

Over the past 50 years, the actual site of passenger screening has moved further and further from the airplane: from the airplane ramp to the gate, to choke points within the terminal. The three primary drivers of the centralization of passenger screening were the geometric increase in passenger volume and terminal capacity, the changing nature of attacks on airports and aircraft, and finally the increased cost of security equipment. Screening points became centralized choke points in passenger flows that were integrated into airport design.[15] Retail concessions and food outlets became key drivers of airport revenue, based on anticipated dwell time. In the "nonspace" of the terminal, between security and the aircraft, airports came to resemble "malls for the mobile."[16] However, passenger acceptance of the delays accompanying centralization was directly related to the ease of passing through this security filter.[17]

We see this particularly after September 11 2001, and the new liquids ban imposed in 2006, when new screening procedures caused massive delays, and public opinion about security measures became extremely negative. With widespread delays, passenger frustration, and concerns by stakeholders across the sector, the industry has moved toward a "risk management" approach to security screening. Rather than using a single, central, intense screening checkpoint, airports are trying to discriminate between low-risk and high-risk passengers—through special programs but also in space. Business travelers are often accorded their own dedicated security lines, because of an assumption that frequent travelers pose less risk. Pilots and aircrew also sometimes enjoy different security access (though this is not uniform). This delocalization of security screening can be seen throughout the airport system: catering, fuel, and maintenance facilities are often located off-site and are part of the larger airport security plan. Catering facilities, for example, have access control at the plant, load catering trucks and stores in a secure environment, and then secure the items for their trip to the airport. Given these security standards, trucks are subject to less stringent security screening when entering the air-side operational area.

Within a risk model, "low-risk" passengers are identified and may register for frequent-flyer or fast-track programs, such as Clear, currently on trial in select U.S. airports, the Privium program at Schiphol, or Fastlane at Ben Gurion Airport. As Stone and Zissu argue, "The RT [Registered Traveler] program has two complementary objectives: to expedite the on-the-spot security screening of passengers who have been vetted and have been cleared by the TSA (the security threat assessment), and to use their security resources more efficiently. By segregating the general population of travelers into those who are not suspect and those who are suspect, the TSA can more effectively allocate their limited security resources to screen the smaller but riskier group of nonregistered travelers."[18]

The low-risk travelers submit to extended security background checks in order to bypass extensive security checks at the airport, although they are of course subject to the same level of security screening (but often with shorter lines and a shorter waiting period). An extensions of this trend toward the investigative model (differentiation in the level of passenger screening) can be seen in the off-site check-in or baggage drop-off, which is currently on trial at a number of airports ( the Heathrow Express system is on trial at Paddington, and in Canada a system is on trial in preparation for the Vancouver Winter Olympics). A final trend in the facilitation of passenger processing has been the increase in self-service. Passengers are able to check themselves into flights, check their baggage, and proceed through border points without engaging with any kind of agent (ticket, airline, or customs). Companies report that this flexibility and increased efficiency is praised by passengers—but it is unclear whether the inherent security function of the face-to-face interaction is preserved in such an impersonal system. Traditionally, passenger facilitation has been contrasted with security. A new movement is afoot among aviation

security professionals, guided by the principles of risk management, to think of security and facilitation as two sides of the same coin.

There is a legitimate concern among analysts and civil libertarians about the extension of surveillance away from legitimate sites of concern, such as the airport, into the very fabric of society. The use of CCTV (closed circuit television) networks, scanner technologies, biometrics, and profiling in public spaces has the effect of creating a chilly political and social climate.[19]

## TECHNOLOGY

Technology is a force-multiplier, enabling screeners to detect prohibited and dangerous items more reliably and efficiently. But hard technology is not a magic solution without the soft technologies of training, human resources, and management. There are four areas of important technological innovation: detection, tracking, data management, and human resources.

Detection technologies have been greatly enhanced over the past 10 years. For the past 40 years, airport screening has been conducted using the X-ray walk-through archway and a handheld wand, with few technological improvements since their invention. These metal detectors create a low-intensity magnetic field that is disrupted when metal is passed through. Consequently, they cannot detect ceramic weapons or explosives. Explosive detection systems (EDS) and improvements in detection technologies, such as CT (computerized tomography) and multiple imaging techniques have increased screening efficacy. New technologies such as ionized EDS systems, millimeter wave scans, and backscatter X-rays all promise new levels of detection. Global standards and recommended practices, set by ICAO, are minimal and do not include these new innovations.

While some developing countries are struggling to provide the basic security equipment and training, American, European, and other developed countries are moving forward with the next generation of technologies. The foundation of these technologies is still the individual screener, who is always more flexible and discerning than any technological system. New research on visual acuity has led to a real advance in training: TIPS (the threat image projection system). In this computer program, which is integrated into both training and line systems, images from a library of prohibited items are superimposed onto screened hand luggage.[20] These continually displayed threat objects help maintain screener awareness and alertness and integrate training into the everyday practice of screening. At the root of these training and audit programs, however, there is a fundamental weakness. It is not clear how to measure the efficacy of different training regimes, technologies, or policies: often measurement is exclusively the number of prohibited items collected or the results of covert infiltration tests.[21] This problem will become acute as Security Management Systems (SeMS) or Enterprise Risk Management (ERM) standards become the global norm.[22]

The reduction in the cost of processing power and data storage has led to new programs for data mining, fuzzy logic, and "nonobvious relationship analysis."[23] More data are being collected and analyzed to generate specific intelligence and general risk profiles. While the actual integration of disparate databases is only nascent, there is potential for a wide-ranging database of passengers.[24] New innovations in electronic boarding passes, mobile devices, and RFID (radio frequency identification) tags have made the tracking of individuals and baggage more robust.

We can expect more dispersed detectors that can be integrated into the whole airport space, including transit, connections, screening, and terminals. Researchers are currently experimenting with systems that can identify individuals from their posture and movements. Passive biometric capture points have been used in large public spaces, such as sports venues, public transport facilities, and airports, to gather facial photographs, which can then be compared to large-scale databases. CCTV control systems can currently track individuals moving through a terminal, and plot their movement over time (and in the past). In short, we can expect that as these systems become more complex, more reliable, and more integrated, security screening will be scattered throughout the airport.

## CONCLUSION

We can point to another possible trend within passenger screening, that is, the desecuritization of screening. A minority view argues that contemporary passenger screening is neither police nor security work. Essentially, screening is a logistical problem. The key concerns of security screeners are not to investigate any criminal or terrorist activity, per se, but rather to process a large number of cases, to resolve alarms, and to use technology to identify prohibited items, each with a high degree of reliability and some degree of customer service. As more security functions in society are taken over by the private sector, it is possible that aviation passenger screening will also be undertaken by nonsecurity firms that can offer trained, efficient, and effective screening, with no natural security expertise.

There are three broad trends in passenger screening, These are increased reliance on technology, the adoption of a risk analysis or investigative model of screening, and the delocalization of screening. This poses challenges as well as offering opportunities: complex, interdependent systems offer the most flexibility and reliability for a task that is constantly changing. However, the core inputs to the system (intelligence, training, and passenger behavior) remain constrained.

## NOTES

1. J. Hainmüllerand J. M. Lemnitzer, "Why Do Europeans Fly Safer? The Politics of Airport Security in Europe and U.S.," *Terrorism and Political Violence* 15 (2002):

1–36; P. Seidenstat, "Terrorism, Airport Security, and the Public Sector," *Public Administration Review* 21 (2002): 274–91.

2. M. B. Salter, "Governmentalities of an Airport," *International Political Sociology* 1 (2007): 49–66.

3. M. B. Salter, "SeMS and Sensibility: Security Management Systems and the Management of Risk in the Canadian Air Transport Security Authority," *Journal of Air Transport Management* 13 (2007): 389–98.

4. H. G. Frederickson and T. R. Lapore, "Airport Security, High Reliability, and the Problem of Rationality," *Public Administration Review* 62 (2004, Special Issue): 33–43.

5. S. B. Donnelly, "A New Tack for Airport Screening: Behave Yourself Time," *Time*, 2006, http://www.time.com/time/nation/article/0,8599,1195330,00.html.

6. B. Seymour, "Behavior Pattern Recognition and Aviation Security," *Journal of Security Education* 1 (2005): 69–79.

7. F. Klauser, J. Ruegg, and V. Novembre, "Airport Surveillance between Public and Private Interests: CCTV at Geneva International Airport," in *Politics at the Airport*, ed. M. B. Salter, 163–90 (Minneapolis: University of Minnesota Press, 2008).

8. S. R. Reddick, "The Case for Profiling," *International Social Science Review* 79 (2004): 154–56.

9. L. Volpp, "Citizenship Undone," *Fordham Law Review* 75 (2007): 2579–86.

10. J. M. Miller, "Conceptualizing the Hijacking Threat to Civil Aviation," *Criminal Justice Review* 32 (2007): 226.

11. Ibid., 228.

12. American Civil Liberties Union, *ACLU of Massachusetts Challenges Use of Behavioral Profiling at Logan Airport*, 2004, http://www.aclu.org/safefree/general/18765prs20041110.html.

13. M. B. Salter, "Passports, Security, Mobility: How Smart Can the Border Be?" *International Studies Perspectives* 5 (2004): 71–91.

14. A. Barnett, "CAPPS II: The Foundation of Aviation Security?" *Risk Analysis* 24 (2004): 909–16.

15. P. Adey, "May I Have Your Attention": Airport Geographies of Spectatorship, Position, and (Im)mobility," *Environment and Planning D: Society and Space* 25 (2007): 515–36.

16. D. Lyon, "Airports as Data Filters: Converging Surveillance Systems after September 11," *Information, Communication and Ethics in Society* 1 (2003): 15.

17. K. Gkritzaa, D. Niemeierb, and F. Mannering, Airport Security Screening and Changing Passenger Satisfaction: An Exploratory Assessment." J*ournal of Air Transport Management* 12 (2006): 213–19.

18. C. A. Stone and A. Zissu, "Registered Traveler Program: The Financial Value of Registering the Good Guys," *Review of Policy Research* 24 (2007): 447.

19. There is an extensive literature on "surveillance studies" that explores this question in greater depth. See D. Lyon, *Surveillance Studies: An Overview* (London: Polity Press, 2007).

20. A. Schwaninger, D. Hardmeier, and F. Hofer, Measuring Visual Abilities and Visual Knowledge of Aviation Security Screeners," *IEEE Proceedings of the International Conference on Security* 38 (2004): 258–64.

21. See U.S. Government Accountability Office, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*, 2003 (GAO-03–1173).

22. Salter, "Governmentalities of an Airport," 2007.

23. J. Jonas, "Threat and Fraud Intelligence, Las Vegas Style," *IEEE Security and Privacy* 4 (2006): 30–31.

24. C. J. Bennett, "Comparative Politics of No-Fly Lists in the United States and Canada," in *Politics at the Airport*, ed. M. B. Salter (Minneapolis, MN: University of Minnesota Press, 2008), 120.

## REFERENCES

American Civil Liberties Union. 2004. "ACLU of Massachusetts Challenges Use of Behavioral Profiling at Logan Airport." Available at: http://www.aclu.org/safefree/general/18765prs20041110.html. Accessed January 4, 2008.

Barnett, A. 2004. "CAPPS II: The Foundation of Aviation Security?" *Risk Analysis* 24: 909–916.

Bennett, C. J. 2008. "Comparative Politics of No-Fly Lists in the United States and Canada." In *Politics at the Airport*, ed. M. B. Salter, 88–122. Minneapolis: University of Minnesota Press.

Donnelly, S. B. 2006. "A New Tack for Airport Screening: Behave Yourself Time." Available at: http://www.time.com/time/nation/article/0,8599,1195330,00.html. Accessed December 27, 2007.

Gkritzaa, K., D. Niemeierb, and F. Mannering. 2006. "Airport Security Screening and Changing Passenger Satisfaction: An Exploratory Assessment." *Journal of Air Transport Management* 12: 213–19.

Hainmüller, J., and J. M. Lemnitzer. 2003. "Why Do Europeans Fly Safer? The Politics of Airport Security in Europe and U.S." *Terrorism and Political Violence* 15: 1–36.

Jonas, J. 2006. "Threat and Fraud Intelligence, Las Vegas Style." *IEEE Security and Privacy* 4: 28–34.

Klauser, F., J. Ruegg, and V. Novembre. 2008. "Airport Surveillance between Public and Private Interests: CCTV at Geneva International Airport." in *Politics at the Airport*, ed. M. B. Salter, 163–90. Minneapolis: University of Minnesota Press.

Lippert, R., and D. O'Connor. 2003. "Security Assemblages: Airport Security, Flexible Work, and Liberal Governance." *Alternatives* 28: 331–58.

Lyon, D. 2003. "Airports as Data Filters: Converging Surveillance Systems after September 11." *Information, Communication and Ethics in Society* 1: 13–20.

Lyon, D. 2007. *Surveillance Studies: An Overview*. London: Polity Press.

Mew, K. 2005. "Airport Security Screening: Privatize or Federalize?" *Public Works Management and Policy* 10: 3–9.

Miller, J. M. 2007. "Conceptualizing the Hijacking Threat to Civil Aviation." *Criminal Justice Review* 32: 209–32.

Salter, M. B. 2004. "Passports, Security, Mobility: How Smart Can the Border Be?" *International Studies Perspectives* 5: 71–91.

Salter, M. B. 2007a. "Governmentalities of an Airport." *International Political Sociology* 1: 49–66.

Salter, M. B. 2007b. "SeMS and Sensibility: Security Management Systems and the Management of Risk in the Canadian Air Transport Security Authority." *Journal of Air Transport Management* 13: 389–98.

Schwaninger, A., D. Hardmeier, and F. Hofer. 2004. "Measuring Visual Abilities and Visual Knowledge of Aviation Security Screeners." *IEEE Proceedings of the International Conference on Security* 38: 258–64.

Seidenstat, P. 2002. "Terrorism, Airport Security, and the Public Sector." *Public Administration Review* 21: 274–91.

Seymour. B. 2005. "Behavior Pattern Recognition and Aviation Security." *Journal of Security Education* 1: 69–79.

Stone, C. A., and A. Zissu. 2007. "Registered Traveler Program: The Financial Value of Registering the Good Guys." *Review of Policy Research* 24: 443–62.

U.S. General Accounting Office. 2003. "Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining." GAO-03–1173. Washington, DC: U.S. Government Accountability Office.

Volpp, L. 2007. "Citizenship Undone." *Fordham Law Review* 75: 2579–586.

# CHAPTER 8

# Operations Research Applications in Aviation Security Systems

*Adrian J. Lee, Alexander G. Nikolaev, Sheldon H. Jacobson, and John J. Nestor*

The terrorist attacks on the twin towers of the World Trade Center and the Pentagon on September 11, 2001, and the foiled plot to destroy 10 United States–bound transatlantic flights in August 2006 are two major events in history that indicate the importance of designing and operating robust aviation security systems to keep our skies safer. Events like these will forever alter the way travelers view aviation security, and we need detailed analyses of all components of the security system to ensure confidence that the aviation security system as a whole will minimize any possibility of future terrorist plots.

Arnold Barnett highlights several important questions and issues surrounding the events of September 11, and how air travel has been and will continue to be affected.[1] Barnett questioned the structure of the passenger and baggage screening system in place prior to the September 11 attacks, asked how the system could have detected the terrorists, and raised the question of tradeoffs between security and safety. Since that time, aviation security systems have undergone significant changes, though the analysis of these systems continues to lag well behind their actual operation. For example, Barnett shows how both the Transportation Security Administration's (TSA) "registered traveler" program and the Computer-Assisted Passenger Prescreening System, CAPPS II, would allow large numbers of passengers the means of becoming exempt from certain security measures.[2] Barnett states, however, that the Registered Traveler program is unlikely to be supported by any convincing cost/benefit analysis, and that CAPPS II may fix in advance the TSA's perception of a potential terrorist's level of risk.

Over the years since the September 11 attacks, aspects of aviation security systems have undergone changes, designed to prevent similar tragic events.

Some of the changes include fitting reinforced cockpit doors, expanding the federal air marshal program, allowing only ticketed passengers to enter the secured areas of airport terminals, utilizing bomb-sniffing dogs, and screening 100 percent of checked baggage for explosives.

Many of the changes have been politically driven—a direct result of the "knee-jerk" emotional response to September 11, rather than the result of any coordinated, systematic analysis and planning. For example, within two months after the attacks, the U.S. Congress mandated 100 percent screening of checked baggage by a federally certified screening device or procedure by December 31, 2002, as part of the Aviation and Transportation Security Act (ATSA). Prior to September 11, only a small fraction of checked baggage was screened in this manner. The rapid deployment of explosive detection devices in order to meet the deadline resulted in several billion dollars being invested before any type of systematic analysis of baggage screening security systems was performed.[3]

The field of operations research provides a unique set of methodologies and tools for designing and analyzing components of aviation security systems, such as passenger and baggage screening, since operations research is based on applying analytical methods to optimally allocate scarce assets and use them in making better-informed decisions. Operations research provides methodologies that can be used to determine the optimal spending of taxpayer dollars and the optimal use of security system assets, such as screening devices and personnel

This chapter provides a survey of aviation security system applications that have been used, or are well positioned to benefit from, operations research modeling and analysis techniques. It discusses the research efforts conducted at several universities, as well as within the Department of Homeland Security, that apply operations research methodologies to problems in passenger and baggage screening at security checkpoints. Five specific issues are highlighted: passenger and carry-on baggage screening, checked baggage screening, the identification of performance measures, the analysis of success rate, and the design of effective passenger and baggage screening systems. Additional information regarding operations research techniques applied specifically to passenger and baggage screening problems can be found in a survey published by Laura A. McLay and colleagues,[4] while operations research techniques applied to a variety of optimization problems within the Department of Homeland Security, including aviation, border, port, and cyber security, can be found in a survey published by P. Daniel Wright and colleagues.[5]

## PASSENGER AND CARRY-ON BAGGAGE SCREENING

There are two basic approaches to passenger screening: uniform screening and selective screening. From the introduction of passenger screening in the early 1970s until 1998, a uniform screening strategy was used, whereby all passengers were screened in the same manner. During this period, passengers

were screened by walk-through metal detectors, and their carry-on baggage was screened by X-ray machines. The main argument for the use of uniform screening is that all passengers may pose a threat and all should therefore receive an equal level of screening. In contrast, a selective screening strategy assigns additional security resources to screen a select few passengers perceived as being of higher risk. The main argument for the use of selective screening is that directing expensive, time-consuming security devices or procedures toward fewer passengers may be more cost effective since the vast majority of passengers do not actually pose a threat.

Passenger screening systems are designed to detect items that are a threat or passengers who are a threat. Through the use of X-ray machines, metal detectors, and trace portals, the passenger screening systems currently being used in the United States are focused on detecting and confiscating objects specified on an extensive prohibited item list managed by the TSA. Although this does not prevent terrorists from boarding airplanes, detecting threat items helps remove tools that can be used to stage an attack. The TSA has pursued the notion of detecting passengers who are a threat by coupling selective screening systems with a computer-based passenger prescreening system that performs a risk assessment of each passenger prior to that passenger's arrival at the airport. The method with which passengers are screened at the airport security checkpoints is then based on their assessed risk.

In 1998, a selective screening system, called the Computer-Assisted Passenger Prescreening System (CAPPS), developed by the Federal Aviation Administration (FAA), Northwest Airlines, and the U.S. Department of Justice, selected certain passengers for additional screening based on their perceived risk. CAPPS was designed to eradicate human bias in the risk assessment decision-making process. Those passengers who were cleared of being a security risk were labeled nonselectees, while those who could not be cleared of being a security risk were labeled selectees. Prior to September 11, the main difference between these two classes of passengers was that the checked bags selectees only were screened for explosives. Although the exact information used by CAPPS is classified, reports in the popular press indicate that it used information provided at the point of ticket purchase, including demographic and flight information, the frequent flyer status of the passenger, and the way the passenger purchased the ticket.

CAPPS was implemented in the selective security screening procedure in 1998, and was in use on September 11 for screening the 19 terrorists, of whom between 6 and 11 were designated as selectees.[6] However, in the procedure used on that day, only the checked baggage of selectees received a higher level of screening, not the passengers themselves, which effectively removed any value that CAPPS might have had in preventing or deterring the resulting attacks. After the events of September 11, aviation security moved in the direction of uniform screening, with the enactment into law of the 100 percent checked baggage screening mandate, eliminating the distinction between selectees and nonselectees.

The TSA revisited selective screening policies through the development of CAPPS II, a refinement of CAPPS. Barnett and Jonathon Caulkins[7] discussed in separate articles the risk involved with the implementation of CAPPS II. They both argued that this prescreening system lacked the proper analysis and tests that should have been carried out during development, and posed a serious risk if CAPPS II was viewed as the backbone of the passenger and baggage screening system. On July 14, 2004, however, the TSA announced that CAPPS II would not be implemented due to privacy concerns, despite having invested $100 million in its development.[8] Shortly thereafter, the TSA announced plans to replace CAPPS II with Secure Flight, a passenger prescreening system that incorporated FBI terrorist watch lists. Secure Flight was used in conjunction with an enhanced version of CAPPS, which effectively partitioned passengers into three risk classes: nonselectees, selectees, and an extremely small group of passengers who are not allowed to fly.

Areas of research have involved the notion of grouping passengers according to their perceived risk in terms of both a constant and a spectrum of threat probabilities. Vellara L. Lazar Babu investigate the benefit of classifying passengers into different groups, where each passenger risk is assumed to be known and identical for all passengers, and each passenger group undergoes a different degree of screening.[9] Babu and colleagues also develop a model that determines the number of screening classes, the devices associated with each class, and the fractions of passengers assigned to each security class.[10] Subject to an FAA specification constraining the false clear probability (the probability that a passenger who is a threat does not activate an alarm), the objective was to minimize the number of false alarms (i.e., the number of passengers who are not a threat but who activate an alarm). Babu and colleagues concluded that this type of passenger grouping was beneficial even when the passenger risk was assumed to be constant across all passengers.

A more complex approach to partitioning passengers involves multilevel passenger prescreening systems. Multilevel systems are those in which an arbitrary number of classes for screening passengers are considered, rather than the three classes (i.e., selectees, nonselectees, and those not allowed to fly) used today. A class involves a set of procedures using security devices for screening passengers. The nonselectee class, for example, may involve screening checked baggage with EDSs, passengers with X- ray machines, and carry-on baggage with metal detectors.

McLay and colleagues introduce multilevel passenger allocation problems which model the screening of passengers and carry-on baggage in a multilevel security system.[11] Each security class is defined by a set of procedures and screening devices, and each passenger is screened according to one of these security classes, according to his or her perceived risk level. In one passenger allocation model, the security classes are defined in terms of their fixed overhead costs, the marginal cost involved in screening each passenger, security level, and passenger capacity, while the passengers are assumed to demonstrate a spectrum of risk. The objective in optimizing this passenger

allocation model is to assign each passenger to a security class such that total security is maximized subject to security class occupancy and budget constraints. McLay and colleagues conclude that using as few as two security classes and utilizing passenger risk information may lead to more effective security screening strategies.[12] In a second passenger allocation problem, the security classes are defined only in terms of security level and passenger capacity. The objective in optimizing this second model is to assign passengers based on their perceived risk, such that the overall security level is maximized subject to security class capacity constraints. The resulting integer programming models offer systematic methods for solving challenging passenger assignment problems through the use of computer-based optimization software.

As in the models described, passenger risk can be determined by a computer-based prescreening system, such as CAPPS, but may only become available either when a passenger purchases his or her ticket or when he or she checks in. Jackrapong Attagara presents an explosive scanning device allocation model for multiple–airport security systems, with the focus on carry-on baggage screening.[13] The objective of this model is to assign both the type and number of devices to each passenger group in such a way that the total security is maximized subject to budget, resource, and throughput constraints. McLay considers the real-time operation of passenger screening systems by formulating a passenger assignment problem as a Markov decision process and shows how an optimal policy can be obtained using dynamic programming.[14]

Alexander G. Nikolaev and colleagues address an optimal device allocation and passenger assignment problem in which each passenger's risk level becomes available sequentially as each passenger checks in or at the time of ticket purchase.[15] Nikolaev and colleagues model the passenger and carry-on baggage screening operations in two stages, where in the first stage security devices are purchased and installed under budget and space constraints, while in the second stage the sequential passenger security class assignments are determined. The objective is to maximize the total security level over all passenger assignments for a fixed time period, given that each passenger's risk level is unknown until he or she checks in, and subject to security device capacity constraints.

Another aspect of passenger and carry-on baggage screening systems is the deployment of screening devices within airports. Julie Virta and colleagues determine where to deploy certain security devices based on the outgoing selectee rate at an airport (i.e., the fraction of originating and transferring passengers at an airport that have not been cleared by CAPPS) and the corresponding impact of transferring selectees at airports.[16] Virta and colleagues conclude that this method of maintaining the outgoing selectee rate can be used to determine which airports pose the greatest threat from selectee passengers, and how to deploy security screening devices at these airports.

## CHECKED BAGGAGE SCREENING

As with passenger and carry-on baggage screening, checked baggage screening is a critical component of the overall aviation security system. Checked baggage is screened by TSA-certified explosion detection systems (EDSs) for threat objects such as explosives and may be selected for closer inspection by either hand search or by bomb-sniffing dogs. Prior to September 11, 2001, only checked baggage for passengers marked as selectees was screened by EDSs. However, these attacks triggered a politically driven response as the U.S. Congress quickly enacted the Aviation and Transportation Security Act (ATSA), which required the TSA to acquire and deploy TSA-certified EDSs to screen 100 percent of checked baggage no later than December 31, 2002. The projected purchase and deployment cost for over 2,500 EDS devices necessary to screen all checked baggage exceeded $2.5 billion and significantly increased labor costs for federally employed screeners, (note that as of mid-2007, between 1,500 and 2,000 EDSs are deployed at commercial airports).[17] The decision to screen all checked baggage was made without the appropriate cost/benefit analysis necessary to ensure that a manageable operation may be maintained within budget restrictions while also increasing the overall security of the aviation security system.

Systems engineering has been used to solve the problem of screening all passengers and luggage while maintaining efficient airport operations. Sean Donovan and colleagues analyze the 100 percent baggage screening problem by applying the Systems Engineering Management Process (SEMP), consisting of four phases: problem definition, design and analysis, decision making, and implementation.[18] However, cost analysis for screening strategies that better utilize baggage screening devices has proven more effective for allocating limited funding.

Cost/benefit analyses of different baggage screening strategies provide a method of assessing and comparing the value of such approaches. Virta and colleagues perform an economic analysis capturing the trade-offs of using explosive detection systems (EDSs) to screen only selectee baggage versus screening both selectee and nonselectee baggage (i.e., the 100 percent baggage screening mandate).[19] They conclude that the marginal increase in security per dollar spent is significantly lower for the 100 percent baggage screening mandate than when only selectee bags are screened. Sheldon H. Jacobson and colleagues incorporate deterrence into this model (one of the indirect benefits of screening both selectee and nonselectee baggage), based on a remark by the inspector general of the U.S. Department of Transportation, and conclude that the cost effectiveness of the 100 percent baggage screening mandate depends on the degree to which it can reduce the underlying threat level.[20]

Jacobson and colleagues evaluate the cost effectiveness of explosive detection technologies in both single-device and two-device systems.[21] A single-device system signals an alarm if the device signals an alarm, whereas a two-device system could signal an alarm either if both devices agree on signaling an alarm or if either device signals an alarm. Device costs and device alarm

probabilities are utilized to investigate the trade-offs between the single- and two-device strategies. Jacobson and colleagues conclude that single-device systems are less costly and have fewer expected numbers of false alarms than the two-device systems, mainly due to the way the second device in a two-device system affects the alarm or clear decision.[22] These cost models provide effective tools for the execution of cost/benefit analyses of alternative device configurations for checked baggage security screening.

In addition to the direct costs associated with the purchase, operation, and maintenance of baggage screening devices, there are also indirect costs associated with the device alarm errors. For example, cost increases occur when a passenger must be rescreened after a false alarm occurs, particularly if this rescreening entails the use of higher-level, more labor-intensive screening devices. Thomas J. Candalino, Jr., and colleagues[23] provide an extension to the cost/benefit analysis reported by Virta and colleagues by introducing a cost function that includes not only direct costs but also the indirect costs associated with device alarm errors.[24] They present an optimization-based tool using simulated annealing to identify lower system cost configurations for the design of efficient and effective aviation security systems.

Cost models may also include the effects of deterrence within checked baggage screening strategies. Jacobson and colleagues present the effects of deterrence on the level of threat at an airport.[25] As the threat level changes, the TSA alters the configurations for explosive detection systems deployed at airports, thereby changing the rate of screening device alarms. A comparison between the expected direct cost per expected prevented attack and the expected cost of an aviation terrorist incident provides a measure of the cost effectiveness of the 100 percent checked baggage screening policy.

The TSA realized that it was not possible for manufacturers to produce the required number of EDS machines to screen 100 percent of checked baggage by December 31, 2002, and called for the relaxation of this requirement by using a combination of EDS and explosive trace detection (ETD) machines. Viggo Butler and Robert W. Poole, Jr. argue that ETD is a flawed technology due to its error rate of false positives at nearly 30 percent with a low throughput rate of 150–200 bags per hour.[26] Furthermore, ETD machines are even slower and more labor intensive and require more total space than EDS machines. They propose that the TSA approve a shift to a multitiered baggage inspection system and extend the deadline for 100 percent checked baggage screening to allow multibillion dollar investments to be made in improved, newer technologies. They also suggest that the focus of baggage inspection should shift from detecting threat objects within baggage to identifying high-risk passengers, while matching inspection technologies to each security risk level.

## IDENTIFICATION OF PERFORMANCE MEASURES

Considering the number of aviation security changes that have been implemented since September 11, 2001, and the fierce political and public debate

surrounding these changes, it is necessary to provide a measurement that defines how well an aviation security system performs. Identifying performance measures is not only important for the long-term planning of security systems but also for efficiently managing day-to-day operations and effectively managing security systems in transition. Performance measures can be incorporated into various types of operations research passenger screening problems, including applications in discrete optimization models, applied probability models, cost/benefit analyses, and risk assessments.

One obvious and appropriate measure of aviation security system performance is the probability that a threat may occur. Jacobson and colleagues present a nonintrusive sampling procedure to estimate the threat probability, defined as the probability that the system signals a clear for a passenger who is a threat.[27] This threat probability is based on the observed number of alarms and clears that occur during day-to-day operations, and is dependent on the device and procedure settings designated by the level of threat believed to be present in the environment. Jacobson and colleagues also develop performance measures for baggage screening security devices; these include uncovered flight segment (i.e., the number of flights containing at least one selectee bag that has not been screened by a baggage screening device) and uncovered passenger segment (i.e., the number of passengers on uncovered flights) measures.[28] However, the optimization models associated with these performance measures do not permit partial screening of flights. Instead, Jacobson and colleagues develop a performance measure in which each selectee bag is assigned an individual value based on the proportion of the flight segment that the bag covers.[29] Likewise, a passenger segment baggage value assigns a value to each selectee bag based on the proportion of the passenger segments that the bag covers. Each of these performance measures is analyzed using an integer programming model, as a result of which optimization techniques measure the relationships between the baggage value measures and other baggage screening security system measures.

Discrete optimization models have also been used to address the effectiveness of aviation security systems. Jacobson and colleagues develop discrete optimization models based on three performance measures that quantify the effectiveness of airport baggage screening security device systems subject to a finite amount of security resources, including both uncovered flight segments and uncovered passenger segments.[30] The models are used to provide the optimal baggage screening device deployments considering the number of passengers on a set of flights whose baggage is subjected to screening, the number of flights in this set, and the size of aircraft within this set of flights. Through examples using data extracted from the Official Airline Guide,[31] Jacobson and colleagues show how the allocations based on the uncovered flight segment measure provide reasonable solutions with respect to the uncovered passenger segment measure.[32] The reverse, however, may not be true, suggesting that the uncovered flight segment measure may provide more robust baggage screening device allocations.

Susan E. Martonosi and Arnold Barnett explore the issue of the antiterrorist effectiveness of airport passenger prescreening systems using a probabilistic analysis.[33] They propose that if terrorists probe the system to better understand their perceived risk, then their act of probing could actually deter attacks that would normally have succeeded. In addition, they demonstrate that improving the base level of screening for all passengers lowers the possibility of a terrorist attack more than improving the automated prescreening system for better profiling of high-risk passengers.

Airports generate revenue from the facilities they provide. Therefore, facility management plays a significant role in defining feasible ways to achieve a satisfactory level of security system performance. Vojin Tosic[34] presents a review of research results in the area of airport passenger terminal operations analysis and modeling, based on information available in the public domain. The scope of this review includes, but is not limited to, terminal configuration, available service space, gate utilization, and the operation of waiting areas and baggage processing facilities. Aghahowa Enoma and Stephen Allen[35] outline the findings from a research project seeking to develop and test a set of key performance indicators for airport facility management, with a particular focus on safety and security. Enoma and Allen also offer a list of such indicators that emerged from their interviews and workshops.

Kwang E. Yoo and Youn C. Cho study the relative importance of the means to improve passenger security at an airport.[36] Three major factors that impact the effectiveness of passenger screening were investigated: human resources, equipment and facilities, procedures, and responsibility structures. The authors performed a hierarchy process analysis of surveyed data to gauge the relative importance of these elements of an aviation security system, with the aim of improving passenger screening. The results suggest that the crucial factor needing improvement to enhance the effectiveness of passenger screening operations is human resources.

Since September 11, 2001, much of the interest in passenger screening systems has been limited to reducing the false clear rate—the conditional probability that there is no alarm response for a passenger or bag containing a threat object. To improve passenger throughput requires a reduction in the false alarm rate—the conditional probability that there is an alarm response for a passenger or bag that does not contain a threat object. However, the false clear and false alarm rates cannot be simultaneously minimized.[37] For example, if all passengers were allowed to board their flights with no screening, the false alarm rate would be 0 percent while the false clear rate would be 100 percent.

Since the vast majority of passengers are not threats, most alarms are in fact false alarms. A system with a low false clear rate may have a large false alarm rate, which can be very expensive, since there must be secondary screening procedures in place to resolve such alarms. In rare cases, bomb squads must be called in to inspect a suspicious bag, or an airport terminal must be shut down for several hours, resulting in millions of dollars in losses to the airlines due to a single false alarm incident.

Other performance measures deal with passenger screening systems in transition. When CAPPS was used to determine which checked baggage was screened for explosives between 1998 and 2001, there were not enough baggage screening devices available in many of the nation's airports to screen all selectee bags for explosives. This partial baggage screening problem was not removed by the 100 percent baggage screening mandate following September 11. Instead, this scenario is repeated when a new screening technology has been partially deployed and is used under a selective screening system and, because of limited capacity, not all passenger selectees can be screened by the new technology. Performance measures focus on the types of risk that can be reduced by a single screening technology or a series of screening devices working together in a system. There may be other types of risks on a flight that are not considered by these performance measures, and hence, additional performance measures must be defined.

Full utilization of baggage screening devices is one possible performance measure for the partial baggage screening problem. Intuitively, it is equally desirable to screen additional checked bags, in such a way that the new screening devices are being used up to their capacity. Jacobson and colleagues introduce two alternate performance measures that capture risk across a set of flights and incorporate these measures into discrete optimization models.[38] The measures are considered for a set of flights carrying both selectee and nonselectee baggage. A flight is said to be *covered* if all the selectee bags on it have been screened and cleared. One measure considers the total number of covered flights. Optimizing over the baseline minimizes the number of flights that may be subject to a particular risk. Another measure considers the total number of passengers on covered flights. Optimizing over this measure minimizes the total number of passengers on flights that may be subject to a particular risk. Note that optimizing over these measures indirectly maximizes the utilization of the baggage screening devices, though, depending on which measure is chosen, the security of the system can be determined to be optimal in two distinct ways, putting either fewer flights at risk or fewer passengers at risk.

## ANALYZING THE SUCCESS RATE OF PASSENGER AND BAGGAGE SCREENING SYSTEMS

Aviation security professionals have expressed concern over the actual effectiveness of selective screening systems like Secure Flight in preventing attacks, given the variety of ways in which such systems can fail. Three research efforts are highlighted to illustrate how operations research tools such as risk analysis, algorithm design, and applied probability can be used to analyze flaws in selective screening systems.

Access control security system architectures involve the process of screening objects such as passengers and baggage entering a secure area within the airport, and are designed to detect and prevent the entry of threats such

as firearms and explosives. Probability models may be used to analyze the success rate of passenger and baggage screening systems by quantifying the probabilities that a threat is or is not detected, given that a threat exists in the passenger population. John E. Kobza and Sheldon H. Jacobson, present probability models based on Type I errors, the probability that a false alarm is given, and Type II errors, the probability that a threat is not detected.[39] Controlled sampling is utilized, where objects may take paths through different sets of screening devices in the system. Kobza and Jacobson show that for specific threat levels, multiple-device systems can be designed that outperform single-device systems in certain types of error probability measurements. Furthermore, dependence between device responses in multiple-device systems may be incorporated, where the dependency structure quantifies how various technologies interact and provides a measure for the impact of device dependence on the Type I and Type II error probabilities. The security systems may then be evaluated to identify the optimal use of security devices and to determine the systems that are the most cost effective. Probability models with device dependence may also be used to determine whether new technologies provide improvements to security, thereby warranting investment.

The design of multiple-device systems is challenging with respect to the false alarm, false clear trade-off. For a given security system and a maximum false clear standard specified by the TSA, there is a minimal false alarm rate that can be achieved. Jacobson and colleagues develop a methodology for determining the false alarm rate by estimating the joint conditional probability density functions for the security device responses.[40] Dynamic programming algorithms are used to address this trade-off problem.

Probability models may also be used to investigate the performance of security screening procedures. Uwe Glässer and colleagues propose a computational approach to checking the consistency, coherence, and completeness of procedural security requirements defined by the FAA security guidelines.[41] Their probability models are used to handle the uncertainty in the security procedure behavior, and combine abstract state machine modeling of the airport security process flow with symbolic model checking, to analyze model parameter variation and to check the consistency and completeness of the model. This type of systematic modeling and performance analysis approach can be refined to handle the complex procedural requirements defined by the security guidelines.

The Federal Aviation Administration conducted an assessment of airport vulnerability and risk in 1999 as a direct result of recommendation 3.13 of the White House Commission on Aviation Safety and Security.[42] The Airport Vulnerability Assessment Project (AVAP) was initiated to assess the security vulnerability and risk of U.S. commercial airports through a combination of automation, analytical methods, and tools. Richard T. Lazarick presents results from field tests of seven methodologies applied to 13 U.S. domestic airports and the evaluation of these tests through several different weighting schemes for a computation of the overall desirability value of each methodology.[43]

Lazarick concludes from the resulting analysis that the airport vulnerability assessments generated trends in terms of commonly identified security upgrades.

John D. Veatch and colleagues present a vulnerability assessment methodology that incorporates procedural tools that were developed and refined from the application to over 100 airport facilities over a 20-year period.[44] They use this methodology to conduct an assessment of two major U.S. domestic airports and consider the threat, target identification, adversary types, malevolent acts of concern, and consequences of an adversary success. They also develop algorithms to analyze the potential consequences and security vulnerability levels, to obtain a relative risk for each threat and target combination, and introduce countermeasures to minimize the risk of each type of threat, which includes an iterative process to search for the most cost-effective method of reducing risk to an acceptable level.

A weakness of any selective screening system is that it may be possible to test and probe the system to find weakness through extensive trial-and-error sampling. At present, passengers are aware of whether they have been classified as selectees or nonselectees each time they travel (most notably, by an indicator on their boarding pass, as well as by the additional screening attention they receive at the security checkpoint). Terrorists can exploit this information to determine how they are most likely to be classified as nonselectees, by flying on a number of flights and effectively sampling the characteristics that result in a nonselectee classification. Therefore, terrorists do not need to understand how the prescreening system works; they merely need to be able to manipulate the prescreening system to get the desired result (i.e., be classified as nonselectees). Samidh Chakrabarti and Aaron Strauss present this strategy as the "Carnival Booth" algorithm, which demonstrates through a probability analysis how a system using prescreening may be less secure than systems that employ random searches.[45]

Another weakness of any selective screening system is its dependence on passenger information to accurately assess passenger risk. The specific details underlying the currently used selective screening system are classified. Moreover, it is not clear how such a system will correctly identify terrorists as selectees when compared to random screening. It is also a challenge to accurately assess whether a selective screening system has been effective, since terrorist attacks are rare events, and the way terrorists behaved in the past may not be predictive of the way terrorists will behave in the future.

Barnett uses risk analysis, applied probability, and data mining to analyze these issues regarding prescreening systems.[46] He concludes that using a prescreening system such as Secure Flight may improve aviation security under a particular set of circumstances, namely, if it does not reduce the screening intensity for nonselectee passengers, if it increases the screening intensity for selectees, and if the fraction of passengers identified as selectees does not decrease. For all these reasons, Barnett recommends that Secure Flight be transitioned from a security centerpiece to one of many components in future aviation security systems.

Barnett and colleagues report the results of a large-scale experiment at several commercial airports in the United States to estimate the costs and disruptions associated with a positive passenger baggage matching policy (PPBM).[47] Under PPBM, unaccompanied checked baggage is removed from aircraft on originating flights. PPBM can be applied to all or a portion of checked baggage. Barnett and colleagues' findings counter predictions by the airlines that using PPBM would be expensive and result in widespread delays when used on all checked baggage. They found that on average, one in seven flights experienced a delay, with each such delay averaging approximately seven minutes.

On January 20, 2006, the TSA announced key elements of the Registered Traveler (RT) program, to be used in conjunction with Secure Flight and CAPPS.[48] The program is designed to provide special security screening lanes for passengers enrolled in the Registered Traveler program, in which such passengers must pass a voluntary background check and submit biometric information for identity verification when traveling. Once they are part of the program, these passengers undergo expedited screening in designated security lanes. Barnett outlines several potential problems with such a program, and suggests that in the worst-case scenario, the Registered Traveler program improves screening efficiency without improving the ability to positively identify terrorists.[49] The Registered Traveler pilot program is currently being tested at commercial airports throughout the United States.

These weaknesses of selective screening systems raise the question of whether to spend security dollars on improving intelligence or on building more effective screening technologies. McLay and colleagues explore this issue by performing a cost/benefit analysis using concepts from applied probability and optimization.[50] In their analysis, more effective (though more expensive) screening technologies are considered for screening selectee baggage, given a range of accuracy levels for a prescreening system in assessing passenger risk. Several selective screening scenarios are identified that are preferable to screening all passenger baggage with explosive detection systems (EDSs), as these scenarios reduce the number of successful attacks with moderate cost increases. The authors conclude that the accuracy of the prescreening system is more critical for reducing the number of successful attacks than the effectiveness of the baggage screening devices used to screen selectee baggage when the proportion of the passengers classified as selectees is small.

## DESIGNING EFFECTIVE PASSENGER AND BAGGAGE SCREENING SYSTEMS

Prohibitive costs, long security lines, and questionable effectiveness in preventing attacks have impeded passenger screening initiatives. Significant infrastructure changes have been made at several airports to accommodate new screening devices, and passengers have been subjected to long lines in airport lobbies awaiting screening. Passenger screening system designs must consider

the potential impact of cost, space, throughput, and effectiveness. Three research efforts using operations research methodologies to design selective screening systems are highlighted.

Robert W. Poole, Jr. argues that the TSA's current approach to aviation security was poorly thought out and fundamentally flawed.[51] The lack of proper cost/benefit analysis and analysis of relative risks wastes passengers' time and improperly consumes large amounts of funding that could be allocated to improving security in other ways. Poole proposes that the current model is flawed in three basic ways. First, the TSA assumes that all passengers are equally likely to be a threat and mandates equal attention to each passenger. Second, the TSA operates in a centralized manner, which is a poor match for various sizes and types of passenger airports. Third, by law, the TSA is placed in the conflicting position of being both the airport security policymaker and also the provider of some airport security services. Poole calls for a reform of the current approach by removing the conflict of interest in the TSA, through phasing out their role in providing airport security services, allowing screening functions to be carried out by each individual airport under TSA oversight, and to screen passengers according to risk-based strategies, thereby targeting resources on dangerous people rather than dangerous objects. These changes call for a new aviation passenger and baggage screening model, designed through a proper cost/benefit analysis, that would become cost effective while also increasing the overall security level.

The Department of Homeland Security (DHS has acknowledged the use of modeling and simulation in providing improvements to aviation security and the deployment of advanced airport security equipment.[52] The DHS agrees that modeling and simulation has become an effective way to target new technology advancements and to evaluate the behavior of complex operational systems. The nature of simulation provides the opportunity to examine the complexities of the airport environment in a nonintrusive and cost-effective way, by examining various configurations and other operational factors of screening devices without actually installing expensive security equipment and performing field tests on it or disrupting passenger and baggage flow.[53] The DHS agrees that the direct result of implementing these tools of analysis tools yield more effective and efficient airport security solutions.

In addition to models of the aviation security system, models can also be developed to analyze terrorist behavior. Yacov Y. Haimes offers a risk assessment and management framework for modeling the risks of terrorism.[54] Models are developed for aviation security systems and terrorist network systems, as well as their interconnections. Haimes paints a roadmap for building risk analysis and system-based methodologies to avoid repeating an ad hoc approach to security system design. It is not clear how effective measurements such as armed guards at terminals and sky marshals (imposed following September 11, 2001) are at deterring or detecting terrorist actions. Leticia J. Pacheco and colleagues argue the need for a more sophisticated technology, operating procedures, and intelligence specifically to detect and deter the weapons,

bombs, and other threat items that terrorists try to use on board airlines.[55] They provide a mathematical tool for modeling the human element of terrorist behavior while incorporating current detection capability, to provide a management tool for allocating resources to the areas that require the highest level of deterrence.

Laura Dugan and colleagues introduce a model of airline hijackings by examining trends in 1,101 attempted aerial terrorist attacks that occurred around the world from 1931 to 2003.[56] They use continuous-time survival analysis to estimate the impact of several major hijacking interventions on the threat of differently motivated hijacking attempts and they use logistic regression analysis to model the predictors of successful hijackings. They also assess which strategies have been most effective in deterring terrorists.

The United States Commercial Aviation Partnership (USCAP), a group of government and industry stakeholders, combine several operations research methods in an analytical process and model that encompasses the U.S.'s commercial aviation industry, including travelers, airlines, airports, airline and airport suppliers, government agencies, and travel and tourism entities.[57] The model helps evaluate the operational economic effects of proposed security measures and provides an understanding of these effects to assist government decisions in regard to the trade-off between the improvement of security and the economic impact. The model uses linear and nonlinear programming, single and multivariate regression, system dynamics, econometrics, and Monte Carlo simulation to estimate the policy impact on screening airport employees, passengers, and cargo, determining security staffing levels, and charging security fees.

One way to improve selective screening systems is to use expensive baggage screening technologies with low throughput to screen passengers perceived as higher risk. This has the potential to be a more cost-effective approach to screening passengers, primarily by increasing throughput. Butler and Poole describe a layered approach to screening passengers and baggage, instead of the existing TSA policy of 100 percent checked baggage screening using EDSs, by considering the economic impact of using different screening technologies.[58] They consider three groups of passengers: lower-risk passengers who have volunteered for extensive background checks, lower-risk passengers about whom little is known, and higher-risk passengers. They recommend screening baggage with three layers of baggage screening devices. Weaving passengers through three layers of security devices composed of EDSs, high-throughput backscatter and dual-energy X-ray devices, and hand searches increases throughput while the overall false clear rate remains at a level comparable to that of the 100 percent baggage screening mandate; Butler and Poole make similar recommendations for passenger screening. One implication of this screening system is that the resulting improved throughput indirectly decreases space requirements and waiting times in airport lobbies, which is of interest because many airport lobbies were not designed to accommodate extensive screening systems and excessively long waiting lines.

Laura A. McLay describes two multilevel passenger screening problems (formulated as discrete optimization models) that provide insights into how screening devices should be purchased and deployed.[59] An analysis of a greedy heuristic for one of these problems suggests that using only two classes is particularly effective, supporting the two-class paradigm of Secure Flight. For this problem, each of the classes is defined in terms of its fixed cost (the overhead costs), its marginal cost (the additional cost of screening a passenger), and its false clear rate, with a passenger prescreening system such as Secure Flight used to differentiate passengers. The objective is to minimize the overall false clear rate subject to passenger assignments and budget constraints. The second problem, complementary to the first, considers screening devices that have been purchased and installed. The second problem illustrates how devices shared by multiple classes can be used, where each class is defined by the device types it uses and each device type has an associated capacity (throughput) in a given unit of time. Optimal solutions for examples with more available classes are more sensitive with respect to changes in passenger volume and device capacity. This research suggests that incorporating prescreening systems into discrete optimization models provides insight into efficient selective screening systems.

## CONCLUSIONS

Operations research provides the opportunity to make a difference in aviation security by exploring new directions that need not merely be makeshift political solutions to complex problems. Instead, they can be the result of careful modeling, rigorous analysis, and detailed planning. By illustrating several ways in which operations research has made an impact on passenger and baggage screening systems, we have shown that it has a place in the design and analysis of aviation security systems. However, operations research modeling (or in fact, mathematical modeling of any type) always has its limitations. For example, one must often make certain assumptions that may limit the applicability of the results obtained. Though such assumptions are often based on reasonable and realistic factors, they may pose difficulties in facilitating the transfer of the operations research analysis to decision makers, since errors can lead to security breakdowns that may place passengers at unnecessary risk. In addition, operations research models quite often consider a measurement of the average or mean performance. In aviation security systems, average performance does not always capture the most interesting and salient aspects of such operations, which are often concerned with rare events such as those connected with terrorist activities.

The applications of operations research can also extend beyond the realm of passenger and baggage security screening. Other problems in aviation security can benefit from operations research methodologies, including improving perimeter access security with respect to airport employees, designing models for cargo screening, analyzing passenger throughput and the space

associated with security lines, and modeling secondary screening of passengers and their baggage when screening devices give an alarm response. In addition, operation research methodologies may be applied to problems in rail and mass public transportation systems, where the potential for terrorist attacks against large populations have been made all too clear by the Madrid train bombing on March 11, 2004, and the London subway bombing on July 7, 2005. Through the use of operations research methodologies to analyze and gain insight into improvements in aviation security system operations and performance, travelers may begin to regain trust in our nation's security and well-being.

## NOTES

This research has been supported by the by the National Science Foundation under Grant No. DMI-0114499 and the Air Force Office of Scientific Research under Grant No. FA9550–07–1–0232. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government, the Department of Homeland Security, the National Science Foundation, and the Air Force Office of Scientific Research.

1. Arnold Barnett, "The Worst Day Ever," *OR/MS Today* 28, no. 6 (2001): 28–31.

2. Arnold Barnett, "Trust No One at the Airport," *OR/MS Today* 30, no. 1 (2003): 72.

3. U.S. Government Accountability Office, *Progress since September 11, 2001, and the Challenges Ahead*, Tech. Rep. (GAO-03–1150T) (Washington, DC: GPO, 2003).

4. L.A. McLay, S. H. Jacobson, and J. E. Kobza, "Making Skies Safer," *OR/MS Today* 32, no. 5 (2005).

5. P. D. Wright, M. J. Liberatore, and R. L. Nydick, "A Survey of Operations Research Models and Applications in Homeland Security," *Interfaces* 36, no. 6 (2006): 514–29.

6. Arnold Barnett, "CAPPS II: The Foundation of Aviation Security?" *Risk Analysis* 24 (2004): 909–16.

7. Barnett, "CAPPS II"; Jonathan P. Caulkins, "CAPPS II: A Risky Choice Concerning an Untested Risk Detection Technology," *Risk Analysis* 24, no. 4 (2004): 921–24.

8. M. Hall, and B. DeLollis, "Plan to Collect Flier Data Canceled," *USA Today*, July 14, 2004, 1.

9. V.L.L. Babu, R. Batta, and L. Lin, "Passenger Grouping under Constant Threat Probability in an Airport Security System," *European Journal of Operational Research* 168 (2004): 633–44.

10. Babu, et al., "Passenger Grouping under Constant Threat," 633–44.

11. L. A. McLay, S. H. Jacobson, and J. E. Kobza, "A Multilevel Passenger Screening Problem for Aviation Security," *Naval Research Logistics* 53, no. 3 (2006): 183–97; L. A. McLay, S. H. Jacobson, and J. E. Kobza, "Integer Programming Models and Analysis for a Multilevel Passenger Screening Problem," *IIE Transactions* 39, no. 1 (2007): 73–81.

12. Mc Lay, Jacobson, and Kobza, "Integer Programming Models."

13. Jackrapong Attagara, "The Explosive Scanning Devices Allocation Problem for Airport Security Systems" (PhD diss., Texas Tech University, 2006).

14. Laura A. McLay, "Designing Aviation Security Systems: Theory and Practice" (PhD diss., University of Illinois at Urbana-Champaign, 2006).

15. A. G. Nikolaev, S. H. Jacobson, and L. A. McLay, "A Sequential Stochastic Security System Design Problem for Aviation Security," *Transportation Science* 41, no. 2 (2007): 182–94.

16. J. E. Virta, S. H. Jacobson, and J. E. Kobza, "Outgoing Selectee Rates at Hub Airports," *Reliability Engineering and System Safety* 76, no. 2 (2002): 155–65.

17. U.S. Government Accountability Office, *Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations*, Tech. Rep. (GAO-04–440T) (Washington, DC: GPO, 2004); U.S. Government Accountability Office, *Progress since September 11, 2001, and the Challenges Ahead.*

18. S. T. Donovan et al., "A Systems Approach to John Wayne Airport Security," in *Proceedings of the 2003 IEEE Systems and Information Engineering Design Symposium* (Chicago: IEEE, 2003), 221–24.

19. J. E. Virta, S. H. Jacobson ,and J. E. Kobza, "Analyzing the Cost of Screening Selectee and Non-Selectee Baggage," *Risk Analysis* 23, no. 5 (2003): 897–908.

20. S. H. Jacobson, T. Karnani, and J. E. Kobza, "Assessing the Impact of Deterrence on Aviation Checked Baggage Screening Strategies," *International Journal of Risk Assessment and Management* 5, no. 1 (2005): 1–15.

21. S. H. Jacobson et al.,, "A Cost-Benefit Analysis of Alternative Device Configurations for Aviation Checked Baggage Security Screening," *Risk Analysis* 26, no. 2 (2006): 297–310.

22. Jacobson, Karnani, and Kobza, "Assessing the Impact of Deterrence on Aviation Checked Baggage Screening Strategies."

23. T. J. Candalino, J. E. Kobza, and S. H. Jacobson, "Designing Optimal Aviation Baggage Screening Systems Using Simulated Annealing," *Computers and Operations Research* 31, no. 10 (2004): 1753–67.

24. Virta, Jacobson, and Kobza, "Analyzing the Cost of Screening Selectee and Non-Selectee Baggage."

25. S. H. Jacobson et al., "Modeling and Analyzing Multiple Station Baggage Screening Security System Performance," *Naval Research Logistics* 52, no. 1 (2005): 30–45.

26. V. Butler and R. W. Poole, Jr., *Rethinking Checked-Baggage Screening*, Reason Public Policy Institute, Los Angeles, California, Policy Study No. 297, 2002, http://www.rppi.org.

27. S. H. Jacobson, J. E. Kobza, and M. K. Nakayama, "A Sampling Procedure to Estimate Risk Probabilities in Access Control Security Systems," *European Journal on Operational Research* 122, no. 1 (2000): 123–32.

28. S. H. Jacobson, J. M. Bowman, and J. E. Kobza, "Modeling and Analyzing the Performance of Aviation Security Systems Using Baggage Value Performance Measures," *IMA Journal of Management Mathematics* 12, no. 1 (2001): 3–22.

29. Jacobson, et al., "Modeling and Analyzing," 3–22.

30. S. H. Jacobson et al., "Modeling Aviation Baggage Screening Security Systems: A Case Study," *IIE Transactions* 35, no. 3 (2003): 259–69; S. H. Jacobson et al., "Integer Program Models for the Deployment of Airport Baggage Screening Security Devices," *Optimization and Engineering* 6, no. 3 (2005): 339–59.

31. *OAG Business Travel Planner*, Official Airline Guides (Bedfordshire, England: OAG, 1998).

32. Jacobson et al., "Modeling Aviation Baggage Screening Security Systems: A Case Study"; Jacobson et al., "Integer Program Models for the Deployment of Airport Baggage Screening Security Devices."

33. S. E. Martonosi, and A. Barnett, "How Effective Is Security Screening of Airline Passengers?" *Interfaces* 36, no. 6 (2006): 545–52.

34. Vojin Tosic, "A Review of Airport Passenger Terminal Operations Analysis and Modeling," *Transportation Research* 26A, no. 1 (1992): 3–26.

35. A. Enoma and S. Allen, "Developing Key Performance Indicators for Airport Safety and Security," *Facilities* 25, no. 7–8 (2007): 296–315.

36. K. E. Yoo and Y. C. Choi, "Analytic Hierarchy Process Approach for Identifying Relative Performance of Factors to Improve Passenger Security Checks at Airports," *Journal of Air Transport Management* 12, no. 12 (2006): 135–42.

37. J. E. Kobza, and S. H. Jacobson, "Probability Models for Access Security System Architectures," *Journal of the Operational Research Society* 48, no. 3 (1997): 255–63.

38. Jacobson et al., "Modeling Aviation Baggage Screening Security Systems: A Case Study."

39. J. E. Kobza and S. H. Jacobson, "Addressing the Dependency Problem in Access Security System Architecture Design," *Risk Analysis* 16, no. 6 (1996): 801–12; Kobza and Jacobson "Probability Models for Access Security System Architectures."

40. S. H. Jacobson, J. E. Kobza and A. E. Easterling, "A Detection Theoretic Approach to Modeling Aviation Security Problems using the Knapsack Problem," *IIE Transactions* 33, no. 9 (2001): 747–59.

41. U. Glässer, S. Rastkar, and M. Vajihollahi, "Computational Modeling and Experimental Validation of Aviation Security Procedures," *Lecture Notes in Computer Science* 3975 (2006): 420–31.

42. White House Commission on Aviation Safety and Security, *The DOT Status Report*, 1998, http://www.dot.gov/affairs/whcoasas.htm.

43. Richard T. Lazarick, "Airport Vulnerability Assessment—A Methodology Evaluation," in *IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology* (Chicago: IEEE, 1999), 120–33; Richard T. Lazarick, "Airport Vulnerability Assessment—An Analytical Approach," in *Proceedings of SPIE* 3575 (1999): 302–10.

44. J. D. Veatch, "Airport Vulnerability Assessment Methodology," in *IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology* (Chicago: IEEE, 1999), 134–51.

45. S. Chakrabarti and A. Strauss, "Carnival Booth: An Algorithm for Defeating the Computer-Aided Passenger Screening System," *First Monday* 7, no. 10 (2002), http://www.firstmonday.org.

46. Barnett, "CAPPS II: The Foundation of Aviation Security?"

47. A. Barnett et al., "Safe at Home? An Experiment in Domestic Airline Security," *Operations Research* 49 (2001): 181–95.

48. Transportation Security Administration, U.S. Department of Homeland Security, "TSA Announces Key Elements of Registered Traveler Program," press release, January 20, 2006, http://www.tsa.gov/press/releases/2006/press_release_0645.shtm.

49. Barnett, "Trust No One at the Airport."

50. L. A. McLay, S. H. Jacobson, and J. E. Kobza, *When Is Selective Screening Effective for Aviation Security?* Technical Report (Urbana, IL, University of Illinois, 2005).

51. Robert W. Poole Jr., *Airport Security: Time for a New Model*, Reason Public Policy Institute, Los Angeles, California, Policy Study No. 340, 2006, http://www.rppi.org.

52. Diane L. Wilson, "Use of Modeling and Simulation to Support Airport Security," *IEEE Aerospace and Electronic Systems Magazine* 20, no. 8 (2005): 3–6.

53. D. L. Wilson, E. K. Roe, and S. A. So, "Security Checkpoint Optimizer (SCO): An Application for Simulating the Operations of Airport Security Checkpoints," in *Proceedings of the 2006 Winter Simulation Conference* (Piscataway, NJ: IEEE, 2006).

54. Y, Yacov Haimes, "Roadmap for Modeling Risks of Terrorism to the Homeland," *Journal of Infrastructure Systems* 8, no. 2 (2002): 35–41.

55. L. J. Pacheco, J. E. Kobza, and S. H. Jacobson, "Modeling and Analyzing Terrorist Behavior within the Aviation Security Environment," in *IIE Annual 2004 Conference and Exhibition* (Washington, DC: IIE, 2004), 373.

56. L. Dugan, G. Lafree, and A. R. Piquero, "Testing a Rational Choice Model of Airline Hijackings," *Criminology* 43, no. 4 (2005): 1031–65.

57. R. M. Peterson et al., "Using USCAP's Analytical Models, the Transportation Security Administration Balances the Impacts of Aviation Security Policies on Passengers and Airlines," *Interfaces* 37, no. 1 (2007): 52–67.

58. Butler and Poole, "Rethinking Checked-Baggage Screening."

59. McLay, Jacobson, and Kobza, "A Multilevel Passenger Screening Problem for Aviation Security."

# CHAPTER 9

# Air Cargo Security

*Erik Hoffer*

The value of the air cargo industry is estimated to be about $60 billion, not including the value of related industries such as packaging-material suppliers, insurance carriers, and providers of ancillary administrative functions. The industry outside of direct shippers is comprised of domestic passenger air carriers, dedicated air couriers, private air freight airlines, forwarders, brokers, and consolidators—just a few of the categories that comprise the air matrix. One severe incident could have a devastating affect on world commerce and effectively shut down commerce as we know it. The 2003 port strike in California cost the commercial supply chain billions in losses daily and crippled sea imports worldwide for six months.

## OVERVIEW

There are many elements of supply chain and logistical security in the air freight business. Physical issues such as secure packaging, handling, storage, transfer, chain of custody, and delivery of goods only scratch the surface where vulnerability is concerned. Weaknesses in any one area can lead to disaster. No matter how hard we try, there is no reasonable way to control all aspects of unattended cargo and air facilities.

This is complicated by the fact that transporting air cargo from shipper to carrier presents a potentially serious threat since chain of custody is rarely verified. Cargo is typically defined as a unit, with no particular emphasis on the physical or X-ray inspection of any one box or pallet. Hence, it is fairly easy to surreptitiously introduce a weapon or contraband into an innocuous bundle. Individual courier packages get rather more inspection than bulk

freight, but because of the generic nature of the packaging, air cargo all looks alike. Thus, little inspection is done until the final sorting, at which time it is too late to interdict tainted cargo.

Since most air cargo is first screened at its destination, the chance to interdict a weapon would only come after arrival—far too late. Security, containment, and control of unattended cargo can only be achieved when all logistics can be verified right down to the preinspection and final verification of boarded cargo. In order to achieve operational efficiency, however, air cargo is moved along quickly, the feature most desired by its biggest clients.

Regardless of the type of transportation that is chosen, secure packaging, sealing, and inspection of cargo is essential. Without it, no one is ever sure if the packaging is original, if the goods are actually still in the box, or if the box was switched with a weapon or loaded with drugs. Since the choice of shipping boxes or containers is made by shippers, and the choice of bundling of various random items of freight is made by carriers, little can be done to create a standard by which inspection procedures could be established. The lack of interaction between cargo handlers makes most air cargo unidentifiable. Typically the smaller, generic packages are placed in C containers, or air totes, with as many as 1,000 small individual boxes inside. The chance of discovering that goods have been stolen, finding tainted freight, or interdicting and disarming a terrorist-planted weapon in air cargo is small.

The random bundling technique associated with air cargo intensifies the risk of tampering with a unit within the bundle since everything looks the same. Containerized sea freight is typically palletized or floor-loaded to the maximum cube of the enclosure, and locked, sealed, and nested aboard a ship. However, air cargo is randomly stacked and net-strapped on aircraft pallets, which creates easy accessibility for skilled thieves or terrorists before, during, and after transport. The speed with which goods are transported, combined with the inherent risks of damage, theft, tampering, spoilage, or the introduction of contraband makes air cargo that much harder to monitor or secure. The fact that as many as five different companies may have handled, packed, or sorted cargo, with none of them responsible for the security function, makes for a perfect environment in which to steal goods or worse. Since most air carriers transfer cargo to trucks for delivery, little information that could pick up peculiarities is shared between the original shipper and the handler.

The ability that air carriers have to deploy cargo quickly is the crux of the issue. “Speed” is the operative word in defining air cargo risk, because the slower the speed of delivery the more apt you are to discover problems before they become disasters. For this reason, interdicting truck or sea cargo is far easier than air. The slower the freight moves, the more hands and eyes are on the cargo and the greater the opportunity to examine paperwork and supporting security protocols. The axiom that “cargo at rest is always cargo at risk” seems to imply that air cargo is less apt to be a target, but this is not the case. The difference between air cargo and other modalities is that in air

freight, commodities become randomly blended with hundreds of other packages shipped by anyone to anywhere in the world, making each box a mere drop in a sea of similar-looking packages.

## THE IMPORTANCE OF PACKAGING

There is a critical need to establish basic security packaging mandates for shippers to give carriers and handlers the best chance of discovering irregularities in cargo prior to its being put on board an aircraft. The recent introduction of intelligence monitoring into the air cargo security equation has begun to help identify potential threats and reduce the chances of tainted cargo being blindly accepted by air carriers. Only through these basic methods of risk reduction can we avert a terrorist incident involving air cargo.

There has been a far greater effort put forth to examine passengers than to examine cargo. In October 2007, the Bush administration issued an executive order mandating the 100 percent examination of cargo on commercial aircraft by 2010. That task is both ambitious and surely doomed to failure, since deploying such a system worldwide is unachievable. The executive order mandates that all cargo boarded on to passenger aircraft in the United States be examined, X-rayed, and evaluated. Funding has yet to be provided and responsibility for this inspection has not been assigned. The failure to create a global policy basically negates the executive order's effectiveness. Air cargo is a cog in a worldwide supply chain and needs to be addressed globally; no regional proposal will work. In any form of transportation, solutions that fail to become all-encompassing are rarely effective.

## THE UGLY STEPCHILD

In the years before September 11, 2001, and since, cargo security has remained the stepchild of the world's supply chain. Funding has been nonexistent and policy undefined. Logisticians failed to become proactively involved with loss control in their quest for speed, cost reduction, and operational efficiency. Since governmental oversight of the commercial supply chain is taboo, no effective protocol has ever been established, leaving the problem to fester and the criminal elements to mature and perfect their craft unabated.

When the Department of Homeland Security (DHS) established programs such as the Customs Trade Partnership against Terrorism (C-TPAT) and the Known Shipper Program, which designed for air cargo, they defined best practices and rewarded compliance with operational efficiency. Although no laws were passed to mandate compliance with C-TPAT standards, the threat to shippers of "slower passage of cargo" for those not willing to sign on was the stick that made compliance with C-TPAT principles a useful carrot. No TSA, DHS, DOD, or CBP programs or policies, however, have addressed air transportation vulnerability to the point where any of them has required, legislated, or mandated any risk reduction component.

No best practices have been recommended or adopted at the federal level and neither carrot nor stick have been offered to participants. It seems that the air cargo industry was expected to "do the right thing," but since this was not defined, the industry has become its own monitor, resulting in no action by anyone. The lack of specificity in policy has resulted in a cloudy interpretation of requirements, making the proposed governmental programs ineffective and inconsistent. Consistency is a basic tenet of effective security. Because we have not had a supply chain incident, most Americans have become complacent and feel confident that the government is actively participating in securing our homeland.

Air cargo is potentially the weakest link in the supply chain and therefore poses the greatest economic threat. Although the Known Shipper program and the soon-to-appear Certified Shipper Program are helpful in establishing best practices for the containment and control of unattended goods, little is really being done to close the security gaps. Our borders are more porous than ever, and with air freight volume increasing every day, we must focus on effective screening techniques and be more willing to settle for reduced speed. While passenger and baggage observation and inspection have been improving, general air cargo, especially courier cargo and most randomly consolidated air freight, still undergo little or no scrutiny coming into the United States. Cargo shipped from this country abroad does get some additional observation and inspection, but moving tainted, contraband, illegal, or hazmat (hazardous material) cargo still remains easy for those with the know-how to bypass the system. With approximately 50 million domestic cargo shipments initiated daily and twice that volume initiated internationally, the problem is acute.

Air vulnerability is not exclusively limited to terrorists and thieves, however; cargo can contain contraband foods, illegal animals, artifacts, skins, drugs, currency, counterfeit items, and even items as small as insects or fruit flies. They all present a real risk to our country and to our national economy. Although some domestic and international passenger baggage is checked with the help of dogs, X-rays, and reviewed intelligence, and is visually inspected, air cargo is more often than not given a green light through most U.S. airports with little or no real chance to interdict dangerous materials.

## A BOARDROOM DECISION

Vulnerability to any type of loss presents a real problem to businesses that opt to import or export by air. To accept risk without remedy is one course of action. "Wait and see" is a dangerous option because certain types of losses can balloon exponentially, potentially causing irreparable financial harm to the shipper or owner of the goods. Brand trust can be compromised and consumer confidence shaken due to theft, contamination, or a terrorist act using the company's shipment as a cover.

For example, the failure to protect certain drugs or controlled substances from theft means that they emerge on the black market. This can result in

death and personal injury that can be traced back to the manufacturer or shipper. Besides contingent financial losses, ingestible goods out of the care and control of the owner or carrier must, by law, be destroyed, thereby negating insurance as a financial remedy. Recovery of lost assets, especially in air cargo, is rare since discovery is rarely made until the item does not show up for delivery. By that time the thief is long gone and the goods are distributed throughout the supply chain.

Issues involving the illicit use of cargo to attack the United States or its assets can, under the PATRIOT Act, result in the prosecution of the original owner of the cargo or asset used by the perpetrators. This puts more pressure on the logisticians, who must continually make supply chain decisions based on routes, times, nature of goods, and of course, the carriers. In many cases carriers, fearful of theft, reject certain types of goods. Items such as jewelry, electronics, chips, ethical drugs, and even eyeglasses often represent the bulk of carrier losses.

Many shippers choose to insure cargo based on route criteria. Goods originating from or being delivered to certain countries present more of a risk than others. Goods staged by forwarders for consolidation are frequently kept in facilities where security is suspect. Insurance is typically focused on the conditions of loss. Many supply chain managers make assumptions that once a carrier has its goods in their care and control, their insurance and the extra policy taken out by the shipper cover all possible conditions of loss. This could not be further from the truth. Losses that occur on carrier property, be they from theft or damage, are typically covered to the extent of the carrier's stipulated limits of liability. Insurance taken out at origin is rarely extended to all handlers of the cargo. Since air cargo may be taken by truck (drayage) to an airport, moved by one or more carriers, and then delivered by yet another third party trucker; the conditions of loss and the magnitude of vulnerability to peril are multiplied many times. Unless specific insurance is taken out by the shipper for any and all conditions of loss, the shipper may suffer. Carriers are liable for cargo based on cents, calculated by the pound, except as specifically noted in the contract of carriage. Unless the air bill covers special conditions, many limits of liability for the cargo are based on the handler's insurance coverage, or lack of it.

## WHO IS THE THREAT?

When looking for an effective remedy for supply chain security problems, regardless of the logistical environment, you must first have an idea of your adversary. Time can often be an adversary in situations regarding time-sensitive goods such as body parts, vaccines, or blood. In some cases, damages might be based on rough handling or even the mysterious disappearance of cargo due to clerical errors. Losses can occur in warehouses, on trucks, on airport property such as in-bond facilities, or in any modality handing the cargo. Cargo in transit is always accessible to people, and many of these handlers

have not been given appropriate vetting to guarantee security for the goods or physical containment on the property. Many airside employees lack the skill to handle sensitive goods according to a given procedure.

Just think about the trucking industry, for instance, remembering that almost all air cargo is moved by truck at some point in its cycle. The annual driver turnover rate in most common carrier companies is approaching 125 percent. Just to keep the trucks on the road, businesses have had to accept applicants with tainted or criminal records, people with no permanent residence, and some who are hired on a day-to-day basis, thereby creating havoc in investigating losses associated with employees. Training and company integrity is consistently lacking in transient labor pools and this makes internal theft and vulnerability a significant concern. In the forwarding business, many carriers are unknown to the shipper or recipient because of interlining. Interlining means that air carriers can legally choose to move your cargo by truck or even rail without permission or knowledge, thus also increasing the risk of loss.

In order to effectively plan for a threat, the threat and the adversary must be defined. Defining threat begins with forming immediate and potential risk into a matrix, weighing each component by the cost of loss and the ways of providing a remedy. As countermeasures are developed to tighten supply chain security, the overall effect is to gradually reduce each specific vulnerability to a manageable level. At times, however, the trade-off for increasing security is operational inefficiency, which defeats the purpose of moving cargo by air. Because a terrorist needs only to be successful once to achieve his goal, the triage approach to controlling the security of your supply chain seems futile. Controlling the international supply chain is all but impossible. As already stated, not all threats are terrorist based, yet conditions of loss pertain to any cargo at any time.

Most companies address threats to cargo from the most important down, hoping that each remedy collaterally addresses lower-level issues without complicating the system. In order to effectively enhance supply chain security, businesses must adopt the mandated programs set forth by our government. Programs that do not echo such federal mandates will become redundant and money invested in them will be lost. For this reason, many in the air cargo, truck, and steamship freight industries have failed to agree to and implement a remedy to terrorism. Basically no one wants to start a program to be told later on that it fails to comply with the "recommended" governmental programs. Since no programs actually exist, no one is rushing to create his own! Whether funded internally by the carrier, provided for by the shipper or clients, or provided by the seaports and airports, most modalities use little real effort to protect freight. Because no consistent programs apply, cargo remains at risk from origin to destination. Unfortunately little is being done by the U.S. government beyond studies and nonbinding suggestions to secure our national supply chain.

The process eventually chosen to increase security must be specific to a particular mode of transport and be maintained throughout that industry on

an international basis. Many countries fail to require any such measures, since they may not be able to fund them or to technologically implement them. The fact that the United States wants to benchmark technology does not make for blind international compliance. Before considering the implementation of a security process, most countries will focus their efforts on what is practical for their conditions, culture, and funding. In many cases this will not even come close to U.S. standards.

Unlike stable and predictable security for a home, an office, or even a vehicle, supply chain security has a number of interdependent dimensions that render most general protective systems ineffective. The approaches to security and operational efficiency used by each vendor differ so radically that a final agreement on security measures would be almost impossible. Besides the fact that freight is predominately unattended, constantly moving, and changing hands, the protection available at any one location may be nonexistent or unavailable. Since air cargo rarely hits stop or choke points until it reaches an airport sorting center, any implementation of interdiction and inspection techniques must be germane to each vendor and handling facility as well as consistent for all cargo entering it. In air cargo, the carrier hauling the freight may change numerous times for many reasons, all of which are unknown (and unnecessary to be known) by the shipper. If the cargo is delivered on time, client expectations are met. Shippers must rely on the integrity of carriers just as carriers must rely on their shippers in initially accepting freight. This mutual trust, albeit self-policing, has become the backbone of the air cargo industry.

In any product move where a threat against specific cargo (such as pharmaceuticals or electronics) is high, you will need to know why someone wants to steal it or tamper with it in order to develop a deterrent strategy. Terrorist threats are far less complex than one would think. Their purpose is clear and direct, yet their technique, the intricacy of the action plan, and the methodology are far more sophisticated and professionally orchestrated. Their motivation, in terms of ideology, determination, and reward for success, and their skill will typically prevent you or your carrier from planning a suitable or sustainable defense. There is no doubt, however, that whether the threat is theft or terrorism, your adversary is still a major concern. If dealing with this is not in your business strategy, it should be.

## ADDRESSING THE THREAT

Indicative packaging is a classic approach to cargo security since it provides a unique identity for each package. When visually inspectable packaging, such as security tapes and self-voiding seals, is provided, an anomaly or obvious breach becomes apparent to each handler, thereby reducing risk. When a feature is provided that indicates a package has been compromised, handlers stand a better chance of finding pilfered cargo. If anyone along the supply chain is aware of a particular package's appearance, unique markings, numbers, or designs, it is easier to ship the package in good order than with if it is shipped in a generic

box. If tamper-evident packaging is used, any handler along the supply chain has a benchmark of characteristics to use for more a thorough inspection. The ability to visually inspect all cargo is beneficial to shipper, carrier, and recipient. The more user-friendly the technology is to supply chain members, the more effective it will be in deterring problems. Most indicative packaging devices are in the form of tamper-evident or shock-indicating self-adhesive seals or tapes that help to visually identify possible penetration or manipulation of a box, pallet, envelope, or container. Self-adhesive seals and tapes are the most common means of closure used for most cargo in boxes or envelopes. When applied onto a bundled asset such as a C container door, trailer door, or aircraft hatch, the device effectively offers containment to all of the products inside. Devices such as tamper-evident tapes and self-voiding security seals help to uniquely identify parcels as well as to indicate penetration. These types of seals are both cost-effective and highly deterrent in nature. They are typically applied at origin and provide inspectability throughout the supply chain. The more simple (KISS—Keep It Simple, Stupid) they are, the greater their usefulness and effectiveness. By creating a risk of discovery for the thief or terrorist, you lessen the chance of an event or loss.

Adversarial analysis requires a working knowledge of a person's ability to effectively complete his mission. Whether the mission is catching the quarry or planting a bomb, the perpetrator's ability to beat you is a mixture of his skills pitted against your countermeasures but weakened by your inherent complacency. Your ability to mitigate loss revolves around your choice of countermeasures, training, and the reliability of your handlers as they carry out the complex coordination required when cargo changes hands. Theft or acts of terrorism occur when the perpetrator surreptitiously gains access to cargo, either en route or prior to shipping or delivery. These situations can occur at any point throughout the transportation and storage phase of shipping. Knowledge of the location, movement, and timing of the goods, coupled with the level of risk the person is willing to take, his motivation, and his expertise, plays a significant role in his success or failure. Your best defense is to plan for problems before they arise and gear your best practices to deter these activities. Neither theft nor terrorism are occurrences that anyone can completely eliminate, regardless of the technology used, the security plan, or its practical application. A perpetrator's reward for success and his ability to choose his time frame are factors that give him the upper hand. With the goal of speed in the air carrier industry as an additional barrier to safety, the chances of deterring an act of terrorism (or theft) that is already in progress are limited at best.

## WHAT'S BEING DONE TO SECURE THE SUPPLY CHAIN?

When President Bush created the Department of Homeland Security (DHS) in 2002, his idea was to create a central hub for the sharing of informa-

tion and for the selection, choice, and implementation of a remedy to terrorism. The concept was designed to reduce the risk of a terrorist strike on U.S. soil by stepping up the processes needed to discover problems before they do harm. The concept was further directed at reducing vulnerability to an attack through the commercial worldwide supply chain by sharing and analyzing business data. By combining all government efforts into a centralized review process for cargo and intelligence, President Bush felt that the deterrent value would be overwhelming and thereby curtail the threat.

His goal would be achieved, at least initially, by the use of the intelligence services and the analysis of data relating to inbound cargo—that is, to identify suspect shipments and shippers and to interdict associated cargo. The president expected that he would get better physical inspection of cargo and the willing participation of the industry, and that his program would become the standard by which the United States would secure its borders and thereby establish logistical security as a defense against another September 11. By using the best and brightest tacticians to review inbound cargo data, the DHS could theoretically identify shipping anomalies and interdict suspect cargo before it reached U.S. shores. The creation of the 24-hour reporting rule for containerized cargo set the stage for data verification, and began to offer hope to the shipping public of an effective security effort within the air cargo industry. With the ability to act unilaterally, Bush felt that these policies, administered by a central agency (DHS), would be the cornerstone of risk reduction worldwide.

Instead of this succinct, focused concept, we now have more than 350,000 people in a newly formed, self-contained bureaucracy called the TSA/DHS that is so mired in its own layers of interpretation of the president's simple original security plan that it has effectively done nothing to secure our supply chain or our borders. Of note, there has been no positive or effective action in air cargo or in domestic trucking, and there have been only some basic improvements in containerized sea freight. We have spent more money on defining and analyzing the potential problems than on solving known risks, by a ratio of 5,000:1. We have dressed up thousands of untrained, part-time TSA passenger air inspectors and armed them with state-of-the-art technology for screening passengers and bags but failed to consider the total picture of air security with relation to the cargo that sits directly below these passengers. We now permit Canadian and Mexican trucks to cross our borders with minimal inspection and no basic rules for safety or security. We have almost no security on the passenger rail system and even less on water craft.

Passenger protection, that is, what is visible to the public, is simply a confidence builder with very low effectiveness against a professional adversary. With over $5 billion in dedicated assets to secure our skies, the TSA has spent only $55 million on protection technology for air cargo.

The TSA is well meaning but has shown itself as organizationally inept and ill-equipped to mandate, implement, select, or fund changes in the security process for cargo across the board. There is neither any reasonable

system that can detect every form of contraband nor any way to guarantee 100 percent success in any security endeavor. However, without challenging industry to self-impose systems and to create more stringent criteria for insuring the integrity of air cargo, we will not improve our current condition. Congress needs to empower those qualified to make such decisions and mandate compliance without regard to politics. Industry has to understand that the speed of commerce is directly proportionate to the risks associated with a terrorist strike. Somewhere between 100 percent physical inspection and administrative scrutiny lies an acceptable and effective mix. If cargo were to be slowed, would that not be a better alternative to having little cargo security?

## SECURITY IS NOT A PERFECT SCIENCE

A number of programs have evolved from the original DHS premise.

By definition, both the Known Shipper Program and conventional cargo screening programs imply an administrative overview of the shipper, cargo, and recipient. The collected data is then used to detect anomalies based on past practices in shipping, commodity norms, or other criteria that would indicate a noticeable change in behavior. This is carried out completely in the back office and rarely if ever becomes "hands on." The obvious flaw in this thinking is that even if the shipper is known and the cargo and recipient both seem innocuous, the box may still contain a bomb. In my personal experience with the package delivery business, even if a box was leaking powder or fumes, or if it had battery cables hanging from it and was poorly packed or labeled, it would probably still manage to arrive at a distribution hub in the United States—and possibly even get delivered to a client! Some news networks have shown this scenario in practical terms by shipping a restricted (nonlethal) package to their offices just as if they had shipped apple pie!

Given that any unsecured and unchecked cargo can be transshipped numerous times, and once at an airport it can be shipped by ground transport to further confuse the process, administrative "back office" scrutiny falls short of a true protection platform. The goal of an economic terrorist is to deploy a weapon of mass destruction, or mass effect, in the U.S. commercial supply chain such that it creates fear, disruption of business, and costly remediation, sufficient to stop commerce at some level. Providing 100 percent protection against such a terrorist is impossible.

## AN AMBITIOUS BUT ACHIEVABLE GOAL

Nothing short of 100 percent screening of both physical (visual) and mechanical operations can totally prevent problems. Such an approach is not only impossible, given the nature of international commerce, but impractical based on the sheer volume of cargo as against the time needed to conduct such an inspection. Air freight moves in predetermined cubes designed to fit

the belly of an aircraft, with rigid weight and volume constraints. Rarely if ever does a package or pallet move independently. Bundling is the norm but it is typically done without respect to the nature of the cargo. In many cases, liquids move in close proximity to other cargo, and hazmat is rarely if ever segregated from other freight on air pallets. Proposed government projects, such as the use of RFID as a quick fix to identify individual packages among the sea of similar-looking cargo, proved ineffective and impractical. Because in theory RFID was viewed as a security rather than a logistics tool, millions of dollars were spent by government and industry in an attempt to implement this technology. The goal was to screen cargo, bundled in containers or on pallets, in such a manner as to find out whether anything was added or removed during transit. Because RFID has severe limitations—reading tags through metallic enclosures, or with metallic interference, and through liquids—this attempt failed!

RFID is available in two forms, passive and active. A signal-emitting or battery-operated RFID seal sends a signal to a receiver where a nonpowered tag simply receives and returns a signal through an antenna. Active RFID proved unsuited for many reasons, especially because of cost and the inability of users to effectively return these devices because they are built directly into the shipping containers. For all practical purposes, security was not achieved with RFID devices, simply because they could not be shown to identify a single box as original, thereby failing to achieve the goal of packaging identity. The infrastructure that was needed to use such a system worldwide was hampered by the fact that not every tag operates at the same frequency. Since cutting back the focus on RFID as a solution, our security gurus have failed to adopt more practical policies and materials, and have basically done nothing.

Diversity of cargo, generic packaging techniques, and bundling of hundreds of packages on air pallets and in C containers contribute to the chaos involved in choosing a fixed inspection (choke) point, product, or process. In many airports throughout the world, in-bond or staged cargo means unattended boxes out on the tarmac or in uncontrolled warehouses and in many cases loose, awaiting palletizing and loading onto aircraft. Very rarely is this staged cargo caged or securely controlled while awaiting loading. In many airports around the world, access to staging areas is easy, and therefore regardless of the security inspection program used when cargo is tendered, the introduction of a weapon or the removal of freight (while being staged) is always possible. The random nature of cargo in terms of size complicates any inspection processes. The lack of dedicated manpower funded by the airlines themselves at every station all but precludes 100 percent inspection of over-the-counter freight. The courier business is notorious for a complete lack of controls. Items picked up in drop boxes or given directly to couriers can seamlessly slip onto both commercial aircraft and freighters with little or no hands-on inspection. A bomb containing a biological agent or an explosive can easily be planted in any size parcel.

## AN IDEA TO HELP THE INSPECTION PROCESS

Placing preinspected cargo into a consistently contained format would not only speed technology inspection and reduce load times but would also improve operational efficiency and throughput for the carrier. Secure packaging done after inspection at airside would create an increased revenue platform for freighters and commercial aircraft alike, because the cube and weight of each "brick" could be preplanned. The contents of each "brick" would already be known on the manifests and the evidence of penetration would be simple and universally understandable. The use of cargo bricks would give carriers boarding and off-loading cargo a visual inspection point for all cargo in the bundle, thereby speeding the off-loading process. By requiring bulk shippers to pack in a predetermined "brick" format, using tamper-evident shrink film, security tapes, or other visibly inspectable components, we would move closer to assuring packaging integrity. These requirements will complement the Known and Certified Shipper initiatives and benefit the carriers tremendously.

Airport choke point inspection for bulk cargo could be achieved, since all cargo would be similar in size and therefore fit on predesigned conveyors using appropriate sniffer and X-ray screening technology. Much like seaport screening, where one point serves many, choke point inspection establishes consistent, monitored controls and thereby adds layers of security to the process at a lower cost while maintaining efficiency. If shippers were brought into this equation through reduced tariffs or other financial incentives for those that comply, they might be more apt to buy into the process. For nonbulk shippers, prescreening at time of delivery to the air carrier would be seamless. These screening items would then be bulk-packed by the carrier into containers, using bricks or some other acceptable bundled container.

## BUYING-IN

The risks associated with tainted air cargo are somewhat greater than with other modalities, since air cargo is predominately shipped with or near people. Air cargo on freighters always arrives at facilities where people are present, whereas sea freight is far more isolated from human contact until it hits the highways. Terrorist threats to ports are, of course, of equal concern and exhibit an economic impact that is equal to or even greater than threats to air cargo. Regardless of the terrorist event, however, the commercial supply chain can take months to recover and the costs in economic losses are staggering. With any disruption in supply chain activities, from a simple theft to a major breach, the costs of loss far exceed any proactive remedial action that could possibly required by the carriers, shippers, or airside facilities.

The fact that security plans require buy-in from air carriers, governments, and shippers is the fly in the ointment. Everyone wants positive change and no one wants to disrupt commerce or affect the bottom line to achieve it.

Not many air cargo companies are willing to fund remedies or to mandate the processes required to increase protection levels. Governments typically balk about security expenses while shippers never want to accept the inherent delays that inspections will surely cause. The carriers will always get their payment for delivering goods, and therefore they seem to choose the course of least resistance. If governments can contribute inspection technology in the form of machinery, a defined security plan, and recommendations and funding for inspection personnel, while carriers and airport operators implement these systems, and if shippers can adjust their delivery schedules around potential delays in their just-in-time (JIT) inventory process, we can be well on our way to reducing air cargo risks.

## WHAT'S BEING DONE?

Law enforcement views cargo theft as the lowest possible priority. The federal government has seen fit to remove all FBI personnel from cargo theft operations and reassign them to antiterrorist task forces. Cargo theft has few defined laws and consequently, there is no real deterrent against theft. There are few convictions and most theft-based prosecutions are limited to the state rather than the federal level. Does no one realize the connection between cargo theft and cargo terrorism? In air security, most investigations are left to the air carrier security personnel, even further diluting the risk to thieves and terrorists. Most cargo criminals are recidivists and most serve no time in jail if actually apprehended. Laws covering cargo theft or theft resulting in endangering human life now include the statutes contained in the PATRIOT Act, which open new avenues of prosecution and make available new resources to deter perpetrators, especially in air cargo incidents. But although there has been a good deal of positive fallout from September 11, related to bolstering airside security through the PATRIOT Act, there has been almost no reduction in vulnerability or interdiction.

The TSA has initiated requirements that any service industry relating to aircraft must be located on a secured site with appropriate fences, locks, cameras, and sign-in processes as well as background checks for employees. Planes flying overnight outside the United States require self-adhesive tamper-evident door seals to identify unauthorized penetration. The TSA has mandated more stringent requirements for vehicles moving freely at airports such as those of food suppliers, refuse companies, truckers, brokers, and forwarders. Food carts must be sealed, as well as the trucks delivering them airside from off-site warehouses.

The PATRIOT Act has given law enforcement and our legal system the tools to help identify those who would attempt to hurt the United States both internally and abroad. It has given law enforcement the ability to verify the identity of a potential terrorist through access to records and to personal information, searches, and verbal communications that previously were available only through subpoena and more fact-based legal orders. This law

actively helps to disrupt terrorist plots and organizational development by stifling the movement of financial resources internationally. This is a sound strategy as it has achieved the creation of useful data that could help determine shipping and cargo anomalies and thereby identify suspect shippers and cargo. The CSI (Container Security Initiative) also has been helpful in data creation on the seaport side. Both of these programs help identify smuggling, theft, contraband, and drug importation as well as money laundering, conspiracies, trade fraud, and terrorism.

However, evaluation is rarely done physically; hence, while the intelligence activity is helpful and necessary, it fails to address the need to hand inspect cargo. Not all intelligence results in finding tainted cargo, and although it provides a strong platform, it fails to account for problems occurring en route or after delivery to a sorting facility.

In the maritime arena, legislation includes the Port and Maritime Security Act of 2001 and the Maritime Transportation Antiterrorism Act of 2002. The G-8 summits have always had cargo security on their agenda and participants have consistently expressed interest, but little action has ever taken place. Operation Safe Commerce (OSC) was to be a public and private partnership dedicated to securing the world's supply chain, but it has also failed to mandate a workable solution and has fallen short of being effective.

Carriers are constantly struggling with increasing fuel costs, salaries, personnel, equipment maintenance, regulatory barriers, and stiff competition, so who can wonder why they balk at taking on the expensive function of cargo security? Notwithstanding their obvious self-interest in security, brand, and equipment protection, and the potential loss of life that can be caused by a terrorist strike, air carriers still feel burdened by the lack of specific direction given to them by the TSA. The confusing nature of government regulation regarding an approved definitive course of action to secure unattended air cargo is such that carriers remain on the fence and take no action at all. Whether it is their job alone to screen cargo is also in question.

One plan is the Known Shipper Program, instituted shortly after September 11 to prevent the random introduction of a bomb into the cargo of large-volume shippers. The members need only sign up online to declare that their personnel are vetted, the facilities of their shippers are secure, and their cargo is safe. The program uses information provided by the shipper himself to his forwarder or directly to the carrier to establish himself as a secure shipper whose cargo is beyond reach. This program is useful in practice if we assume that every terrorist, thief, or smuggler is always honest and forthcoming! It allows the shipper (even if it is a front operation, so long as he pays his bills) to demonstrate through the submission of a form the fact that he is a "good guy" and deserves a "pass" through the rigors of air cargo security screening and inspection. In these cases, the shipper becomes the inspector in a technique I call the "wolf in the henhouse."

The Custom Trade Partnership against Terrorism (C-TPAT) program for sea freight, dictates that all those who sign up for the program will have full

background screening for their employees, secure yards and stuffing facilities, and appropriate tamper-evident security packaging and sealing for their containers and trailers. There is no such mandate for air cargo and even if there were, it could not be universally enforced, based on the diversity of air cargo. C-TPAT itself is a voluntary program that again offers the "feel good" approach to security rather than a true effort to secure the world's supply chain. The C-TPAT program has been in effect for almost four years; however, little is being done to actually validate members, systems, processes, or containers. Currently, less than half of 1 percent of sea containers is actually opened for inspection.

U.S. Customs and Border Protection came out with the C-TPAT program some years ago as a means for industry to participate in securing the world's sea freight through the use of best practices. Since CBP had no experienced personnel available to design sealing security programs nor any original ideas, it asked the International Standards Organization (ISO) to use its seal criteria as a basis for securing containers. As a result, ISO developed ISO 17712, a set of recommended, not required, best practices and products to securely seal sea freight containers. Among these recommendations was the infamous "bolt seal" recommendation. This was (after four years of misinformation) withdrawn in August of 2006, but it still exemplifies the worst our government has to offer in recommending appropriate remedies for supply chain threats.

The standards used to recommend best practices dealt with form rather than function. In the air cargo industry, no such recommendation was proposed because there are far too many bundling techniques available for air cargo and air cargo can not be sealed permanently as can sea freight. Cargo handlers must have access to air cargo at all times, and thus the use of self-adhesive seals rather than barrier-type products is required. There are no doors to close or locks to apply when it comes to air cargo. Because of ISO's inability to tackle the problem, remedial recommendations have effectively been left to chance.

## THE COSTS OF LOSS

There is no denying that the United States has porous borders. Regardless of the level of inspection at crossing points, trucks with cargo and people move in and out of the United States daily. In the transportation industry and especially in air cargo, we base much of our security on blind trust, because over the years that has been our societal norm. In our economic system, we cannot add more barriers to commerce without completely disrupting logistics as we know it. Logistics is the backbone of commerce, and integrating walls and barriers to that system cannot be done without significant push-back from all quarters. Unfortunately, terrorism gets press coverage only for a while, and it fades from public view when its media value has elapsed. As a consequence, funding to prevent a cross-border event is precarious and prone to mimic public awareness rather than consistent real world threats. The fact

that billions of dollars are being spent on the Mexican Fence project clearly shows that money is dedicated when there is a direct correlation between political benefit and public outcry. It seems the illegal immigrant worker issue became the instigating factor rather than concern that a terrorist can get on to United States soil with little skill and effort.

The costs of loss to our economy and GNP through a terrorist strike can be catastrophic, but proactive spending to reduce this known risk is currently nonexistent and will not be allocated unless it is federally mandated. If we take cargo theft from air, truck, or sea freight, and combine its effects with smuggling, money laundering, and other conditions of loss, we get costs approaching $55 billion. This type of information rarely hits the news media.

The cost to our government to deploy a domestic technology-based air cargo inspection plan would be about $3.6 billion. These funds would purchase automated inspection equipment and arrange deployment to major air hubs both here and eventually worldwide. Funding such a move would establish benchmark inspection techniques that could be enhanced by carriers and governments and subsequently benefit world commerce. Initially, the program would be clearly designed to bolster the security of U.S. bound cargo. What could be a better use of funds? In addition to dealing with technology, workable process controls for shippers and carriers need to be both designed and implemented. These controls would entail a minimum of 24-hour reporting prior to arrival of cargo data as well as establish a hold on suspect or noncompliant shipments for 100 percent inspection. Prenotification in air cargo, as is done currently in sea freight, gives the authorities time to filter intelligence into the security equation to help identify anomalies before the goods enter the supply chain.

The competitive nature of companies will help define this system's effectiveness. Everyone wants JIT cargo and so few will accept changes. Air cargo still basically travels unencumbered by paperwork. E-shipping is the standard and e-data is kept to a minimum by design. The more data that is required, the more cost and time delays are created. By maintaining the requirements for minimal data collection but enhancing the inspection process, shippers and carriers could reasonably enjoy some of the benefits they have now, while decreasing the risks. The added inspection process simply involves time, the component that is least available in air cargo. This problem can be solved by creating efficiencies in packaging and loading and providing means to easily recognize packaging anomalies, thereby increasing throughput.

Data has currently become a point of contention among shippers and carriers, since they look at sharing cargo data as tantamount to compromising business intelligence. Who maintains the data, who has access to it, and how it will be evaluated are all questions that have been raised. Collectively, industry has resisted data collection because of the uncertainty of its use or of its impact if compromised.

Intelligence aside, the TSA and industry partnership has attempted to address cargo security through the use of studies rather than action. The TSA

has spent millions of dollars on these studies with Deloitte, Lockheed, and other think tank consortia with little to show for the investment. There are currently 300–400 cargo security professionals at the TSA focused on the threats and vulnerabilities to air cargo; however this represents only 1 percent or less of the TSA's workforce. What it has come down to is that, according to a report from the Center for American Progress, "The TSA allows the 1.5 million Known Shippers, 4,000 freight forwarders (10,000 individual branches and millions of personnel), and 300-plus commercial air carriers that form the air cargo supply chain, to largely police themselves." Scary.

Air cargo risk can be viewed in many ways, but remedial action must be ordered in such a manner as to direct resources to the most critical areas first. By defining individual risks, air carriers and their clients can leverage their choices of whose job it is to do which task and therefore collectively participate in reducing risk. Matters such as security tapes and seals would automatically become the shipper's responsibility, while the carrier's responsibility may be to visually inspect the boxes at each hub and prior to boarding. Carriers would be ultimately responsible for the X-ray inspection of cargo prior to boarding and during a delivery sort, while CBP would pick up the oversight at both ends as well as acting as the enforcement arm if problems are identified.

## A POSSIBLE UNILATERAL SOLUTION

Courier boxes and envelopes supplied by carriers should be required to have an original number and (if possible) a tamper-evident seal and markings (tied to the bill of lading), so that it is harder to replace a package with a similar box. Recipients would have the ultimate responsibility to compare manifest numbers with packages before accepting them. Carriers may elect to physically pack, inspect, and seal counter-tendered goods from certain shippers, to protect against theft and the introduction of piggybacked contraband. In this scenario the carrier would control the packaging components and security systems and bear the costs associated with this level of protection-based safety. Shippers would be charged for this service, just like the security charges that the airports add to passenger tickets. By offering a participatory plan whose outcome is mutually beneficial, carrier and shipper or carrier and government can cooperatively work to provide the unique component of security that each one does best and at the lowest cost.

## SPECIFIC RISKS AND THREATS

Cargo theft is alive and well in air shipping as well as in most other modalities. It is conservatively estimated that air cargo theft is an annual worldwide problem approaching $25 billion. Most of it occurs at unprotected airside facilities, at distribution and sort hubs, and at points before, during, and after arrival. Luxury goods such as sunglasses, jewelry, electronics, watches, CDs,

software, designer clothes, and pharmaceuticals are among the long list of targeted goods. Many of these items, like any air cargo, are most vulnerable when left unattended in in-bond areas or in unprotected airside warehouses. Stealing can be easy for those with access and is almost impossible to detect, due to the sheer volume and chaos associated with cargo sorting and staging. Theft may involve either the total or the partial removal of the contents, making detection even harder. Small-volume pilferage mounts up quickly when dealing with controlled substances, jewelry, or electronics, and because many companies fail to keep records of this kind of theft, it continues unabated, costing businesses millions of dollars in hidden losses. Chips are often more valuable than diamonds and, cash is no longer king in theft targeting.

Claims of mysterious disappearances plague the shippers and the insurance industry, but many never get filed simply because of the cost and the effect on future business. No business wants to air its dirty linen by informing the public that some ethical drug, blood, cell phone, or commodity has been stolen and available for sale by thieves. The negative press a business receives when admitting that its goods were stolen and are now astray in the market can ruin a brand and bring stock value to its knees. This is especially true for items such as pharmaceuticals, baby formula, or foods.

It is possible to surreptitiously open a box, remove items from it, and reseal it with little or no scrutiny, because packaging is typically generic and opaque and there is no viable or reliable means to detect opening and reclosure. Tampering is usually undetectable until the item is delivered. No matter how hard air carriers and air couriers try, this form of loss continues to escalate. There is little or no reliable data on the dollar volume of cargo theft on an international basis, because no one wants to make the data public. Insurance data is also quite fuzzy since most transportation loss, where employee infidelity is the proven cause, is not an insurable event. The Carmack amendment covers many of the carrier's transportation losses based on the "pound weight" of the item rather than on wholesale or market value. This biased approach to compensation makes financial recovery through insurance impossible for many high-value goods.

Issues such as a company's reluctance to share critical loss or other embarrassing data further complicate the effort to assess the magnitude of actual air cargo theft losses on a national basis. Without access to such data, it is far more difficult to propose government programs, since the matter is not viewed as critical. Many carriers still deny that the problem exists in their company, since the exposure of a theft problem could hurt their business. Government statistics and available loss data from industry fail to show the magnitude of the problem, so little attention is given to creating a legal remedy for it.

With the advent of government-mandated counterterrorist activities in airport facilities, theft control is being positively impacted, but as a collateral rather than a primary focus. For air carriers, theft control has always been the stepchild of operational efficiency. Since they have little or no control of packaging, type of goods, or daily volume, carriers must rely on the use of best security practices to prevent theft.

Many air carriers sell cargo insurance as a means of increasing their profit, since actuarially insurance is a tremendous profit maker. Carriers sell the concept of protection at an acceptable rate for the shipper and work the numbers and trends to bolster their income. Insurance in the cargo area, however, unless issue specific, is rarely effective.

A lesser-known form of theft is the compromising of intellectual data placed in courier boxes or envelopes and subsequently opened and read prior to final delivery. This is prevalent in the courier business, because generic courier packaging lends itself to this form of surreptitious penetration. Since most courier packaging is unmarked, unnumbered, generic by design, and lacks an original number, opening the box or replacing the original box with an exact replica is impossible to detect. A perfect example of this form of theft occurred some years ago on Wall Street. Venture data involving mergers and acquisitions was becoming known in advance, because couriers were able to open, read, and replace documents in overnight letters.

### Damage

Most cargo suitable for air shipping is highly valuable, critical by nature and design, and in some way sensitive or delicate. From body parts, blood, and vaccines in coolers to newly calibrated electronic devices, air cargo can be almost anything. Blood, pharmaceuticals, and foods that need constant refrigeration are vulnerable to damage through delays or equipment failures. Electronic items such as plasma TVs are frequently damaged through rough handling, while smaller items are frequently crushed or exposed to conditions that adversely affect their value. Unlike palletized cargo moving in sea containers or rail cars, air cargo is randomly packed for shipping at the time of loading on air pallets. Items can be flung into C containers, loaded on air pallets, and covered with 5,000 pounds of various other types of cargo. Little or no priority is given to bulk air freight insofar as commodity classification or stacking priorities are concerned. The random nature of loading and stacking causes most damage.

Because of the speed with which air cargo navigates the supply chain, if damage is not discovered at a sort facility, it is rarely ever found until the item is opened by the recipient. Air claims involving concealed damage or loss resulting from packaging deficiencies are hard to prove, as shippers are frequently unable to document packaging specifics; therefore, many claims are denied. Outside insurance on air cargo is harder to secure than on truck, sea, or rail cargo and it is considerably more expensive and issue specific. Most air carriers offer the purchase of cargo insurance as an add-on through their profit center. The Carmack amendment created benchmark valuations for lost or damaged goods that are of little use in assessing the true cost of a loss. Values of $.25 per pound remain as active benchmarks for uninsured freight claims regardless of commodity. Little can be done to improve or bolster packaging without a considerable increase in shipping expense, as all air cargo is based on a cube/weight ratio.

Damage claims in air freight outpace theft by a ratio of approximately 3:1, where damage claims in truck and rail are at a ratio of easily 10:1.

The introduction of contraband into legitimate cargo has been going on for many years, but it was not recognized as a problem until September 11. Threat awareness brought this condition out into the open, but agencies such as DEA and CBP have been dealing with it for more than 30 years. Drugs and other contraband have moved freely in the world supply chain and are regularly inserted into cargo of every description. This underground supply line is all but invisible to inspection because in many cases the product masks the contraband. Coffee blocks smell, drugs encased in tile are invisible, and nested cargo (cargo placed inside larger items) is rarely examined, because few parcels are opened. Interdiction technology has only recently been adopted. More effort has been put into these areas in the last 10 years than has been allocated to any theft controls. The collateral positive effect of this type of scrutiny is that it is becoming a better means of discovering weapons and drugs than any other tool. Passenger inspection personnel supplied by the TSA have done little to improve detection in these areas since most inspectors are unskilled and poorly trained. Also most smuggling is done in cargo, which is outside the scope of passenger inspection The programs that mandate checking accompanied baggage and freight are only now being put into regular practice. According to the Center for American Progress, only 5 percent of the 2.8 million tons of air cargo carried onto commercial aircraft are screened for explosives and other dangerous devices. That would mean that there is almost no screening for the almost 1 million tons of freight passing through passenger terminals. Illegal food, animal, and agricultural cargo can also be the basis for the deployment of a weapon of mass effect or mass destruction by air. Biologics and related chemicals are next to impossible to detect in the sea of small packages on an aircraft or in passenger baggage or freight. The fact that animals can be an effective terrorist tool makes all cargo suspect and no cargo inherently safe.

## Smuggling

Smuggling can be defined as the shipping into the United States of contraband cargo, which is cargo that is either misclassified to avoid tariffs and duties or is made up of illegal or banned goods or people. Misclassification is an easy and reliable way to beat the system, regardless of the size of the cargo. Smuggling can involve dangerous cargo, ethical drugs, controlled substances, animals, or any type of seemingly innocuous cargo that is deemed by our government to be unacceptable for importation. In addition, counterfeiting is fed by smuggling efforts. A creative terrorist can easily introduce a weapon, explosive, or biologic inside cargo, nested as a piggyback to some approved shipment or inside a person or animal. It is extremely difficult to detect this form of smuggling. Intelligence typically is the key to the discovery of this form of threat, whereas conventional physical inspection techniques

are ineffective. Nesting is extremely common in drug or currency smuggling, where smaller bags are nested in larger cargo or vast amounts of contraband cargo are broken down and sent to many locations, to be combined and transshipped elsewhere once inside the United States.

## INDUSTRY OVERVIEW

Passenger-accompanied air cargo is a major profit maker for the airline industry. It accounts for approximately 15 percent of the industry's overall revenue with no additional expenditures required. Requiring more physical security in this one area of revenue would not only decrease profits but would also add residual operational costs, slowdowns, and dedicated personnel. The balance between each revenue-generating component in the air industry affects its willingness to fund and implement enhancements, so unless these are mandated, the industry has no incentive to introduce them.

Air cargo security is an uphill, no-win battle between what is industry-practical and what is mandated by law. Numerous congressional attempts have been made to mandate 100 percent inspection through legislation. The cost of 100 percent cargo screening on commercial passenger aircraft would be in the billions of dollars. Funding such an inspection mandate would be a challenge. It has been proposed that there be a fee charged for security, much like the airport security fee for passengers. With millions of air shipments being made daily, funds would be amassed quickly. The issue is, who administers these funds? What guidelines would be needed to purchase technology, and, of course, what technology would be purchased and from whom? Since there are really no answers to these questions, no one can begin this process.

According to the International Air Transport Association there will be a 26 percent increase in Asian air freight in the next few years, resulting in a tremendous bottleneck. Worldwide air cargo inspections also face the issue of a country's ability to fund inspections, and the question of whether the current airside facilities can handle the inspections in a secure manner. The EU has a range of air facilities, both excellent and suspect. Third world countries can rarely if ever provide even minimal standards of care and inspection for air freight.

The Asian market is surely the greatest revenue generator in the air cargo industry. The growth rate of goods shipped by air from China and the Pacific Rim is staggering, with no end to that growth in sight. Every air freight carrier and every commercial passenger airline is embroiled in getting a market share. The more encumbered air cargo becomes by inspection requirements, the slower it becomes. There is a delicate balance between what a shipper is willing to pay to move goods and the options he has to alter his supply chain and modality. Speed is a value proposition for air freight; however with the complex interconnection between modalities that exist today, switching from purely air to a sea/air or sea/land combination is possible. Price is always an issue, but with the fluctuations in fuel costs and the possible implementation

of security processes, airlines are sensitive to the balancing of freight rates with these potential new expenditures in mind. The higher cost of inspection combined with the possible operational slowdowns due to security requirements could cost shippers more than they are willing to spend. The new developments in sea freight and dedicated sea-lanes, combined with the faster speed of sea cargo, are major concerns to the air industry. At what point do shippers bail out because of cost v. speed considerations?

In spite of what can be seen as slower transit times, the globalization of our supply chain is here to stay and there are basically no choices for some shippers and commodities other than air, regardless of the increases in cost, paperwork, and time, and reductions in schedules. Commodities such as consumer electronics, toys, high-end apparel, and footwear are some of the time- and market-sensitive products that mandate air transport, so despite the pitfalls and increased costs, these items will continue to fly. The higher costs of transit, however, will soon make their way to the market. Since the air cargo industry's infrastructure cannot support the increased security requirements of a changing world, shippers will soon be seeing surcharges on air freight and even higher premiums on smaller shipments. Since many Asian routes are growing faster than predicted, these ship points will soon become choke points as they are obliged to accommodate security procedures, and some shippers may be forced to change modality to get goods to the market. Sailing direct from many Asian ports to the United States can reduce sea times significantly, and the resultant decline in the delivery gap between air cargo and sea/land services will make financial sense to many. The trend in choosing modality is to take account of the fine line between costs and time, and the choice is no longer clear cut.

## CONCLUSIONS

Legislation means different things to different countries. Laws created in the United States have no binding effect elsewhere. Security systems such as background screening for transportation workers (TWIC cards) are excellent ways to know who is handling your cargo, but they do not apply elsewhere. C-TPAT's best practices asks that overseas cargo container stuffers (packers) be vetted to insure compliance with antiterrorist security procedures. This is a fine concept that is all but impossible to guarantee. The Known Shipper program requires a complete background check on volume air shippers to help speed their cargo through the system, but it fails to account for the thousands of consolidators who become the middlemen in logistical moves. Here again, it is a fine concept but easily corrupted by anyone able to infiltrate companies and use their good name as a screen for covert activities. E-manifests have been proposed as a security tool, but because these documents can say anything and are written by the shipper, their use as security components is suspect at best.

Overall, the air cargo industry provides a reliable and cost-effective way to speed goods to market from worldwide points. The industry recognizes its

role in commerce and, like any business, views profitable operation as its main strategy. Given the changing world in which we live and the threats we face to our way of life, we must find a way to mandate changes in industry processes and thereby effectively protect our borders while not disrupting commerce. Vulnerability is the new paradigm for long-term planning in any business, but especially in logistics. It need not take another September 11 to motivate our law makers to act in this regard.

# CHAPTER 10

# Selection and Preemployment Assessment of Aviation Security Screeners

*Diana Hardmeier and Adrian Schwaninger*

For years, terrorist attacks have presented a constant threat to civil aviation and highlighted the importance of aviation security. Threats that have reached new dimensions demand a reliable security check, not only for hold baggage but also for passengers and their carry-on baggage. For example, the terror attack on September 11, 2001, has revealed a new dimension. Former terror attacks were comparable to Lockerbie 1988, when Pan Am Flight 103 was destroyed by a bomb in the hold baggage. As a result, immediate changes regarding hold baggage screening were introduced, and automated systems for detecting improvised explosive devices (IEDs) in hold baggage were developed. However, in the recent past, suicide bombings have become more likely, and therefore enhanced security checks of passengers and their carry-on bags have become necessary.

Although new state-of-the-art technology, such as automatic liquid detectors, millimeter wave systems, X-ray machines with automatic detection of explosive materials, and so forth, facilitate the detection of threat items, the final decision is still made by human operators (screeners). It has been argued that with advances in technology, the cognitive demands on humans are increased rather than lowered.[1]

While procedural and predictable tasks can be carried out by machines, the human operators are still indispensable for tasks that require inference, diagnosis, judgment, and decision making. In aviation security, the human operator is a critical decision maker and probably the most capable and adaptable resource in the system. Above all, now that changes in regulations cannot be anticipated in many cases and have to be implemented within a short period of time (e.g., the liquid regulation after the terror plot in London

2006 was uncovered), the human operator is an essential component of aviation security. Nevertheless, he/she can also be the weakest link if not skilled or trained enough. The challenge in aviation security is to ensure maximum security while keeping the workflow at checkpoints efficient. Moreover, a reliable security check demands sufficient time and human resources, which is sometimes in conflict with the commercial pressure that security companies are facing. In order to increase security and efficiency, relevant factors in the security process should be evaluated by means of a job and further task analysis. Once the job requirements are defined, reliable and valid measures can be developed to increase security and efficiency.

Furthermore, analyses should investigate whether the measured factors relate to relatively stable abilities and aptitudes or to training effects. The more clearly the relationship between abilities, aptitudes, and acquirable knowledge is defined, the better the selection criteria will be. Factors that cannot be trained should be addressed by a preemployment assessment procedure to ensure that only people who have the capabilities needed to fulfill the job requirements are employed.

In this chapter, we describe the main results of various studies of the selection and preemployment assessment of screeners. We start by explaining how a job and task analysis can be applied in order to define the relevant job requirements and further define selection, competency assessment, and training criteria.

## JOB AND TASK ANALYSIS TO DEFINE THE IMPORTANT TASKS AT SECURITY CHECKPOINTS

### Job and Task Analysis

Job and task analytic techniques are useful tools to understand the context in which the human operator's work is taking place. A job and task analysis should be performed primarily in order to identify the important tasks and responsibilities of a specific job.[2] The job and task overview then provides a clear description with which to define the most important tasks. These should further be analyzed by means of a traditional or cognitive task analysis (CTA), depending on the task demands.

The methods that can be used to perform a job or task analysis are similar to each other, and they should be chosen carefully in order to best match the goals. Generally, two data collection techniques can be distinguished: subject- and observation-based techniques.[3] That is, inputs from persons who are familiar with the task can be collected using verbal protocols and questionnaires (subject-based) or experts can be observed on the job (observation-based). Subject-based methods include among others the critical incident technique (CIT), questionnaires, interviews, and verbal protocols. The CIT was developed by John Flannigan and is a widely used method in which critical incidents are reported using questionnaires or interviews. These incidents

involve human behaviors that have critical significance to the task.[4] Activity sampling and observations are observation-based data collection techniques. Activity sampling is a method that collects information about the time spent on employees' activities. Therefore, a large number of observations are made over a period of time.[5] It is also suggested that observations and unstructured interviews are best used as part of a preliminary task analysis.[6] The data analysis should also be in line with the goals and match the data collection. Results can be visualized with charts, summarized using statistical methods, or presented in a verbal report.

## Job and Task Analysis at the Security Checkpoint: An Example

In this section we report a primary job and task analysis in the field of aviation security as an example. At Zurich Airport there are three areas/workplaces: cabin baggage screening (CBS), hold baggage screening (HBS) and cargo screening. All screeners are assigned to one workplace only. Because of the separated workplaces and slightly varying tasks, CBS and HBS were examined separately in order to identify the primary job tasks. For cargo screening, no job analysis was performed. In this chapter we report our findings for CBS only.

The major task of aviation security screeners is a reliable security check of passengers and passenger bags to ensure that no threat items or dangerous goods are brought into the security restricted area or on board the aircraft. Furthermore, this check should be done as efficiently and in as customer-friendly a way as possible. For the job analysis in CBS, a subject- and observation-based data collection method was chosen. That is, inputs from persons who were familiar with the task were collected, and observation methods were applied by professionals. First, professionals observed aviation security screeners at their workstation. Further, unstructured interviews with screeners were conducted regarding the primary tasks they have to fulfill. Based on these inputs the security check can be reported as follows.

As can be seen in Figure 10.1, the security check of passengers and their carry-on bags is conducted by a crew that consists of four to six screeners. Each screener works at an assigned position for a defined period of time. Normally after 20 to 30 minutes, positions are changed. Each position is linked to a specific task. Besides the body and baggage check, X-ray screening of passenger bags (see Figure 10.1, position 2) is one of the most important tasks at the checkpoint, since missing a threat item in a passenger bag could have terrible consequences. Note that if a screener is not effective in the visual inspection of X-ray images and therefore sends too many harmless bags to be hand-searched, long waiting lines at the checkpoint will occur. Many objects look quite different in X-ray images than in reality. Thus, for the screening process, visual abilities and knowledge of the visual appearance of threat items in X-ray images could be assumed to be rather important determinants in achieving a certain level of security without sacrificing efficiency in

**Figure 10.1**
**Elements of Passenger Screening**


X-ray screening. If the screener decides that a piece of baggage has to be hand searched, another screener (see Figure10.1, position 3) is responsible for hand searching the bag.

For this task, language and communication skills are needed, because screeners have to ask the passenger whether they can manually inspect the bag and sometimes communicate with the passenger to find out what certain items are used for. In addition, the conversation with the passenger can provide information on whether the passenger and/or the bag might be a threat. Passengers could also try to bring prohibited items into the security restricted area and the airplane by wearing them on their body. Therefore, at minimum one female and one male screener are responsible for the body check (Figure10.1, position 4). At Zurich Airport, the body check is done by means of a metal detector and sometimes an additional manual body search. In coming years, this manual body search might be replaced by new technology (e.g., millimeter wave systems). Millimeter wave technology allows the scanning of people for the presence of threat objects. As clothing and other organic materials are translucent, an image of the passenger can be provided, which can then be interpreted. Whether this body search is done manually or using millimeter wave systems, specific abilities should be considered for both approaches.

Another position is in front of the X-ray machine (Figure 10.1, position 1). The assigned screener has the responsibility to inform passengers about the security check and place their bags on the belt. This is done by the screener to ensure that terrorists cannot place the bag on the belt in a way that would make it more difficult to detect a threat item (for example, because it would reappear in a difficult view in the X-ray image (Figure 10.3, for which see

below, will provide an example). In addition, this procedure ensures also that the distance between two bags is large enough and thus enough time is provided to the operator who has to interpret the X-ray image.

For nearly all positions in the CBS area, dealing with passengers is important. As a result, communication between aviation security screeners and passengers can be assumed to play a key role in ensuring an efficient workflow. Hence, language and communication skills as well as customer service skills were defined as basic job requirements. Moreover, a crew always consists of several screeners who have to work as an efficient team, not only during normal operations but especially in stressful situations. This factor becomes even more important taking into consideration the fact that screeners are randomly assigned to a crew and especially at bigger airports do not know each other very well. Furthermore, passengers are often not pleased to have to pass through security control, and therefore screeners have to be very patient and need the ability to cope with negative feedback even if they do their job very well.

In summary, the job analysis revealed X-ray screening, baggage search, body search, dealing with passengers, teamwork, and coping with negative feedback to be important for airport security screeners working in the CBS area.

## COGNITIVE TASK ANALYSIS IN X-RAY SCREENING

Based on the job analysis, the abilities, aptitudes, and knowledge that are needed to perform the tasks proficiently should be identified. Depending on the task, a traditional (behavioral) task analysis or a cognitive task analysis (CTA) can be applied. Whereas the traditional task analysis focuses mainly on noncritical procedural tasks, the CTA identifies and describes cognitive elements, processes such as decision making, problem solving, and so on, as well as the knowledge and skills that are required for similar job components.[7] Behavioral task analysis describes the task in terms of time spent, criticality, and frequency.[8] In contrast, CTA should be used for-high performance tasks that require large amounts of knowledge or information, significant decision making or problem solving, heavy workload or time pressure, multitasking, situations that change substantially, or considerable amounts of teamwork. Generally, these cognitive processes are more difficult to study because they are not directly observable. Traditional task analysis and CTA can also be used as complementary tools. Usually traditional task analyses are used to specify the basic job tasks and precede the CTA.

Quite often a CTA includes a comparison of novices and experts, to find out which skills and knowledge are domain specific.[9] These findings can help to identify selection criteria for required skills and define the training sessions needed to acquire job specific knowledge and procedures.

CTAs can be conducted using either research or operational methods. Although research methods are often considered too complex and time consuming in operational settings, they can be very useful if the field of application is

very broad and relatively unknown. The methods used to collect and analyze the data are the same as described above for the job and task analysis. The results of the analysis can then be implemented within a few weeks or months.[10] The final report should provide a clear description of the CTA. This should include the objective of the CTA, job description, analyzed tasks, participant selection, materials and procedures used for data collection, data analyses, results, and conclusion.

As an example, we performed a CTA for the X-ray screening task, which is considered to be one of the most important tasks at airport security checkpoints. First, a primary data collection was conducted, to describe the cognitive structures and processes underlying the X-ray screening task. Based on this information, data collection and analysis were performed using various research methods. As the job analysis was previously reported, we focus here on the description of the CTA.

### Primary Data Collection Regarding the X-Ray Screening Task

Often, screeners have only a few seconds to decide whether an X-ray image of a passenger bag contains a threat item or not. At security checkpoints it is of the utmost importance that threat items can be detected quickly and reliably without sacrificing efficiency. If too many bags are wrongly judged as not "OK" and have to be hand searched, long waiting lines at checkpoints can be the result. The X-ray screening task demands a knowledge of which items are prohibited and what they look like in X-ray images, certain visual cognition abilities, decision making, and often multitasking under time constraints. Because of these factors, a CTA is recommended. The CTA presented here focuses on the visual inspection task only.

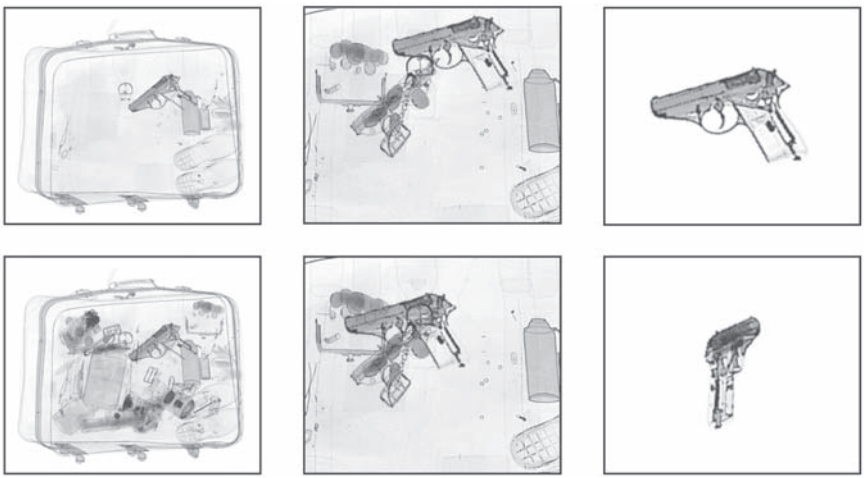
In a first step, unstructured interviews, verbal reports, and observations were conducted for the primary data collection. The results of these data collection techniques as well as theories from basic research studies in object recognition allowed us to assume that the screening process involves both knowledge-based and image-based factors.

Knowledge-based factors include which items are prohibited and what they look like in X-ray images.[11] Often X-rayed objects like the electric shock device depicted in the left image in Figure 10.2 look quite different than they do in reality. Certain threat items look like harmless objects but are in fact threat items that are not allowed on board an airplane (see, for example, the knife in the center image of Figure 10.2). Other objects, like the improvised explosive devices (IEDs) in the right image of Figure 10.2, are normally not seen at checkpoints and are therefore more difficult for screeners to recognize if they have not received appropriate training.

It has been pointed out that bag complexity, superimposition, and viewpoint of threat items in X-ray images can influence detection performance (see Figure 10.3 for examples).[12] The detection of a gun becomes more dif-

**Figure 10.2**
**Prohibited Items (I)**

**Figure 10.3**
**Prohibited Items (II)**



ficult if there are many other objects in the bag that distract attention from it (high bag complexity). If other objects in the bag are superimposed on the gun or if it is shown in an unusual view, detection also becomes more difficult. These have been defined as image-based factors in X-ray screening.[13] Bag complexity, superposition, and the viewpoint of threat items are related to visual cognition processes such as visual search, figure-ground segregation, and mental rotation. Visual search studies have revealed that it becomes harder to detect a target object if many objects are presented within a scene.[14] Detection is more difficult if other objects are superimposed on the target object and relevant components are not visible.[15] Finally, viewpoint-dependent theories in object recognition predict the systematic effects of viewpoint and

familiarity.[16] The term "canonical" refers to the viewpoint that is easiest to recognize.[17] This is related to the number and diagnosticity of the features that are visible but also to how often an object is encountered in a certain view. Different views of an object can be stored in visual memory to facilitate recognition despite changes in viewpoint. However, people with good mental rotation abilities are probably more able than others to detect a prohibited item when it is shown in a rotated view that they have not seen before.

In state-of-the art X-ray screening equipment, different materials in X-ray images (organic, metallic materials, etc.) are coded using different colors. Therefore, it can be assumed that a color vision deficiency can impair the task of interpreting the X-ray image. There are different kinds of color deficiencies that are genetically determined. The most common form is the red/green color blindness, which occurs in about 8 percent to 12 percent of males and about 0.5 percent of females.[18]

## Materials and Procedure

### *Knowledge-based Factors*

An important factor in the X-ray screening task is knowledge of which items are not allowed in the security restricted area and what they look like in X-ray images. To measure whether such knowledge-based factors could in fact be improved with on-the-job experience or specific training, the X-Ray Prohibited Items Test (X-Ray PIT) was developed. This test includes all kinds of prohibited items according to international prohibited items lists (EU, ECAC, ICAO). To keep the image-based factors relatively constant, all items are shown in the easy view in bags of medium complexity with medium superposition by other objects. In the X-Ray PIT a total of 160 trials are shown to participants; 80 of the images are harmless bags (i.e., without any prohibited item). Each image is shown for 10 seconds on the screen. For each X-ray image, participants have to decide whether the bag is OK (no prohibited item contained) or NOT OK (the bag contains a prohibited item) by clicking on the appropriate button on the screen. Participants also have to indicate to which category the prohibited item(s) belong(s) and how sure they are in their decision. More information about this test and its reliability and validity measures can be found in Hardmeier, Hofer, and Schwaninger (2006).[19]

### *Image-based Factors*

The X-Ray Object Recognition Test (X-Ray ORT) was developed in order to measure how well people can cope with the effects of viewpoint, superposition by other objects, and bag complexity. This test includes a total of 256 X-ray images of passenger bags. In this test, only guns and knives, object shapes that are well known by novices, are shown. All the X-ray images are displayed in grayscale, as the meaning of color in X-ray images is not known by novices.

All three image-based factors in the test are varied systematically. A total of eight different guns and eight different knives are used. All of them are shown in an easy and rotated view. Each of these items is then placed in a bag, once in a bag with high complexity level and once in a bag with low complexity level, that is in a bag with high superposition by other items and in a bag with low superposition by other items. Thus, all the factors are combined with each other and each threat item is shown once in each possible combination. The X-Ray ORT is a computer-based test that is very easy to use. Test participants receive a short introduction that explains the test, as well as some exercise trials to familiarize them with the test-taking procedure. In order to ensure that the object shapes are known, all the guns and all the knives are shown for 10 seconds on the screen before the test starts either in the frontal or in the rotated view. All images are displayed for four seconds only on the screen. For each X-ray image, participants have to indicate whether the bag is OK (i.e., it contains no gun and no knife) or NOT OK (i.e., it contains a gun or a knife), by clicking on the appropriate button on the screen. Additionally, participants have to indicate how sure they are in their decision, by using a slider control.[20] The test itself is subdivided into four parts, and after each part participants can take a short break if desired.

### *Procedure*

To investigate whether knowledge-based and image-based factors can be distinguished, the detection performance of experts and novices was compared in the X-Ray PIT (rather knowledge-based factors) and the X-Ray ORT (image-based factors). There was an expectation of larger differences between the groups for the X-Ray PIT because the knowledge of which items are prohibited and what they look like in passenger bags has to be acquired through experience and training.[21] As explained above, the X-Ray ORT is assumed to measure how well someone can cope with image-based factors such as the effects of viewpoint, superposition, and bag complexity. Schwaninger and colleagues assumed such abilities to be relatively independent of training and experience. To test these hypotheses, the detection performance in both tests of aviation security screeners was compared with the detection performance of novices. Then, the performance of aviation security screeners in both tests was compared before and after two years of individually adaptive computer-based training (CBT). Further, correlations between the X-Ray ORT (representing on-the-job performance) and the PIT (representing theoretical knowledge) were compared. Finally, the detection performance of screeners who were employed using the X-Ray ORT as a preemployment assessment tool and screeners who were employed without using the X-Ray ORT was compared.

## Participants

The results that are going to be presented here are based on 453 aviation security screeners aged between 24 and 65 years ($M$ = 48.94 years, $SD$ = 9.09

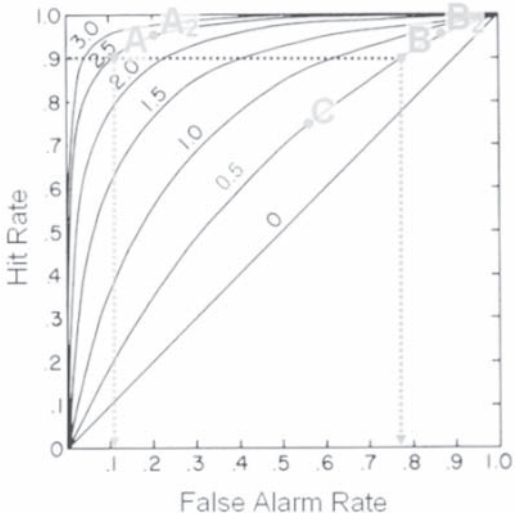
years). A total of 134 novices aged between 21 and 26 years ($M$ = 23.24, $SD$ = 1.22) and 101 job applicants aged between 19 and 55 years ($M$ = 35.25, $SD$ = 9.79) who were employed using the X-Ray ORT as a preemployment assessment tool were tested. Depending on the analysis, the sample size had to be adjusted.

### Data analysis

Signal detection provides valid measures of the detection performance of screeners, taking the hit rate and the false alarm rate into account.[22] A hit is a correctly identified threat item, whereas sending a harmless bag to be hand searched is called a false alarm. Missing a threat item is defined as a miss and a correctly identifying a harmless bag is called correct rejection.

Figure 10.4 shows why the hit rate alone is not a valid detection performance measure. For example, screener B in Figure 10.4 reaches a hit rate of 90 percent by simply judging most bags as NOT OK. This becomes apparent when considering his false alarm rate, which is nearly 80 percent. In contrast, screener A reaches the same hit rate, but with a very low false alarm rate (about 10 percent). Thus, screener A achieves a high level of security without sacrificing efficiency. The detection performance measures d' and A' take the hit and false alarm rate into account. The outcome d' equals z(pHit)—z(pFA alarm), whereas pHit refers to the hit rate, pFA to the false alarm rate, and z to the z-transformation (see Green and Swets 1966).[23] The outcome d' of screeners is related to the receiver operating characteristics (ROC) curves that can be seen in Figure 10.4. These curves show how the hit rate of a screener

**Figure 10.4**
**Hit Rate and False Alarm Rate**



changes as a function of changes in the false alarm rate. As an example, d' of screener A with 2.5 is much higher than d' of screener B with 0.5. The detection performance measure d' is assumed to be independent of subjective response bias.

The response bias can vary depending on the personality of the screeners, the subjective and objective costs and benefits of the response, target prevalence (i.e., how often threat items occur), and other factors. As a consequence, the response bias can change quickly, while changes of d' require much more time and are related to the selection and training of security screeners. A terrorist attack would result in an immediate change of the response bias, but d' scores would remain relatively unaffected according to signal detection theory. This is illustrated in Figure 10.4 for screeners A and B. Both of them would immediately send more bags to be hand searched (judged as "NOT OK") after a terrorist attack. This would result in higher hit rates but also higher false alarm rates. Thus, while screeners change their position on their ROC curve (change in response bias), they remain on the same curve (their d' remains the same). In order to create a basis of comparison, all results in this chapter are calculated using d'.

## Results

### *Effect of Experience and Training on Knowledge- and Image-based Factors*

In order to examine whether experience affects knowledge-based and image-based factors, previous tests looked at the detection performance of experienced aviation security screeners and novices in the X-Ray PIT and the X-Ray ORT.[24] The results showed that detection performance differed remarkably between experts and novices in the X-Ray PIT, but only little in the X-Ray ORT. This difference becomes even more evident if the relative difference between experts and novices is computed using the following formula:

$$\frac{DetectionPerformance_{Experts} - DetectionPerformance_{Novices}}{DetectionPerformance_{Novices}}$$

As can be seen in Figure 10.5a, the percentage difference between experienced screeners and novices was 94 percent in the X-Ray PIT and only 31 percent in the X-Ray ORT. A detailed analysis for image-based factors revealed that the detection performance decreased significantly if threat items were shown in close-packed bags, had other items in the bag superimposed on them, or were shown in an unusual view (see Figure 10.5b and 10–5c). Although experienced screeners perform at a higher level than novices, large differences in terms of viewpoint, superposition, and bag complexity were

found among individual screeners, whether they were experienced or novices. For both groups, large differences between individuals were found as indicated by the standard deviations in Figure 10.5b and 10.5c.

In summary, it was found that experience results in better detection performance in the X-Ray PIT, which measures whether screeners know which items are prohibited and what they look like in X-ray images (knowledge-based factors). In contrast, experience does not result in large increases in the X-Ray ORT, which rather measures the visual abilities needed to cope with image-based factors such as viewpoint, superposition, and bag complexity.

Several scientific studies have shown that computer-based training can be a powerful tool to increase the X-ray image interpretation competency of screeners.[25] First, some threat items are very rarely encountered at checkpoints (e.g., bombs). Second, other prohibited items look quite different in the X-ray image than in reality (e.g., the electric shock device in Figure 10.2). An individually adaptive training system that includes all kinds of prohibited items in different views investigated whether such training (20 minutes twice a week) affects knowledge-based and image-based factors differently.[26]

As can be seen in Figure 10.6a, the detection performance of experienced but untrained aviation security screeners (first measurement) is generally lower than the performance of trained screeners (second measurement) in both tests. Further, detection performance increase was higher for the X-Ray PIT than for the X-Ray ORT. The relative difference for the X-Ray PIT was 85.0 percent, but it was only 22.7 percent for the X-Ray ORT (see Figure 10.6b).

**Figure 10.5**
**Differences in Detection Performance**

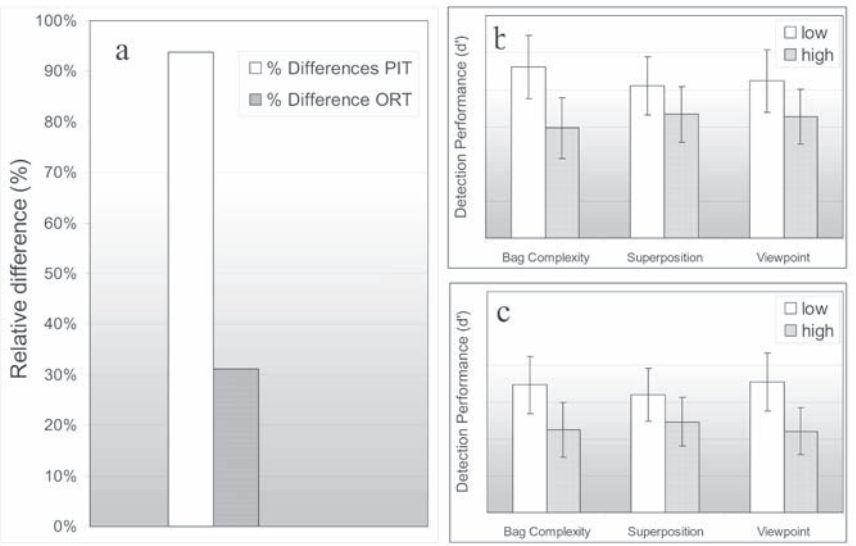
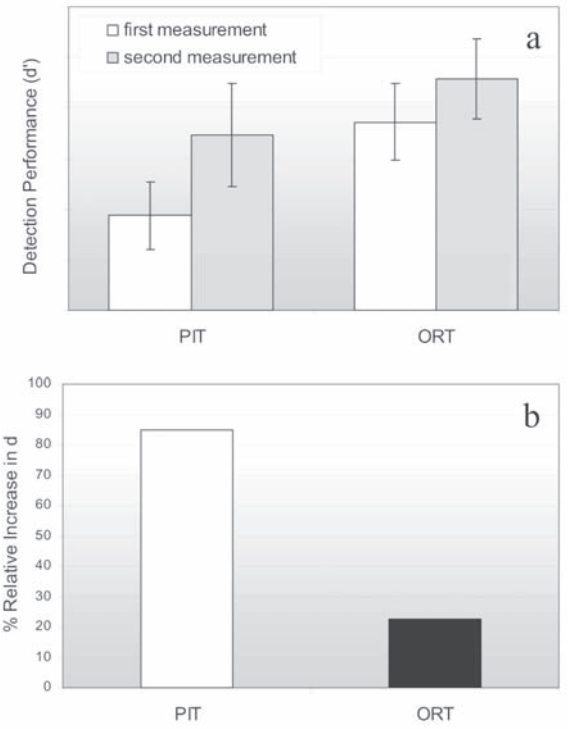


**Figure 10.6**
**Improvements in Detection Performance**




Thus, an individually adaptive CBT can strongly increase the knowledge of which items are prohibited and what they look like in X-ray images and result in better detection performance of screeners. In contrast, the abilities to cope with image-based factors such as viewpoint, superposition, and bag complexity are influenced by training only to a limited extent. Therefore, it could be valuable to use a test such as the X-Ray ORT as part of the preemployment assessment procedure, in order to select people who have the visual abilities to cope with the image-based factors needed in X-ray screening.

### *The X-Ray ORT as Preemployment Assessment Tool*

The rather small difference in the X-Ray ORT between novices and experienced aviation security screeners as well as between trained screeners and those who are experienced but not trained supports the assumption that this test measures relatively stable visual abilities needed in X-ray screening. Compared to knowledge-based factors, these abilities can only be increased to a limited amount through experience and training. Therefore, the X-Ray ORT could be a useful instrument for preemployment assessment purposes. Before applying

this test to job applicants, the X-Ray ORT was validated.[27] A medium correlation between both X-ray screening tests was expected as both tests deal with X-ray images. The X-Ray PIT measures mainly the knowledge of prohibited items in X-ray images, as image-based factors were kept relatively constant.

Nevertheless, in the X-Ray PIT image-based factors play along as well. However, the CBQ, which is a multiple-choice test about airport-specific issues and procedures at airports should show a lower correlation with the X-Ray ORT. Further, test results in the X-Ray ORT were correlated with TIP data. TIP is a technology that allows us to measure detection performance on the job by projecting fictional threat items into real passenger bags. After each TIP image, screeners receive a feedback message that a fictional threat item was present. TIP data for 86 aviation security screeners were aggregated over a period of 17 months.

If the ability to cope with image-based factors is in fact important for the X-ray screening task, screeners with high ability should also show a better detection performance on the job. Indeed, there was a rather high correlation ($r = .62$) between the X-Ray ORT and the X-Ray PIT (see Figure 10.7a). As expected, there was only a small correlation between the detection of prohibited items in X-ray images and theoretical knowledge of airport-specific issues ($r = .25$), which was measured with the CBQ, a multiple-choice test (Figure 10.7b). Regarding TIP data, a medium to high correlation ($r = .51$) between detection performance in the X-Ray ORT and on-the-job performance was found (Figure 10.7c).

Based on these results, it was concluded that the X-Ray ORT is a valid instrument that can account for a part of the detection performance variability and therefore should be used as a preemployment assessment tool to select job applicants.[28] A total of 101 job applicants who passed the preemployment assessment successfully were employed as aviation security screeners. All of them had to reach a defined score in the X-Ray ORT, was above the average detection performance level. Further, job applicants had to pass the color blindness test, an English and German language test, a physical examination, and a job interview. Whether the X-Ray ORT in fact helps to improve the detection performance of aviation security screeners later on the job was also investigated.[29] The detection performance in the X-Ray PIT of screeners

**Figure 10.7**
**Performance Clusters**

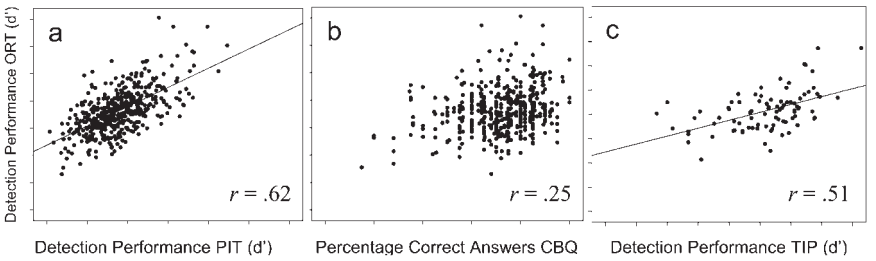
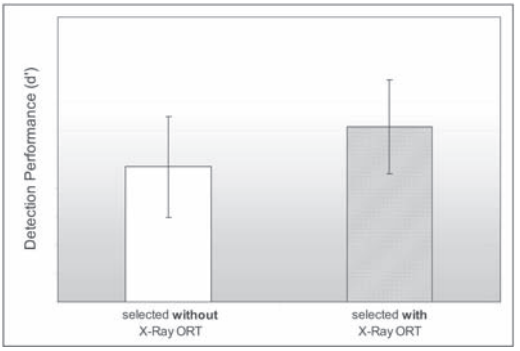


**Figure 10.8**
**X-Ray ORT Impact**




who were employed with the X-Ray ORT and the performance of screeners who were employed without the X-Ray ORT were compared. Screeners who were not employed using the X-Ray ORT had working experience of between 2 and 26 years ($M$ = 9.71, $SD$ = 5.50 years). Screeners who were all hired as aviation security screeners based on the test results in the X-Ray ORT had a maximum of one year of working experience when taking the X-Ray PIT. The results show a significant difference between these two groups in terms of their performance measure d' (see Figure 10.8). Thus, if the X-Ray ORT was used as an additional selection criterion as part of the preemployment assessment procedure, detection performance measured one year later using the X-Ray PIT was increased significantly.

## CONCLUSION

All results support the assumption that image- and knowledge-based factors are important determinants in the X-ray screening task. The hypothesis that image-based factors (bag complexity, superposition, viewpoint) are related to visual abilities that are not very dependent on experience and training was verified. The detection performance decreased with increasing bag complexity, superposition, and unusual viewpoint of threat items for experienced and trained aviation security screeners as well as for novices. Further, large individual differences within all three groups could be found.

That means that there are large differences between people in their ability to cope with image-based factors, and these differences are still evident after weekly recurrent computer-based training over several months. Further analyses could show that results in the X-Ray ORT correlates with the detection performance in the X-Ray PIT and above all with TIP data, a measure of operational performance. Therefore, the ability to cope with image-based factors should be defined as a basic job requirement and be measured within a preemployment assessment procedure. Whether detection performance can

in fact be increased using the X-Ray ORT as a preemployment assessment tool was investigated in a second step. The results showed that screeners who were selected with the X-Ray ORT showed a significantly better detection performance after one year of employment compared to screeners who were not hired using the X-Ray ORT. Besides the ability to cope with image-based factors, the knowledge of the visual appearance of threat items is essential. In comparison with experienced aviation security screeners, novices showed a poor performance in detecting prohibited items in X-ray images of passenger bags. Thus, the knowledge of what threat items look like can be learned with experience and on-the-job training. A follow-up study found that individually adaptive computer-based training can substantially increase the detection performance of aviation security screeners that is related to knowledge-based factors, that is, they show better knowledge of which items are prohibited and what they look like in X-ray images of passenger bags.

### General Discussion

This chapter could show how useful a task and cognitive task analysis is in understanding a specific task like X-ray screening. The task analysis revealed that the job of an aviation security screener includes various tasks that should be taken into account when job applicants are employed. Besides X-ray screening, baggage and body search, dealing with passengers, teamwork, and coping with negative feedback were found to be important for screeners working in the CBS area. Similar requirements could be found for the HBS area. A CTA was performed for the X-ray screening task, which is supposed to be one of the most important tasks at security checkpoints.

As could be seen, X-ray screening includes various factors that should be taken into account when employing and training aviation security screeners. Whereas knowledge-based factors should be taken care of through training, the cognitive abilities needed to cope with image-based factors in X-ray screening, such as viewpoint, superposition, and bag complexity, should be tested as part of a preemployment assessment procedure. The X-Ray ORT is a reliable and valid instrument to measure the ability to cope with bag complexity, superposition, and rotation of threat items (effect of viewpoint) in X-ray images. Further studies should clarify whether the remaining defined tasks, such as baggage and body search, dealing with passengers, teamwork, and coping with negative feedback, are more related to abilities and have to be clarified within a preemployment assessment or can be learned on the job.

## ACKNOWLEDGMENT

This research was financially supported by the European Commission Leonardo da Vinci Programme (VIA Project, DE/06/C/F/TH-80403). This chapter is a summary of Work Package 5: Pre-employment assessment tests. For more information, see www.viaproject.eu.

## NOTES

1. William C. Howell and Nancy J. Cooke, "Training the Human Information Processor: A Look at Cognitive Models," in *Training and Development in Work Organizations: Frontiers of Industrial and Organizational Psychology*, ed. Irwin L. Goldstein, 121–82 (San Francisco,: Jossey-Bass, 1989).

2. Thomas L. Seamster, Richard E. Redding, and George L. Kaempf, *Applied Cognitive Task Analysis in Aviation* (Aldershot, England: Avebury Aviation, 1997), 29, 233.

3. Barry Kirwan and Les K. Ainsworth, *A guide to Task Analysis* (London: Taylor & Francis, 1992), 35.

4. David H. Jonassen, Wallace H. Hannum, and Martin Tessmer, *Handbook of Task Analysis Procedures* (New York: Praeger, 1989).

5. Thomas L. Seamster, Richard E. Redding, and George L. Kaempf, *Applied Cognitive Task Analysis in Aviation* (Aldershot, England: Avebury Aviation, 1997).

6. Ibid.

7. Ibid.

8. Ibid.

9. Ibid.

10. Ibid.

11. Adrian Schwaninger, Diana Hardmeier, and Franziska Hofer, "Aviation Security Screeners' Visual Abilities and Visual Knowledge Measurement," *IEEE Aerospace and Electronic Systems* 20 (2005): 29–35.

12. A. Schwaninger, Evaluation and Selection of Airport Security Screeners," *AIRPORT*, February 2003, 14–15.

13. Schwaninger, Hardmeier, and Hofer, "Aviation Security Screeners' Visual Abilities and Visual Knowledge Measurement," 29–35.

14. Jeremy M. Wolfe, "Visual Search in Continuous, Naturalistic Stimuli," *Vision Research* 34 (1994): 1187–95.

15. Stephen E. Palmer, *Vision Science—Photons to Phenomenology* (Cambridge, MA: MIT Press, 1999).

16. Michael J. Tarr and Heinrich H. Bülthoff, *Object Recognition in Man, Monkey and Machine* (Cambridge, MA: MIT Press, 1998).

17. Stephen E. Palmer, Eleanor Rosch, and Paul Chase, "Canonical Perspective and the Perception of Objects," in *Attention and Performance IX*, ed. John Long and Alan Baddeley (Hillsdale, NJ: Erlbaum, 1981), 135–52.

18. There is no treatment for color vision deficiencies, since they are caused by missing or incorrect visual pigments. The genetically determined red–green color blindness affects men much more often than women, because the genes for the red and green color receptors are located on the X chromosome, of which men have only one and women have two. Thus, males are redgreen color blind if their single X chromosome is defective. Women are color blind only if both X chromosomes are defective.

19. Diana Hardmeier, Franziska Hofer, and Adrian Schwaninger, "Increased Detection Performance in Airport Security Screening Using the X-Ray ORT as Pre-Employment Assessment Tool," in *Proceedings of the 2nd International Conference on Research in Air Transportation, ICRAT 2006, Belgrade, Serbia and Montenegro, June 24–28* (Geneva, Switzerland: ICRAT, 2006): 393–97.

20. For the analysis of detection performance only OK and NOT OK responses were taken into account.

21. Schwaninger, Hardmeier, and Hofer, "Aviation Security Screeners' Visual Abilities and Visual Knowledge Measurement," 29–35.

22. David M. Green and John A. Swets, *Signal Detection Theory and Psychophysics* (New York: Wiley, 1966).

23. Ibid.

24. Schwaninger, Hardmeier and Hofer, "Aviation Security Screeners' Visual Abilities and Visual Knowledge Measurement," 29–35.

25. A. Schwaninger, F. Hofer, and O. E. Wetter. "Adaptive Computer-Based Training Increases on the Job Performance of X-Ray Screeners," *Proceedings of the 41st Carnahan Conference on Security Technology*, Ottawa, October 8–11 (Ottawa: Carnahan, 2007).

26. Adrian Schwaninger, "Training of Airport Security Screeners," *AIRPORT*, May 2003, 11–13.

27. Schwaninger, Hardmeier and Hofer, "Aviation Security Screeners' Visual Abilities and Visual Knowledge Measurement," 29–35.

28. Ibid.

29. Ibid.

# CHAPTER 11

# Terminal Insecurity: A Photo Essay

*Ross Rudesch Harley*

Every day, close to 2 million passengers are screened, sorted, and processed in U.S. airports. According to the Airports Council International, annual global passenger figures for 2006 continued to increase, despite the difficulties and inconveniences associated with post–September 11 security measures:

- 4.4 billion passengers used the world's airports
- 85 million tonnes of cargo were shipped through airports
- 74 million aircraft movements were recorded
- $US38 billion were spent by the world's airports on development
- 4.5 million people were employed at airports globally

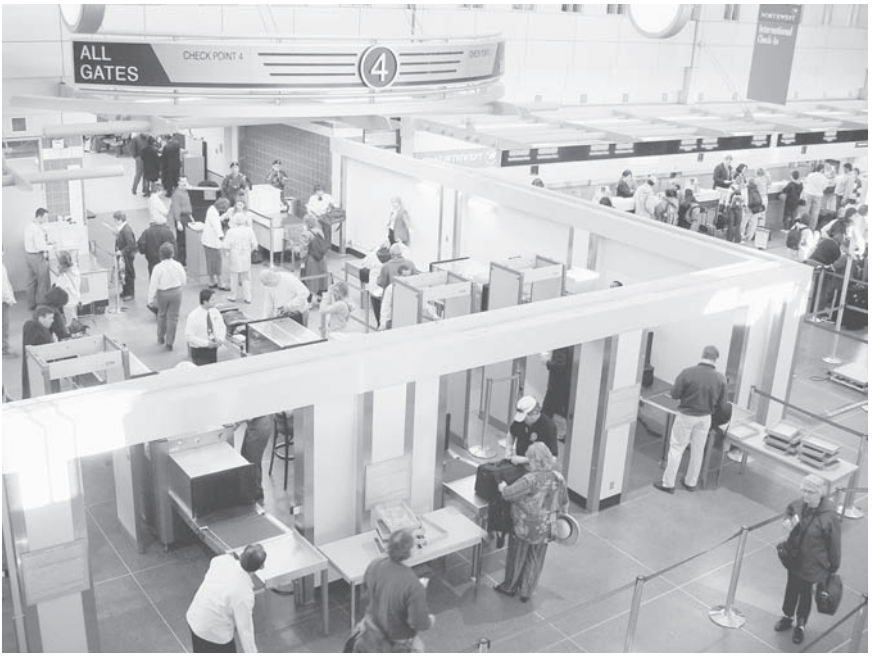
Many of these resources are devoted to preventing harm to aircraft, passengers, and crew by placing special emphasis on the potential for insecurities in the design and management of air terminals. In this way, the global nature of the "War on Terror" is embedded in the porous architecture of the airport, where the automation of security at these "weak points" creates suspects of us all. Suspicion is everywhere enacted in the long lines that wind their way past new inspection machines and screeners. The right to fly now requires a willingness to demonstrate one's innocence before a labyrinth of machines, screenings, and modern rites of passage that monitor, confirm, and deny our global identities.


Modern air travel.

During 2006 the Transportation Security Administration (TSA) screened the following:

708,400,522 passengers
(Average wait time 3.79 minutes; average peak wait time 11.76 minutes)
535,020,271 individual pieces of checked luggage
13,709,211 prohibited items at security checkpoints
(11,616,249 lighters and 1,607,100 knives)

What does it mean to be a suspect in this network, and how is suspicion organized into spatial forms and technological practice? The primary threat of devastating terrorist activity comes in the shape of camouflaged "nodes" or "cells" that may operate undetected within the global network itself. Unseen terrorists are conceived of as using global infrastructures of information to communicate and plan deadly attacks. Appearances are deceiving. An everyday object (a parked car, a bottle of water, an iPod, or a bag of trash) may not

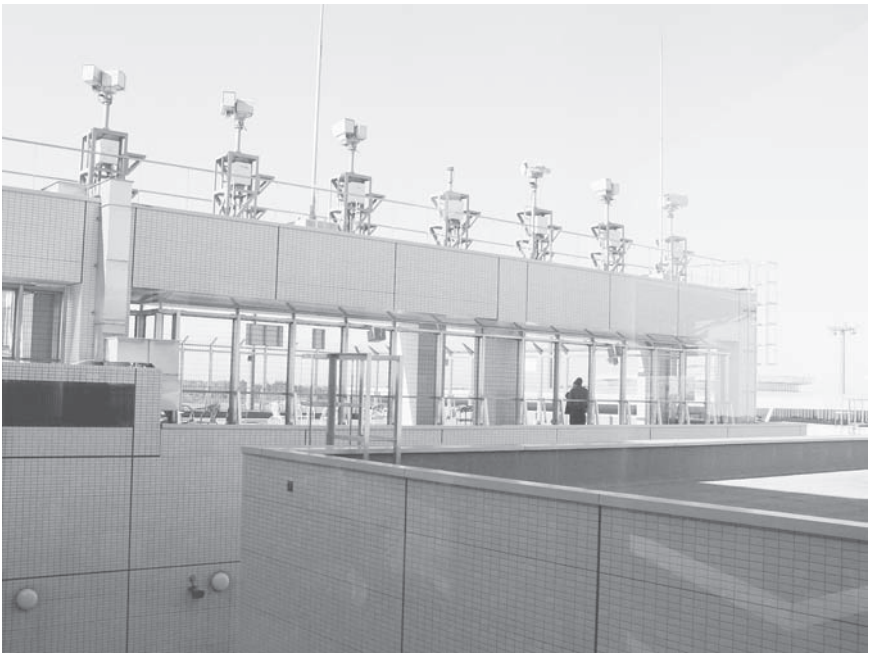



The security regimen.

Perimeter security.


The secure area.

Suspicion reigns.



Big brother.

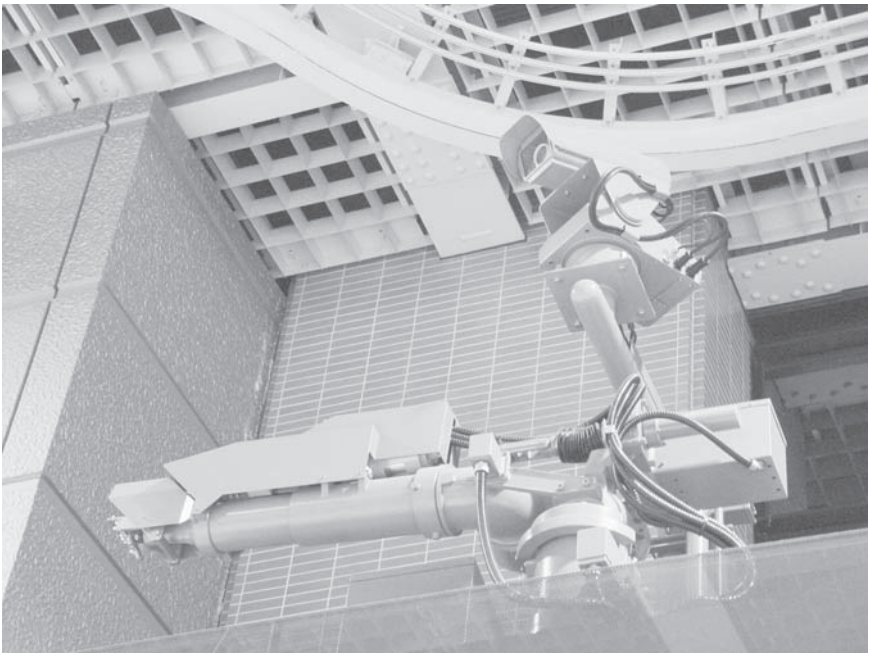
be what it seems. Hence the official response, "It takes a network to fight this network," which is to say that we cannot manage this threat without the aid of information tech nologies designed to detect all manner of irregularities and suspicious activities. The new screening technologies designed and implemented under the rubric of managing risk and increasing passenger and worker safety highlight our insecurities in order to guarantee increased layers of "protection."

This layered approach is a deliberate strategy to further scrutinize passengers and things for potential breach or threat. Layers of information gathered before flights are added to physical, visual, and behavioral inspections of the multitudes who proceed through the terminal to the air. Through the daily use of inventions such as the Threat Image Projection (TIP) software program, security officers are routinely tested on their ability to detect weapons and explosives by X-ray. Other programs such as Secure Flight observe behaviors and activities in the airport environment, checking every passenger manifest against terror watch lists. The implementation of these "stringent" screening technologies is touted as one of the largest civilian undertakings of all time.

Thanks to unprecedented international cooperation among 67 countries, a great majority of the world's air travelers come under a common set of


Prohibited items on display.

security rules for the first time. Central to all such global programs is the impossible dilemma of enforcing security without compromising privacy: the ultimate aim of total surveillance society. In the end it seems to be all about us, the "viewing subjects" who watch thousands of "screenings" around us. The spectacle of guilt observed. The cool mechanical objectivity of information. No one is beyond suspicion or beyond the scope of the layered network of information and its inescapable sequence of checkpoints, thresholds, and bodily checks. We are faced with the grand posture of transparency, hiding beneath the obscene underbelly of Code Orange and Red Alerts.



Closed-circuit everywhere.

Find the camera.

The solitude of travel.

# Federal Efforts to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be Strengthened

April 30, 2007

Congressional Requesters

Recent instances of human stowaways hiding in cargo holds on international flights bound for the United States, and cargo smuggling and theft at foreign cargo facilities, have heightened concern over the security of air cargo by revealing vulnerabilities that could be exploited by terrorists. According to Department of Homeland Security (DHS) officials and air cargo industry stakeholders, terrorists could exploit such vulnerabilities to introduce an explosive device in cargo transported onboard a passenger aircraft, hijack an all-cargo aircraft and use it as a missile, or smuggle a weapon of mass destruction (WMD) in cargo transported on either type of aircraft.[1] While DHS reports that it has no specific intelligence indicating terrorist plans to exploit air cargo vulnerabilities, DHS's National Strategy for Transportation Security identifies cargo aircraft operations and high-volume cargo facilities as aviation assets at significant risk of terrorist attack.[2]

In response to the terrorist attacks of September 11, 2001, the Aviation and Transportation Security Act was enacted in November 2001, which created

1. A weapon of mass destruction could include nuclear, biological, chemical, or radiological devices. For the purposes of this report, the term "weapon of mass destruction" also encompasses weapons of mass effect or scenarios that could result in a great loss of life and destruction.

2. DHS and Department of Transportation, National Strategy for Transportation Security, 2005. Other aviation assets identified as being at significant risk of terrorist attack include passenger aircraft operations, major and midsized airport facilities, general aviation aircraft operations and airports/airfields near major urban areas, and critical national airspace system infrastructure. DHS is required to update its National Strategy for Transportation Security, and planned to update it for submission to Congress by the end of 2006, and every 2 years thereafter. However as of February 2007 it had not been updated.

the Transportation Security Administration (TSA) and required it to provide for the screening of all passengers and property, including cargo, U.S. mail, and carry-on and checked baggage that is transported onboard passenger aircraft.[3] It also required that a system be put into place as soon as practicable to screen, inspect, or otherwise ensure the security of cargo transported on all-cargo aircraft.[4] The act applies to air cargo transported into the United States from foreign countries onboard passenger and all-cargo aircraft, as well as cargo transported domestically and out of the United States to a foreign location on these aircraft.

Within DHS, two agencies have responsibilities related to the security of air cargo bound for the United States from a foreign country, referred to as inbound air cargo.[5] TSA has primary responsibility for securing U.S.-bound flights from destruction or hijacking, and as a result, is primarily concerned with preventing the illicit loading of explosives or stowaways onto aircraft prior to departure for the United States. TSA enforces statutory and regulatory requirements on passenger and all-cargo air carriers to secure air cargo bound for the United States. Both domestic air carriers and foreign air carriers with service to the United States are responsible for implementing security requirements, such as inspecting a portion of air cargo transported to the United States, in accordance with the applicable laws, TSA regulations, security directives, emergency amendments, and security programs. DHS's U.S. Customs and Border Protection (CBP) has primary responsibility for preventing terrorists and implements of terrorism from entering the United States. Specifically, CBP screens and inspects international air cargo upon its arrival in the United States to ensure that cargo entering the country complies with applicable laws and does not pose a security risk.[6] CBP's efforts include analyzing information on cargo shipments to identify high-risk air cargo arriving in the United States that may contain terrorists or weapons of

3. Aviation and Transportation Security Act, Pub. L. No. 107–71, 115 Stat. 597 (2001). See 49 U.S.C. §§ 114(a), 44901(a).

4. The terms "inspecting" and "screening" have been used interchangeably by TSA to denote some level of examination of a person or good, which can entail a number of different actions, including manual physical inspections to ensure that cargo does not contain weapons, explosives, or stowaways, or inspections using nonintrusive technologies that do not require the cargo to be opened in order to be inspected. For the purposes of this report, the term "screening" is used when referring to TSA or CBP efforts to apply a filter to analyze cargo related information to identify cargo shipment characteristics or anomalies for security risks. Moreover, for the purposes of this report, we use the term "inspection" to refer only to air carrier, TSA, or CBP efforts to examine air cargo through physical searches and the use of nonintrusive technologies.

5. Cargo transported by air within the United States is referred to as domestic air cargo, and cargo transported by air from the United States to a foreign location is referred to as outbound air cargo.

6. CBP aids in the enforcement of law and regulations of non-DHS agencies. For example, CBP regulates the entry of sugar into the United States (see 7 U.S.C. §§ 3601–04, pertaining to the U.S. Department of Agriculture), assists in the enforcement of the Bank Secrecy Act (see 12 U.S.C. §§ 1951–59, pertaining to the U.S. Department of the Treasury), and aids in the enforcement of regulations related to safety standards for the transportation of hazardous materials (see 49 U.S.C. §§ 5101–28, pertaining to the U.S. Department of Transportation).

mass destruction, commonly known as targeting, and physically inspecting this cargo upon its arrival.[7] According to DHS and industry estimates, only a small percentage of the air cargo that is bound for the United States from a foreign country is inspected by passenger and all-cargo air carriers prior to an aircraft's departure for the United States, and a very small percentage of international air cargo is inspected by CBP officers upon its arrival in the United States.[8] Congress has allocated at least $255 million from fiscal years 2005 through 2007 for the purpose of enhancing the security of air cargo, through such actions as the development and testing of new and existing inspection technologies. Further, several laws have required TSA to take additional steps to secure domestic, outbound, and inbound air cargo. For example, the Department of Homeland Security Appropriations Act of 2005 required the Secretary to amend security directives and programs to, at a minimum, triple the percentage of cargo inspected on passenger aircraft.[9] In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 required, among other things, that TSA develop technology to better identify, track, and screen air cargo, and issue a final rule to enhance and improve the security of air cargo transported on both passenger and all-cargo aircraft.[10]

In October 2005, we reported on TSA's efforts to secure domestic air cargo, or cargo transported on passenger and all-cargo aircraft within the United States.[11] We reported that while TSA had taken a number of actions intended to strengthen air cargo security, such as establishing a centralized database on people and businesses that routinely ship air cargo within the United States, and implementing requirements for the random inspection of air cargo, factors existed that potentially limited their effectiveness. For example, TSA exempted certain types of air cargo from inspection, potentially creating security weaknesses. We also reported that TSA's plans for enhancing air cargo security posed financial, operational and technological challenges to both the agency and to air cargo industry stakeholders. In addition, we reported that while TSA had taken initial steps toward applying a risk-based approach to address air cargo security, it had not yet established a methodology and schedule for completing assessments of air cargo vulnerabilities and critical assets. Moreover, we reported on the potential challenges the agency and air cargo industry stakeholders may face in implementing measures to strengthen air cargo security. We made several recommendations to assist TSA in developing a comprehensive risk-based approach for securing the domestic air cargo transportation system. TSA agreed with our recommendations and informed us that it is taking steps to address some of these recommendations. For

7. In this report, the term "targeting" refers to the use of information obtained from the screening process to identify high-risk air cargo shipments for inspection.
8. DHS determined that the exact percentage of air cargo physically screened or inspected is Sensitive Security Information.
9. See Pub. L. No. 108–334, § 513, 118 Stat. 1298, 1317 (2004).
10. See Pub. L. No. 108–458, §§ 4051–54, 118 Stat. 3638, 3728–29 (2004).
11. GAO, *Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security*, GAO-06–76 (Washington, D.C.: October 2005).

example, in October 2006, TSA revised some of the inspection exemptions for domestic and outbound air cargo transported on passenger air carriers, consistent with our recommendation. TSA also issued an air cargo security rule in May 2006 that included a number of provisions aimed at enhancing the security of inbound air cargo.

This report provides the results of our examination of the efforts of DHS, through TSA and CBP, to secure inbound air cargo, and represents the second phase of our congressionally requested work addressing air cargo security.[12] To help Congress evaluate the status of DHS's efforts to secure inbound air cargo, we answered the following questions: (1) Within DHS, what actions have TSA and CBP taken to secure inbound air cargo, and how, if at all, could these efforts be strengthened? (2) What practices have the air cargo industry and select foreign governments adopted that could potentially be used to enhance TSA's efforts to strengthen inbound air cargo security, and to what extent have TSA and CBP worked with foreign governments to enhance their air cargo security efforts?

To determine what actions DHS, through TSA and CBP, has taken to secure inbound air cargo, and how, if at all, these efforts could be strengthened, we reviewed relevant documents such as TSA's air cargo strategic plan, air carrier security programs, and related TSA guidance to determine the requirements placed on air carriers for ensuring inbound air cargo security.[13] We interviewed officials from DHS, TSA, and CBP regarding their efforts to develop a strategy for securing inbound air cargo and conduct assessments of the vulnerabilities and critical assets associated with this area of aviation security and compared these efforts with GAO's risk management framework. In addition, we interviewed TSA and CBP officials to obtain information on their current and planned efforts to secure inbound air cargo. We also reviewed the results of TSA's compliance inspections to determine the agency's progress in evaluating air carriers' compliance with air cargo security requirements, and we reviewed the results of foreign airport assessments to identify any deficiencies found related to international air cargo standards. We discussed the reliability of TSA's compliance inspection data for the period July 2003 to February 2006 with TSA officials and concluded that they were sufficiently reliable for the purposes of this review. We conducted site visits to three U.S. airports, which collectively receive about 50 percent of the total amount of air cargo transported into the United States, to observe inbound air cargo security operations and CBP efforts to inspect inbound air cargo. We selected

12. The security of cargo transported from the United States to other countries, referred to as outbound air cargo, is subject to similar security requirements and procedures that apply to domestic air cargo. Because these security measures were addressed in our October 2005 report (GAO-06–76 ), they are not included in this report except in our discussion of how foreign air cargo security measures could be considered for strengthening domestic air cargo.

13. "Air carriers" refers to both foreign and U.S.-based passenger air carriers whose aircraft have been configured to accommodate both passengers and cargo, and all-cargo carriers whose aircraft transport only cargo.

these airports based on several factors, including airport size, the volume of air cargo transported to these airports from foreign locations, and geographical dispersion. Because we selected a nonprobability sample of airports, the results from these visits cannot be generalized to other U.S. airports. Further, we conducted site visits to seven countries in Europe and Asia to observe air cargo security processes and technologies, observe air cargo facilities, and obtain information on air cargo security practices implemented by foreign governments and industry stakeholders to identify those practices that could potentially enhance the department's efforts to secure air cargo.[14] We selected these countries based on several factors, including TSA threat rankings, airports located within these countries that process high volumes of air cargo, and discussions with U.S. and foreign government officials and air cargo industry representatives regarding air cargo security practices that may have application to TSA's efforts to secure air cargo. Moreover, we observed air cargo security practices at 8 foreign airports, 4 of which rank among the world's 10 busiest cargo airports in terms of volumes of cargo transported. We also obtained information on the air cargo security requirements implemented by 10 additional foreign countries from foreign government officials and publicly available documents. We selected these countries based on geographical dispersion as well as additional stakeholder input on countries implementing air cargo security practices that differ from those in the United States. To obtain information on air cargo industry and foreign government actions to secure air cargo, and TSA's and CBP's efforts to coordinate their security practices to enhance security and increase efficiency, referred to as harmonization, we interviewed foreign and domestic air carrier (passenger and all-cargo) officials from those air carriers that transport the largest volume of air cargo. Specifically, we spoke with officials representing 7 of the top 10 air cargo carriers based on volume of cargo transported. We also interviewed representatives of foreign freight forwarders, foreign and domestic airport authorities, air cargo industry associations, and U.S. and foreign governments.[15] More detailed information on our scope and methodology is contained in appendix I.

We conducted our work from October 2005 through February 2007 in accordance with generally accepted government auditing standards.

## RESULTS IN BRIEF

The two DHS components with responsibilities related to air cargo security, TSA and CBP, have taken initial steps to enhance the security of inbound air cargo. However, the agencies are only beginning to implement inbound air cargo security programs, and opportunities exist to strengthen these efforts. TSA and CBP have taken some preliminary steps to use risk management

14. For the purposes of this report, the term "air cargo security practices" collectively refers to requirements, standards, processes, and measures aimed at securing air cargo.

15. A freight forwarder is an entity that consolidates air cargo shipments and delivers them to air carriers.

principles to guide their investment decisions related to inbound air cargo, as advocated by DHS, but most of these efforts are in the planning stages. For instance, TSA completed a risk-based strategic plan to address domestic air cargo security, but has not developed a similar strategy for addressing inbound air cargo security, including how best to partner with CBP and international air cargo stakeholders. Further, TSA has identified the primary threats associated with inbound air cargo, but has not yet assessed which areas of inbound air cargo are most vulnerable to attack and which inbound air cargo assets are deemed most critical to protect. TSA plans to assess inbound air cargo vulnerabilities and critical assets—two crucial elements of a risk-based management approach—but has not yet established a methodology or time frame for how and when these assessments will be completed. Without such assessments, TSA may not be able to appropriately focus its resources on the most critical security needs.

Another action TSA has taken is the issuance of its May 2006 air cargo security rule, which includes a number of provisions aimed at enhancing the security of inbound air cargo. For example, the final rule acknowledges that TSA amended its security directives and programs to triple the percentage of cargo inspected on domestic and foreign passenger aircraft. To implement the requirements contained in the air cargo security rule, TSA drafted revisions to its existing security programs for domestic and foreign passenger air carriers and created new security programs for domestic and foreign all-cargo carriers. However, TSA requirements continue to allow inspection exemptions for certain types of inbound air cargo transported on passenger air carriers.[16] This risk is further heightened because TSA has limited information on the background and security risk posed by foreign shippers whose cargo may fall within these exemptions. TSA officials stated that the agency is holding discussions with industry stakeholders to determine whether additional revisions to current air cargo inspection exemptions are needed. TSA also inspects domestic and foreign passenger air carriers with service to the United States to assess whether the air carriers are complying with air cargo security requirements, such as inspecting a certain percentage of air cargo. TSA, however, does not currently inspect all air carriers transporting cargo into the United States. While TSA's compliance inspections provide useful information, the agency has not developed an inspection plan that includes performance goals and measures to determine to what extent air carriers are complying with security requirements.

In addition, while CBP was previously targeting inbound air cargo on passenger and all-cargo aircraft for illicit items such as drugs and contraband, CBP has only recently begun targeting inbound air cargo transported on passenger and all-cargo aircraft that may pose a security risk and inspecting such cargo once it arrives in the United States. Further, TSA and CBP have taken steps to

16. DHS determined that details on the types of inbound air cargo transported on passenger and all-cargo aircraft exempt from TSA inspection requirements are considered Sensitive Security Information. A description of these exemptions is provided in the restricted version of this report, GAO-07–337SU.

coordinate their efforts to safeguard air cargo transported into the United States to include sharing information on TSA's technology development programs, among other efforts. However, TSA and CBP do not have a systematic process in place to share information that could be used to strengthen their efforts, such as the results of TSA air carrier compliance inspections, assessments of foreign airports, and air carrier inspections of inbound air cargo. Without a systematic process to share relevant air cargo security information, TSA and CBP could be missing opportunities to more effectively secure inbound air cargo.

Foreign governments that regulate airports with high volumes of cargo, and domestic and foreign air carriers that transport large volumes of cargo, employ various air cargo security practices that might have the potential to strengthen TSA's efforts to secure inbound air cargo. Some of these practices may also help strengthen the security of domestic air cargo. We identified four categories of security practices required or employed by foreign governments and foreign air carriers, as well as domestic air carriers implementing practices required by host governments, that are currently not used in the United States. TSA officials acknowledged that the agency has not systematically analyzed these foreign practices to determine whether they would help strengthen the domestic and U.S.-bound air cargo supply chains or the costs associated with implementing such practices. For example, air carriers in some foreign counties inspect air cargo for potential WMDs prior to its loading on a U.S.-bound flight, which neither TSA nor CBP requires.[17] TSA officials acknowledged that compiling and analyzing information on air cargo security practices implemented by foreign air carriers and foreign governments may provide opportunities to enhance the department's air cargo security program, and they have begun an initial review of practices in select countries. However, officials also cited challenges to applying these practices in the United States and the inbound air cargo supply chain. For example, TSA officials stated that increasing the percentage of cargo inspections and utilizing various inspection technologies may not be applicable to the United States because the volume of air cargo processed in the United States is much larger than in most countries. While we recognize that differences in cargo volumes and inspection capabilities exist and could affect the feasibility and cost of implementing certain practices to secure domestic and inbound air cargo, we believe that systematically identifying and evaluating the feasibility and costs associated with promising foreign air cargo security practices has the potential to benefit TSA's efforts to secure domestic and inbound air cargo. TSA has also begun working with foreign governments to coordinate their security practices to enhance security and increase efficiency, referred to as harmonization. For example, TSA officials worked with foreign governments to develop internationally agreed upon standards for securing air cargo. However, challenges to harmonizing security practices may limit the effectiveness of these efforts.

17. DHS determined that other examples of air carriers' efforts to secure air cargo are Sensitive Security Information. Information on these examples is provided in the restricted version of this report, GAO-07–337SU.

For instance, some countries may be hesitant to expend additional resources that may be necessary to implement common security standards that exceed their current security requirements. In addition, some foreign governments may have different views than TSA regarding the threats and risks associated with air cargo and where their resources should be directed.

To better ensure the security of inbound air cargo, we are recommending that DHS direct TSA and CBP to take several actions. These include more fully developing a risk-based strategy to address inbound air cargo security, including establishing goals and objectives for securing inbound air cargo and establishing a methodology and time frames for completing assessments of inbound air cargo vulnerabilities and critical assets that can be used to help prioritize the actions necessary to enhance security; establishing a time frame for completing an assessment of whether existing inspection exemptions for inbound air cargo pose an unacceptable security vulnerability, and taking steps, if necessary, to address identified vulnerabilities; developing performance goals and measures to evaluate foreign and domestic air carrier compliance with inbound air cargo security requirements; developing a systematic process for ensuring communication between TSA and CBP regarding their efforts to secure inbound air cargo; and compiling and analyzing information on air cargo security practices implemented by domestic and foreign air cargo industry stakeholders and foreign governments to identify those that could be used to strengthen DHS's overall air cargo security program.

We provided a draft of this report to DHS for review. DHS, in its written comments, generally concurred with the report and recommendations. However, we have concerns that the actions DHS intends to take may not fully address our recommendations. The full text of DHS's comments is included in appendix VIII.

## BACKGROUND

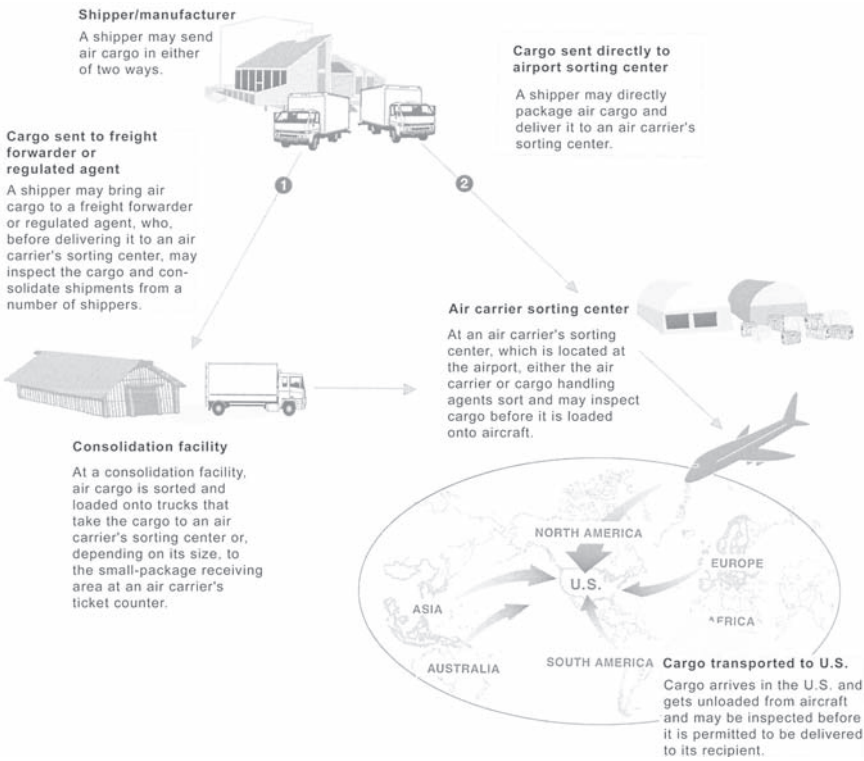
The transportation of air cargo between global trading partners provides the world economy with critical goods and components. Air cargo valued at almost $400 billion entered the United States in fiscal year 2004. According to TSA, approximately 200 U.S. and foreign air carriers currently transport cargo into the United States from foreign countries. During calendar year 2005, almost 9.4 billion pounds of cargo was shipped by air into the United States. About 40 percent of this amount, or 4 billion pounds, traveled onboard passenger aircraft. Typically, about one-half of the hulls of each passenger aircraft transporting cargo are filled with cargo.

Air cargo includes freight and express packages that range in size from small to very large, and in type from perishables to machinery, and can include items such as electronic equipment, automobile parts, clothing, medical supplies, other dry goods, fresh cut flowers, fresh seafood, fresh produce, tropical fish, and human remains. Cargo can be shipped in various forms, including large containers known as unit loading devices that allow many packages to be consolidated into one container that can be loaded on an aircraft, wooden crates, assembled pallets, or individually wrapped/boxed pieces, known as break bulk cargo.

Participants in the international air cargo shipping process include shippers, such as individuals and manufacturers; freight forwarders or regulated agents, who consolidate shipments and deliver them to air carriers; air cargo handling agents, who process and load cargo onto aircraft on behalf of air carriers; and passenger and all-cargo carriers that store, load, and transport air cargo.[18] International air cargo may have been transported via ship, train, or truck prior to its loading onboard an aircraft. Shippers typically send cargo by air in one of two ways. Figure 1 depicts the two primary ways in which a shipper may send cargo by air to the United States.

A shipper may take its packages to a freight forwarder, or regulated agent, which consolidates cargo from many shippers and delivers it to air carriers.

**Figure 1**
**Flow of Air Cargo Transported to the United States**




*Source:* GAO (analysis), MapArt (map), ArtExplosion and GAO (art).

18. The International Civil Aviation Organization defines a regulated agent as an agent, freight forwarder, or any other entity that conducts business with an aircraft operator and provides security controls that are accepted or required by the appropriate government authority with respect to cargo or mail.

The freight forwarder usually has cargo facilities at or near airports and uses trucks to deliver bulk freight to air carriers—either to a cargo facility or to a small-package receiving area at the ticket counter. A shipper may also send freight by directly packaging and delivering it to an air carrier's ticket counter or sorting center where either the air carrier or a cargo handling agent will sort and load cargo onto the aircraft. The shipper may also have cargo picked up and delivered by an all-cargo carrier, or choose to take cargo directly to a carriers' retail facility for delivery. As noted in figure 1, the inspections of air cargo can take place at several different points throughout the supply chain. For example, inspections can take place at freight forwarder's or regulated agent's consolidation facility, or at the air carrier's sorting center.

## TSA AND CBP RESPONSIBILITIES FOR ENSURING THE SECURITY OF INBOUND AIR CARGO

### TSA's Responsibilities Related to Securing Inbound Air Cargo

The Aviation and Transportation Security Act (ATSA) charged TSA with the responsibility for ensuring the security of the nation's transportation systems, including the transportation of cargo by air into the United States.[19] In fulfilling this responsibility, TSA (1) enforces security requirements established by law and implemented through regulations, security directives, TSA-approved security programs, and emergency amendments, covering domestic and foreign passenger and all-cargo carriers that transport cargo into the United States; (2) conducts inspections to assess air carriers' compliance with established requirements and procedures; (3) conducts assessments at foreign airports to assess compliance with international aviation security standards, including those related to air cargo; and (4) conducts research and development of air cargo security technologies.[20]

Air carriers (passenger and all-cargo) are responsible for implementing TSA security requirements, predominantly through a TSA-approved security program that describes the security policies, procedures, and systems the air carrier will implement and maintain in order to comply with TSA security

19. Other federal entities involved in securing or safeguarding air cargo include the Department of Homeland Security–U.S. Customs and Border Protection, the United States Postal Service, the Department of Commerce, the Department of Transportation, and the Department of the Treasury.

20. Foreign air carriers landing or taking off in the United States must adopt and use a TSA-approved security program that requires adherence to the identical security measures required of U.S. air carriers serving the same airports. See 49 U.S.C. § 44906. TSA regulations provide that a foreign air carrier security program will only be deemed acceptable if it provides passengers a level of protection similar to the level of protection provided by U.S. air carriers serving the same airports. See 49 C.F.R. § 1546.103(a)(1). For example, a foreign air carrier must prohibit cargo from being loaded on board its aircraft unless handled in accordance with the foreign air carrier's TSA-approved security program.

requirements.[21] These requirements include measures related to the acceptance, handling, and inspection of cargo; training of employees in security and cargo inspection procedures; testing employee proficiency in cargo inspection; and access to cargo areas and aircraft. If threat information or events indicate that additional security measures are needed to secure the aviation sector, TSA may issue revised or new security requirements in the form of security directives or emergency amendments applicable to domestic or foreign air carriers. The air carriers must implement the requirements set forth in the security directives or emergency amendments in addition to those requirements already imposed and enforced by TSA.

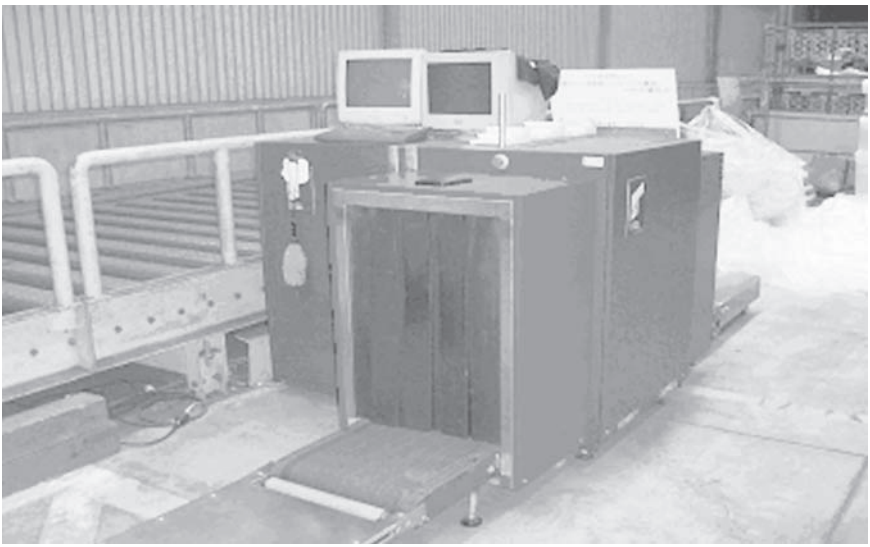
Under TSA regulations, the responsibility for inspecting air cargo is assigned to air carriers. TSA requirements, described in air carrier security programs, security directives, and emergency amendments, allow air carriers to use several methods and technologies to inspect domestic and inbound air cargo. These include manual physical searches and comparisons between airway bills and cargo contents to ensure that the contents of the cargo shipment matches the cargo identified in documents filed by the shipper, as well as using approved technology, such as X-ray systems, explosive trace detection systems, decompression chambers, explosive detection systems, and TSA explosives detection canine teams.[22] (For an example of X-ray technology used by air carriers to inspect air cargo prior to its transportation to the United States, see fig. 2). TSA currently requires passenger air carriers to randomly inspect a specific percentage of non exempt air cargo pieces listed on each airway bill.[23] Under TSA's inbound air cargo inspection requirements, passenger

21. As of January 2007, TSA security programs include the (1) Aircraft Operator Standard Security Program, which applies to domestic passenger air carriers; (2) Indirect Air Carrier Standard Security Program, which applies to domestic indirect air carriers; (3) Domestic Security Integration Program, a voluntary program that applies to domestic all-cargo carriers; (4) Twelve-Five Program, which applies to certain operators of aircraft weighing more than 12,500 pounds in scheduled or charter service that carry passengers, cargo, or both; (5) Model Security Program, which applies to foreign passenger air carriers; and (6) All-Cargo International Security Procedures, which applies to each foreign air carrier engaged in the transportation of cargo to, from, within, or overflying the United States in all-cargo aircraft with a maximum certified takeoff weight of more than 12,500 pounds. TSA drafted new security programs for foreign and U.S. all-cargo carriers with operations to, from, and within the United States. TSA expects to finalize these programs in early 2007.

22. Explosive trace detection (ETD) equipment requires human operators to collect samples of items to be inspected with swabs, which are chemically analyzed to identify any traces of explosive material. Explosive detection systems use probing radiation to examine objects inside baggage and identify the characteristic signatures of threat explosives. Certified explosive detection canine teams have been evaluated by TSA and shown to effectively detect explosive devices. Decompression chambers simulate the pressures acting on aircraft by simulating flight conditions, which cause explosives that are attached to barometric fuses to detonate.

23. DHS determined that details on the percentage of air cargo required to be randomly inspected are considered Sensitive Security Information. Information on the percentage of air cargo randomly inspected is provided in the restricted version of this report, GAO-07–337SU.

**Figure 2**
**Type of X-ray Technology Used by Some Foreign Air Carriers to Inspect Air Cargo Bound for the United States**



*Source:* GAO.

air carriers can exempt certain cargo from inspection.[24] TSA does not regulate foreign freight forwarders, or individuals or businesses that have their cargo shipped by air to the United States.

To assess whether air carriers properly implement TSA inbound air cargo security regulations, the agency conducts regulatory compliance inspections of foreign and domestic air carriers at foreign airports. Currently, TSA conducts compliance inspections of domestic and foreign passenger carriers transporting cargo into the United States, but does not perform such inspections of all air carriers transporting inbound air cargo. TSA inspects air cargo procedures as part of its broader international aviation security inspections program, which also includes reviews of regulations such as aircraft and passenger security. Compliance inspections can include reviews of documentation, interviews of air carrier personnel, and direct observations of air cargo operations.[25] Air carriers are subject to inspection in several areas of cargo security, including

24. DHS determined that details on the types of inbound air cargo transported on passenger and all-cargo aircraft exempt from TSA inspection requirements are considered Sensitive Security Information. A description of these exemptions is provided in the restricted version of this report, GAO-07–337SU.

25. Unlike its domestic air cargo inspection program, TSA's inbound air cargo security program does not include a covert testing component to identify air cargo security weaknesses. TSA officials stated that foreign governments do not allow the agency to conduct such tests.

accepting cargo from unknown shippers, access to cargo, and security training and testing. Appendix II contains a detailed description of TSA's efforts to assess air carrier compliance with inbound air cargo security requirements.

In addition, TSA assesses the effectiveness of the security measures maintained at foreign airports that serve U.S. air carriers, from which foreign air carriers serve the United States, or that pose a high risk of introducing danger to international air travel.[26] To conduct its assessments, TSA must consult with appropriate foreign officials to establish a schedule to visit each of these foreign airports. TSA assessments evaluate the security policies and procedures in place at a foreign airport to ensure that the procedures meet baseline international aviation security standards, including air cargo security standards. For further information on TSA's foreign airport assessments including the results of its assessment conducted during fiscal year 2005, see appendix III.

## CBP's Responsibilities Related to Inbound Air Cargo Security

CBP determines the admissibility of cargo entering the United States and is authorized to inspect inbound air cargo for security purposes. Specifically, CBP requires air carriers to submit cargo manifest information prior to the aircraft's arrival in the United States.[27] CBP also has authority to negotiate with foreign nations to place CBP officers abroad to inspect persons and merchandise prior to their arrival in, or subsequent to their exit from, the United States, but has not yet negotiated arrangements with foreign host nations to station CBP officers overseas for the purpose of inspecting high-risk air cargo shipments.[28] At U.S. airports, CBP officers may conduct searches of persons, vehicles, baggage, cargo, and merchandise entering or departing the United States.[29] Since September 11, 2001, CBP's priority mission has focused on keeping terrorists and their weapons from entering the United States.[30] To carry out this responsibility, CBP employs several systems and

26. 49 U.S.C. § 44907(a)(1). TSA assumed responsibility for conducting foreign airport assessments from the Secretary of Transportation (as delegated to the Federal Aviation Administration) in accordance with the Aviation and Transportation Security Act, enacted in November 2001. See 49 U.S.C. § 114(d). TSA conducts these assessments utilizing a standard for analysis based, at least, on the standards and appropriate recommended practices of Annex 17 to the Convention on International Civil Aviation. § 44907(a)(2). The Secretary of Homeland Security determines whether an airport maintains and carries out effective security measures using the results of TSA's assessments. See § 44907(c).

27. See 19 C.F.R. § 122.48a (implementing a provision of the Trade Act of 2002, Pub. L. No. 107–210, § 343, 116 Stat. 933, 981–83, as amended, requiring the electronic submission of inbound cargo information prior to arrival in the United States).

28. See 19 U.S.C. § 1629.

29. See 19 U.S.C. §§ 482, 1467, 1499, 1581, and 1582.

30. Historically, CBP has been responsible for interdicting and seizing contraband and illegal drugs. CBP targets and inspects cargo on behalf of 16 other federal agencies, including the U.S. Dept. of Agriculture, the Food and Drug Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, and the Drug Enforcement Agency.

programs. CBP's Automated Targeting System (ATS) is a model that combines manifest and entry declaration information into shipment transactions and uses historical, specific enforcement, and other data to help target cargo shipments for inspection.[31] ATS also has targeting rules that assign a risk score to each arriving shipment based in part on manifest information, as well as other shipment information, and potential threat or vulnerability information, which CBP staff use to make decisions on the extent of inspection to be conducted once the cargo enters the United States.[32] To support its targeting system, CBP requires air carriers to submit cargo manifest information prior to the flight arriving i n the United States.[33] CBP officers use the ATS risk scores to help them make decisions regarding the extent of inspection to be conducted once the cargo arrives in the United States.[34] Shipments identified by CBP as high risk through its ATS targeting system are to undergo mandatory security inspections. CBP officers may also inspect air cargo if they determine that a particular shipment is suspicious or somehow poses a threat.[35]

CBP uses a variety of non intrusive technologies and methods to inspect some air cargo once it arrives in the United States. For example, CBP officers carry personal handheld radiation detectors, as well as handheld radioactive isotope identification devices which can distinguish between different types of radiological material, such as that used in medicine or industry, from weapons-grade material. Other technologies and methods CBP uses to inspect inbound air cargo include mobile X-ray machines contained in vans, pallet X-ray systems, mobile vehicle and cargo inspection systems (VACIS), and canine

31. CBP defines an inspection as a physical examination and/or the imaging of cargo using non-intrusive inspection technology to identify contraband and terrorist-related items.

32. DHS determined that details on the type of shipment information used by ATS to assign a risk score to air cargo shipments are considered Sensitive Security Information. A description of the shipment information used by ATS is discussed in the restricted version of this report, GAO-07–337SU.

33. Pursuant to the Trade Act of 2002, as amended, CBP established time frames in which air carriers are required to electronically submit air cargo manifest information. See 19 C.F.R. § 122.48a(b). Air carriers departing from any foreign location in the Americas, including Mexico, Central America, and areas of South America north of the equator, must submit manifest information no later than the time of flight departure (the time at which wheels are up on the aircraft and the aircraft is en route directly to the United States.). In the case of air carriers departing from any other foreign location, CBP requires that manifest information be submitted 4 hours prior to the flight's arrival in the United States.

34. Officers who are members of CBP's Anti-terrorism Contraband Enforcement Teams specialize in targeting and examining inbound air cargo shipments to identify potential contraband and terrorist-related items.

35. CBP also conducts inspections based on specific, usually classified, intelligence that points to a specific threat and directs field officers in specific airports to take certain actions. The results of field officer efforts may be analyzed and shared with the intelligence community. These inspections are not part of CBP's routine efforts to address ongoing air cargo threats associated with the smuggling of contraband or WMD.

**Figure 3**
**CBP Officers Using Nonintrusive Technology to Inspect Inbound Air Cargo**


*Source:* GAO.

teams.[36] The results of the nonintrusive inspections determine the need for additional measures, which could include physical inspections conducted by CBP officers. Figure 3 shows an example of CBP officers using nonintrusive technology to inspect inbound air cargo upon its arrival in the United States.

To strengthen the security of the inbound cargo supply chain, the U.S. Customs Service (now CBP) initiated the voluntary Customs-Trade Partnership Against Terrorism (C-TPAT) program in November 2001. This program provides companies that implement CBP-defined security practices a reduced likelihood that their cargo will be inspected once it arrives in the United States.[37] To become a member of C-TPAT, companies must first submit signed C-TPAT agreements affirming their desire to participate in the voluntary program. Companies must also provide CBP with

36. The pallet VACIS unit consists of a self-contained gamma ray imaging system designed to quickly image pallets or pallet-sized containers. A mobile VACIS, similar to a pallet VACIS unit, consists of a truck-mounted, gamma ray imaging system that produces a radiographic image used to evaluate the contents of trucks, containers, cargo, and passenger vehicles in order to determine the possible presence of contraband.

37. The SAFE Port Act, enacted in October 2006, specifically authorized the Secretary of Homeland Security, acting through the Commissioner of CBP, to establish the C-TPAT program in accordance with requirements set forth in the law. *Security and Accountability for Every (SAFE) Port Act of 2006, Pub. L. No. 109–347, §§ 211–223, 120 Stat. 1884, 1909–15.*

security profiles that describe the current security procedures they have in place, such as pre-employment screening, periodic background reviews, and employee training on security awareness and procedures. CBP reviews a company's application to identify any weaknesses in the company's security procedures and work with the company to resolve these weaknesses. Once any weaknesses are addressed, CBP signs an agreement stating that the company is considered to be a certified C-TPAT member, eligible for program benefits.[38]

After certification, CBP has a process for validating that C-TPAT members have implemented security measures. During the validation process, CBP staff meet with company representatives to verify supply chain security measures. The validation process includes visits to the company's U.S. and foreign sites, if any. Upon completion of the validation process, CBP reports back to the company on any identified areas that need improvement and suggested corrective actions, as well as a determination of whether program benefits are still warranted for the company. According to CBP officials, they use a risk-based approach for identifying the priority in which C-TPAT participants should be validated.[39]

## INTERNATIONAL AIR CARGO SECURITY STANDARDS AND RECOMMENDED PRACTICES

The International Civil Aviation Organization (ICAO) is a specialized agency of the United Nations in charge of coordinating and regulating international air transportation. ICAO was established by the Convention on International Civil Aviation (also known as the Chicago Convention) in 1944 and is composed of over 180 member nations with aviation service capabilities. In 1974, ICAO established aviation security standards and recommended practices to ensure a baseline level of security. These standards are aimed at preventing suspicious objects, weapons, explosives, or other dangerous devices from being placed on board passenger aircraft either through concealment, in otherwise legitimate shipments, or through gaining access to air cargo shipments via cargo-handling areas. The standards call for member nations to implement measures to ensure the protection of air cargo being moved within an airport and intended for transport on an aircraft, and to ensure that aircraft operators do not accept cargo on passenger flights unless application of security controls has been confirmed and accounted for by a regulated agent or that such cargo has been subjected to appropriate security controls. ICAO standards also provide that except for reasons of aviation

38. In May 2005, CBP began using a three-tiered approach in providing C-TPAT participants with benefits. Under this approach, air carriers' benefits, including a reduction in their risk score, increase based on (1) whether the carriers are certified,(2) whether they are validated, and (3) whether they are implementing security requirements that exceed minimum guidelines.
39. DHS determined that details on the information CBP uses to prioritize which C-TPAT participants should be validated are Sensitive Security Information. A description of this information is included in the restricted version of this report, GAO-07–337SU.

security, member states should not require the physical inspection of all air cargo that is imported or exported. In general, member states should apply risk management principles (such as targeting higher-risk cargo) to determine which goods should be examined and the extent of that examination. While compliance with these standards is voluntary, all 180 ICAO members, including the United States, have committed to incorporating these standards into their national air cargo security programs.[40]

The International Air Transport Association (IATA) represents about 260 air carriers constituting 94 percent of international scheduled air traffic. Building upon ICAO's standards, IATA issued voluntary recommended practices and guidelines to help ensure that global air cargo security measures are uniform and operationally manageable. For example, IATA published a manual that, among other things, encourages air carriers to implement measures and procedures to prevent explosives or other dangerous devices from being accepted for transport by air, conduct pre-employment checks on individuals involved in the handling or inspection of air cargo, and ensure the security of all shipments accepted from persons other than known shippers[41] or regulated agents through physical inspection or some type of screening process. IATA also developed guidelines to assist air carriers in developing security policies by providing detailed suggestions for accepting, handling, inspecting, storing, and transporting air cargo.

The World Customs Organization (WCO) consists of 166 member nations, representing 99 percent of global trade, including cargo transported by air. In June 2005, WCO established its Framework of Standards to Secure and Facilitate Global Trade that, among other things, sets forth principles and voluntary minimum security standards to be adopted by its members. The framework provides guidance for developing methods to target and inspect high-risk cargo, establishes time frames for the submission of information on cargo shipments, and identifies inspection technology that could be used to inspect high-risk cargo.

## APPLYING A RISK-MANAGED APPROACH FOR SECURING INBOUND AIR CARGO

Risk management is a tool for informing policy makers' decisions about assessing risks, allocating resources, and taking actions under conditions

40. Although adopting these standards is voluntary, in the sense that each contracting state signs onto the convention of its own accord, a state may face consequences for not adopting and following the ICAO standards. For example, if a state does not amend its own regulations or practices in light of amendments to the ICAO standards, all other states will be notified of the difference existing between the international standards and the corresponding national practice of the state. Similarly, TSA is authorized under U.S. law to conduct foreign airport assessments using, at least, the ICAO standards and appropriate recommended practices to determine if the airport maintains and carries out effective security measures, and to take appropriate actions in the event the airport does not maintain effective security measures. See 49 U.S.C. § 44907.

41. A known shipper is an individual or business with an established history of shipping cargo on passenger carriers.

of uncertainty. In recent years, the President, through Homeland Security Presidential Directives (HSPD), and Congress, more recently through the Intelligence Reform and Terrorism Prevention Act of 2004, required federal agencies with homeland security responsibilities to apply risk-based principles to inform their decision making regarding allocating limited resources and prioritizing security activities. The National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission), recommended that the U.S. government identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort.[42] In addition, DHS issued the National Strategy for Transportation Security in 2005 that describes the policies DHS will apply when managing risks to the security of the U.S. transportation system.[43] We have previously reported that a risk management approach can help to prioritize and focus the programs designed to combat terrorism. As applied in the homeland security context, risk management can help officials make decisions about resource allocations and associated tradeoffs in preparing defenses against acts of terrorism and other threats. We have recommended that TSA apply a comprehensive risk-based approach for securing the domestic air cargo transportation system.[44]

The Homeland Security Act of 2002 also directed the department's Directorate of Information Analysis and Infrastructure Protection to use risk management principles in coordinating the nation's critical infrastructure protection efforts.[45] This includes integrating relevant information, and analysis and vulnerability assessments to identify priorities for protective and support measures by the department, other federal agencies, state and local government agencies and authorities, the private sector, and other entities. Homeland Security Presidential Directive 7 and the Intelligence Reform and Terrorism Prevention Act of 2004 further define and establish critical infrastructure protection responsibilities for DHS and those federal agencies given responsibility for particular industry sectors, such as transportation. In June

42. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, D.C.: 2004). The 9/11 Commission was an independent, bipartisan commission established in late 2002, to prepare a complete account of the circumstances surrounding the September 11 terrorist attacks, including preparedness for and the immediate response to the attacks. The commission was also mandated to provide recommendations designed to guard against future attacks.

43. The Intelligence Reform and Terrorism Prevention Act of 2004 requires the Secretary of Homeland Security to develop, prepare, implement, and update, as needed a National Strategy for Transportation Security and transportation modal security plans. See Pub. L. No. 108–458, § 4001, 118 Stat. 3638, 3710–12 (codified at 49 U.S.C. §§ 114(t), 44904(c)-(d)).

44. GAO-06–76.

45. In 2006, DHS reorganized the Information Analysis and Infrastructure Protection Directorate and moved its functions to the Office of Intelligence and Analysis and Office of Infrastructure Protection.

2006, DHS issued the National Infrastructure Protection Plan (NIPP), which named TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector, which includes all modes of transportation.[46] The NIPP requires federal agencies to work with the private sector to develop plans that, among other things, identify and prioritize critical assets for their respective sectors. In accordance with the NIPP, TSA must conduct and facilitate risk assessments in order to identify, prioritize, and coordinate the protection of critical transportation systems infrastructure, as well as develop risk-based priorities for the transportation sector. TSA officials reported that work is now under way on specific plans for each mode of transportation, but as of January 2007, they were not completed.

To provide guidance to agency decision makers, we have created a risk management framework, which is intended to be a starting point for applying risk-based principles. Our risk management framework entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives. DHS's NIPP describes a risk management process that closely mirrors our risk management framework.

Setting strategic goals, objectives, and constraints is a key first step in applying risk management principles and helps to ensure that management decisions are focused on achieving a purpose. These decisions should take place in the context of an agency's strategic plan that includes goals and objectives that are clear and concise. These goals and objectives should identify resource issues and other factors to achieving the goals. Further, the goals and objectives of an agency should link to a department's overall strategic plan. The ability to achieve strategic goals depends, in part, on how well an agency manages risk. The agency's strategic plan should address risk-related issues that are central to the agency's overall mission.

Risk assessment, an important element of a risk-based approach, helps decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks. Risk assessment is a qualitative and/or quantitative determination of the likelihood of an adverse event occurring and the severity, or impact, of its consequences. Risk assessment in a homeland security application often involves assessing three key elements—threat, vulnerability, and criticality or consequence. A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities. A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses. A criticality

46. DHS designated TSA as the lead agency for addressing HSPD-7 as it relates to securing the nation's transportation sector. The Department of Transportation also has a collaborative role for addressing HSPD-7.

or consequence assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy, as a basis for identifying which structures or processes are relatively more important to protect from attack. Information from these three assessments contributes to an overall risk assessment that may characterize risks on a scale such as high, medium, or low and provides input for evaluating alternatives and management prioritization of security initiatives. The risk assessment element in the overall risk management cycle may be the largest change from standard management steps and can be important to informing the remaining steps of the cycle. For further details on our risk management framework, see appendix IV.

## DHS HAS TAKEN INITIAL STEPS TO SECURE INBOUND AIR CARGO, AND OPPORTUNITIES EXIST TO STRENGTHEN THESE EFFORTS

The two components within DHS responsible for air cargo security, TSA and CBP, have initiated efforts to better secure inbound air cargo, but these efforts are in the early stages and could be enhanced. While TSA and CBP have taken some preliminary steps to use risk management principles to guide their decisions related to inbound air cargo security, most of TSA's and CBP's efforts to enhance inbound air cargo security are still largely in the planning stages. For instance, TSA has completed a strategic plan to address domestic air cargo security and has identified the primary threats associated with inbound air cargo. However, the agency has not identified goals and objectives for addressing inbound air cargo security, such as how it will coordinate with CBP to ensure that all relevant areas of inbound air cargo security are addressed. Further, TSA has not assessed which areas of inbound air cargo are most vulnerable to attack and which assets are deemed most critical to protect. Another action TSA has taken is the publication of its final air cargo security rule in May 2006 that included a number of provisions aimed at enhancing the security of inbound air cargo. However, TSA's inbound air cargo inspection requirements continue to allow for a number of exemptions for cargo transported on passenger air carriers, which could be exploited to transport an explosive device. In addition, TSA conducts compliance inspections of domestic and foreign passenger air carriers transporting cargo into the United States, but the agency has not developed an inspection plan that would establish goals and measures for its inspection program to evaluate air carriers' performance against expected results. Also within DHS, CBP has recently initiated efforts to mitigate the threat of a WMD entering the United States by targeting inbound air cargo transported on passenger and all-cargo aircraft that may pose a security risk and inspecting such cargo once it arrives in the United States. CBP also manages the C-TPAT program, which encourages those businesses involved in the transportation of cargo into the United States to enhance their security practices. However, CBP is still in the early stages

of developing specific security criteria for air carriers participating in the program. In addition, DHS is in the early stages of researching, developing, and testing technologies to enhance the security of air cargo, but has not yet assessed the results or determined whether these technologies will be deployed abroad. Finally, TSA and CBP have taken steps to coordinate their responsibilities to safeguard air cargo transported into the United States, but the two agencies do not have a systematic process in place to share information that could be used to strengthen their efforts to secure inbound air cargo.

*This page intentionally left blank*

# Vulnerabilities Exposed through Covert Testing of TSA's Passenger Screening Process

*Statement of Gregory D. Kutz, Managing Director Forensic Audits and Special Investigations*
*John W. Cooney, Assistant Director Forensic Audits and Special Investigations*

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to discuss our latest test of airport security. In March 2006, we reported on the results of covert security vulnerability testing at 21 airports across the country. These tests clearly demonstrated that our nation's airlines were vulnerable to a suicide bomber using commercially available materials to detonate an explosive device onboard an airplane. During these covert tests, our investigators passed through airport security checkpoints carrying prohibited explosive components without being caught by Transportation Security Administration (TSA) security officers.[1] Later that year, in August 2006, British authorities uncovered the alleged transatlantic bomb plot. The discovery of this bomb plot, in which terrorists allegedly sought to detonate improvised explosive devices (IED)[2] in airplanes as they crossed the Atlantic Ocean, caused TSA to substantially modify its screening procedures—all liquids, gels, and aerosols with some exceptions were banned from being carried through passenger screening checkpoints and onto aircraft until the plot was further investigated. These restrictions were later relaxed to allow small amounts of liquids, gels, and aerosols through the checkpoint.

---

This testimony was revised on November 16, 2007, to include a link to digital video. This digital video shows test footage of the improvised explosive devices (IED) and improvised incendiary device (IID) that GAO investigators successfully brought through airport security checkpoints. A link has been added in the Creating Functioning IED and IID Devices section on page 6.

1. Our March 2006 report is classified, but TSA has authorized this limited discussion.
2. An IED is an apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, or distract through high-speed projectiles and overpressure.

This report responds to your request that we test whether security vulnerabilities exist in the TSA passenger screening process. To perform this work, we attempted to (1) obtain the instructions and components needed to create devices that a terrorist might use to cause severe damage to an airplane and threaten the safety of passengers and (2) test whether investigators could pass through airport security checkpoints undetected with all the components needed to create the devices.

To obtain instructions on creating devices a terrorist might use, we reviewed publicly available information and performed Internet searches. We obtained components for these devices at local stores and over the Internet. We devised methods to conceal the prohibited components using public information about TSA policies and procedures and obtained items to conceal the components at local stores and over the Internet. We then conducted our covert tests at a nonrepresentative selection of 19 airports across the country. The criteria we used to select the airports resulted in our testing a variety of U.S. commercial airports, some of which employed private screeners.[3]

Our work was not intended to evaluate the overall design and effectiveness of TSA's airport security program, which contains multiple layers of security. Rather, our work was performed to test specific security vulnerabilities related to the three major elements of TSA's passenger screening process—human capital (i.e., people), processes, and technology employed at the checkpoint. We tested the effectiveness of our explosive device at a national laboratory in July 2007. We had previously tested the effectiveness of less powerful explosive and incendiary devices in the Washington, D.C., metro area with help of a local law enforcement organization. We conducted work for this investigation from March 2007 through July 2007 in accordance with quality standards for investigations as set forth by the President's Council on Integrity and Efficiency.

## SUMMARY

Our investigators succeeded in passing through TSA security screening checkpoints undetected with components for several IEDs and an improvised incendiary device (IID)[4] concealed in their carry-on luggage and on their persons. The components for these devices and the items used to conceal the components were commercially available. Specific details regarding the device components and the methods of concealment we used during our

3. Specific details about which airports employed private screeners as opposed to transportation security officers are considered sensitive security information and are not included in this testimony. Therefore, the term transportation security officer is used throughout this testimony, but may, in some cases, also refer to private screeners that we tested.

4. A IID is an apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, or distract by creating intense heat or fire.

covert testing are classified by TSA; as such, they are not discussed in this testimony.

Using publicly available information, our investigators identified two types of devices that a terrorist could use to cause severe damage to an airplane and threaten the safety of passengers. The first device was an IED made up of two parts—a liquid explosive and a low-yield detonator. Although the detonator itself could function as an IED, investigators determined that it could also be used to set off a liquid explosive and cause even more damage. In addition, the second device was an IID created by combining commonly available products (one of which is a liquid) that TSA prohibits in carry-on luggage. Investigators obtained the components for these devices at local stores and over the Internet for less than $150. Tests that we performed at a national laboratory in July 2007, in addition to prior tests in February 2006 that we performed in partnership with a law enforcement organization in the Washington, D.C., metro area, clearly demonstrated that a terrorist using these devices could cause severe damage to an airplane and threaten the safety of passengers.

Investigators then devised methods to conceal the components for these devices from TSA transportation security officers, keeping in mind TSA policies related to liquids and other items, including prohibited items. By using concealment methods for the components, two investigators demonstrated that it is possible to bring the components for several IEDs and one IID through TSA checkpoints and onto airline flights without being challenged by transportation security officers. In most cases, transportation security officers appeared to follow TSA procedures and used technology appropriately; however, we uncovered weaknesses in TSA screening procedures and other vulnerabilities as a result of these tests. For example, although transportation security officers generally enforced TSA's policies, investigators were able to bring a liquid component of the IID undetected through checkpoints by taking advantage of weaknesses identified in these policies. These weaknesses were identified based on a review of public information. TSA determined that specific details regarding these weaknesses are sensitive security information and are therefore not discussed in this testimony. We did not notice any difference between the performance of private screeners and transportation security officers during our tests.

We provided TSA officials with two timely briefings to help them take corrective action. While we understand that TSA faces a significant challenge in balancing security concerns with efficient passenger movement, we are recommending that the Secretary of Homeland Security consider several actions to improve aspects of TSA's passenger screening program, including elements of human capital, processes, and technology.

## BACKGROUND

TSA is responsible for securing all modes of transportation while facilitating commerce and freedom of movement for the traveling public. In

performing its responsibilities, TSA is guided by risk-based planning, which generally involves a consideration of threats, vulnerabilities, and the criticality or consequence of an attack if it were to be carried out. Specifically, in its approach to securing the domestic aviation sector, TSA maintains numerous programs that provide a layered approach to security, including intelligence gathering and analysis, checking passenger manifests against watch lists, and assigning undercover air marshals to certain flights. The general public associates TSA mainly with its security effort at airport passenger checkpoints. One primary goal of the passenger checkpoint screening program is to provide for the safety and security of persons and property on an aircraft against the introduction of an unauthorized weapon, explosive, or incendiary.[5] As we reported in April 2007, TSA continues to modify its checkpoint screening program based on a number of factors including passenger feedback, risk-based planning, and its own internal review and testing process.[6] TSA's well-publicized recent policy change in response to the alleged transatlantic bomb plot of August 2006 is an important example of risk-based planning. Known as the 3–1-1 rule, this procedural change prohibits liquid, gel, or aerosol items over 3.4 fluid ounces in carry-on luggage; in addition, all liquid and gels should be placed in a 1-quart bag, and only one 1-quart bag is allowed per passenger.

## Passenger Screening Process

TSA focuses on the checkpoint screening process as a primary means of detecting prohibited items. Items that TSA has prohibited passengers from bringing aboard an aircraft include, among other things, firearms and knives; gasoline and lighter fluid; disabling chemicals, including chlorine and liquid bleach; and many additional items that may be seemingly harmless but could be used as weapons. During the passenger screening process, transportation security officers follow standard operating procedures and utilize technology such as walk-through metal detectors and X-ray machines to detect prohibited items either on a passenger's person or in his or her carry-on luggage. The passenger checkpoint screening process is composed of the following three elements:

5. 49 C.F.R. §§ 1542.101, 1540.107, and 1540.111.

6. GAO, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved*, GAO-07–634 (Washington, D.C.: Apr. 16, 2007).

The process of screening a passenger who continues to alarm the walk-through metal detector provides an example of how these three elements intersect. According to TSA's Screening Checkpoint Standard Operating Procedures manual, a passenger who continues to alarm the walk-through metal detector must be screened using a hand-wand search. Passengers may alternatively request a full-body pat-down search. The manual describes the process that transportation security officers are to follow during the additional screening, which includes the use of ETD swabbing and a pat-down of the passenger to detect any irregularities in their body contour that could represent concealed items.

- **Transportation security officers** (also known as TSOs) screen all passengers and their carry-on luggage prior to allowing passengers access to their departure gates. Among other responsibilities, transportation security officers attempt to detect prohibited items that passengers may try to carry beyond the security checkpoint.
- **Technology** is used during the screening process, which primarily consists of walk-through metal detectors, X-ray machines, handheld metal detectors, and explosive trace detection (ETD) equipment.[7]
- **Standard operating procedures** establish the process and standards by which transportation security officers are to screen passengers and their carry-on items at screening checkpoints.

### TSA Efforts to Improve the Passenger Screening Process

TSA faces a significant challenge in balancing security concerns with efficient passenger movement. In our April 2007 report, we described how TSA monitors transportation security officer compliance with passenger checkpoint screening procedures through its performance accountability and standards system and through testing.[8] Compliance assessments include quarterly observations of transportation security officers' ability to perform particular screening functions in the operating environment, quarterly quizzes to assess their knowledge of procedures, and an annual knowledge and skills assessment. TSA conducts tests to evaluate, in part, the extent to which transportation security officers are able to detect simulated threat items hidden in accessible property or concealed on a person. TSA modifies its standard operating procedures based on the professional judgment of TSA senior-level officials and program-level staff, daily experiences of airport staff, complaints and concerns raised by the traveling public, and an analysis of risks to the aviation system. For example, in December 2005, TSA modified its prohibited items list to allow passengers to carry certain scissors and tools as long as they did not exceed a certain length. TSA's stated purpose in removing certain scissors and tools from the prohibited items list was to shift the focus of transportation security officers from items considered by TSA to pose a low threat to items considered to pose a high threat.

## CREATING FUNCTIONING IED AND IID DEVICES

Investigators found instructions on the Internet for creating both an IED and IID and purchased the components from the Internet and from a local store for approximately $150. The IED was conceived as a two-part

7. ETD works by detecting explosive vapors and residue. Human operators collect samples by rubbing swabs along an object, such as a carry-on suitcase. They then place the swabs in an ETD machine. The ETD machine chemically analyzes the swab to identify traces of explosive materials.
8. GAO-07–634.

device—a detonator component that, on its own, could function as an IED, and a mixture of fuel and oxidizer that would require the explosion of the detonator.[9] Although the detonator component could be considered an IED, for the purposes of this report, we are referring to the combination of the detonator and the liquid explosive as a single IED. Information about liquid explosives was publicly available on several Web sites and discussed in media articles related to various terror plots, including the failed London subway bombing of July 21, 2005, and the transatlantic bomb plot of August 2006. In addition, we obtained information about creating an IID from the Internet. We also found videos on the Internet of the intense fire resulting from an IID. One of the components for the IID is a liquid that TSA prohibits passengers from bringing through security checkpoints. Specific details regarding the device components and the methods of concealment we used during our covert testing are classified by TSA; as such, they are not discussed in this testimony.

A group of tests conducted in February 2006 and July 2007 show that the IED proposed for this investigation functions as intended.[10] In 2006, within the scope of our original covert testing report, we worked with a law enforcement organization in the Washington, D.C., metro area to confirm that the detonator would function as an IED. A test performed by local law enforcement officials confirmed that the detonator would cause damage to an aircraft and threaten the safety of passengers. Because our proposed IED for this investigation was composed of two parts (the detonator and the liquid explosive), in July 2007 we sought assistance to confirm that this more complex IED would function as intended. Several tests conducted at a national laboratory demonstrated that this IED can function as intended, with the initial explosion by the detonator successfully causing the liquid explosive to detonate in several tests. Explosion data indicate that this device exploded with a force sufficient to cause severe damage to an aircraft. The IID is a far simpler device. Our work with a law enforcement organization in the Washington, D.C., metro area in February 2006 confirmed that the components of the IID (one of which is a liquid) could function as intended, causing damage to an aircraft and threatening the safety of passengers.

## TESTING AT 19 AIRPORT SECURITY CHECKPOINTS

Our investigators devised methods that would allow them to conceal the prohibited components for these devices from transportation security officers. During this planning phase, they considered publicly advertised TSA policies related to liquids and other items, including prohibited items. They

9. Many chemical explosives consist of a mixture of oxidizer and fuel. When heat is added to the mixture, an explosion occurs.

10. This testimony was revised on November 16, 2007, to include a link to digital video. This digital video shows test footage of the IEDs and IID that GAO investigators successfully brought through airport security checkpoints. The video was shot during the 2006 and 2007 tests: http://www.gao.gov/media/video/gao-08–48t/

also judged that some components could be hidden in either their carry-on luggage or on their persons. They developed covert test procedures to challenge TSA screening measures using these components and methods. Specific details regarding the methods of concealment we used are classified by TSA; as such, these details are not discussed in this testimony.

By using various concealment methods, our investigators demonstrated that it is possible to bring the components for several functioning IEDs and one functioning IID through checkpoints and onto airline flights without being challenged by transportation security officers. In most cases, transportation security officers appeared to follow TSA procedures and used technology appropriately; however, we uncovered weaknesses in TSA screening procedures and other vulnerabilities as a result of these tests. For example, although transportation security officers generally enforced TSA's 3–1-1 rule, we were able to bring a liquid component of the IID undetected through checkpoints by taking advantage of weaknesses we identified in TSA's policies based on a review of public information. TSA determined that specific details regarding these weaknesses are sensitive security information and are therefore not discussed in this testimony. We did not notice any difference between the performance of private screeners and transportation security officers during our tests.

### Covert Test Series One

From March 19 through March 23, 2007, two investigators tested the TSA checkpoint screening process at a number of U.S. airports. Transportation security officers did not interact with our investigators at every airport. Interactions that did occur included the following:

- On March 19 and March 20, 2007, transportation security officers advised our investigators to use a 1-quart clear plastic bag rather than the larger bags they were using, but did not require them to do so before passing through the checkpoint.
- Also at another airport, on March 23, 2007, a transportation security officer did not allow one investigator to bring a small, unlabeled bottle of medicated shampoo through the checkpoint. This was a legitimate toiletry item used by one of our investigators. The officer cited TSA policy and stated that since the bottle was not labeled, "it could contain acid." She did not allow our investigator to bring the unlabeled medicated shampoo bottle through the checkpoint. However, a liquid component of the IID—despite being prohibited by TSA—was allowed to pass undetected through the checkpoint. We had identified this weakness based on a review of public information before performing our tests.

### Covert Test Series Two

From May 7 through May 9, 2007, two investigators tested the TSA checkpoint screening process at a number of U.S. airports. Transportation security officers did not interact with our investigators aside from the following:

- On May 8, 2007, one investigator deliberately placed coins in his pockets to ensure that he would receive a secondary inspection. The transportation security officer

used a hand-wand and performed a pat-down search of our investigator. However, the transportation security officer did not detect any of the prohibited items our investigator brought through the checkpoint.

### Covert Test Series Three

From June 5 through June 8, 2007, two investigators tested the TSA checkpoint screening process at a number of U.S. airports. Transportation security officers did not interact with our investigators at every airport. Interactions that did occur included the following:

- Inclement weather forced our investigators to change their flight plans at one airport. After changing their plans, they were selected for secondary inspection at the TSA security checkpoint. Transportation security officers performed pat-downs at the checkpoint. However, the transportation security officers did not detect any of the prohibited items our investigators brought through the checkpoint.

## CORRECTIVE ACTION BRIEFINGS

We briefed TSA officials on August 16, 2007, and September 5, 2007, to discuss our findings. Officials from TSA's Security Operations Office were present during our second briefing. At these briefings, we suggested that TSA consider how the results of our covert testing should affect its risk-based approach to airport security. This could include implementing one or more measures to reduce the likelihood that terrorists could successfully bring IED and IID components through checkpoints using a similar methodology to ours in the future.

The specific nature of our suggestions to TSA is considered sensitive security information. Put generally, we suggested that, among other things, TSA (1) establish, depending on airport capacity, one or more special passenger screening lines to screen individuals based on risk and individuals with special needs; (2) introduce more aggressive, visible, and unpredictable deterrent measures into the passenger screening process at airports nationwide, to potentially include the implementation of enhanced individual search procedures (e.g., pat-downs and hand-wand screening) to detect concealed components; and (3) continue to develop and deploy new technology to be used at passenger screening checkpoints that would be able to better detect concealed components.

TSA officials indicated that they did not disagree with our suggestions in principle and that they would examine them closely to determine whether and how they should be implemented. They acknowledged vulnerabilities in human capital, processes, and technology. They also indicated that they are deploying additional specialized personnel to enhance security at existing checkpoints and that they are exploring methods for enhancing transportation security officer training and transforming the culture of their workforce. Regarding standard operating procedures, officials said that they are continuously revisiting and revising their policies. They also indicated that they were

moving forward to develop a "checkpoint of the future" that would incorporate new and emerging technology to address terror threats. Such technology could include innovative imaging techniques.

## CONCLUSION

Our tests clearly demonstrate that a terrorist group, using publicly available information and few resources, could cause severe damage to an airplane and threaten the safety of passengers by bringing prohibited IED and IID components through security checkpoints. Given our degree of success, we are confident that our investigators would have been able to evade transportation security officers at additional airports had we decided to test them. We understand the challenges TSA faces in balancing security risks with the efficient movement of passengers; however, from a strict security standpoint, current policies allowing substantial carry-on luggage and related items through TSA checkpoints increases the risk of a terrorist successfully bringing an IED, an IID, or both onto an aircraft undetected. Even if current carry-on luggage policies are left unchanged, our testing shows that risks can be reduced through improvements in human capital, improved processes, and continued advances in technology.

GAO is currently performing a more systematic review of these issues and expects to issue a comprehensive public report with recommendations for TSA in early 2008.

Mr. Chairman and Members of the committee, this concludes our statement. We would be pleased to answer any questions that you or other members of the committee may have at this time.

## GAO CONTACTS

For further information about this testimony, please contact Gregory D. Kutz at (202) 512–6722 or kutzg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony.

*This page intentionally left blank*

# Index

# About the Editor and Contributors

ANDREW R. THOMAS is assistant professor of marketing and international business and associate director of the Taylor Institute for Direct Marketing at the University of Akron. He is founding editor-in-chief of the *Journal of Transportation Security*, the first peer-reviewed journal dedicated to the study and practice of this critical business component. A *New York Times* best-selling writer, Dr. Thomas is author, coauthor, or editor of:

- *Supply Chain Security and Innovation*
- *The Distribution Trap!*
- *Direct Marketing in Action: Proven Strategies for Finding and Keeping Your Best Customers*
- *The New World Marketing*
- *Growing Your Business in Emerging Markets: Promise & Perils*
- *The Rise of Women Entrepreneurs: People, Processes, and Global Trends*
- *Defining the Really Great Boss*
- *Managing by Accountability: What Every Leader Needs to Know About Responsibility, Integrity—and Results*
- *Change or Die! How to Transform Your Organization from the Inside Out*
- *Aviation Security Management*
- *Aviation Insecurity: The New Challenges of Air Travel*
- *Air Rage: Crisis in the Skies*

Dr. Thomas has published articles in leading management journals such as *MIT Sloan Management Review*, *Business Horizons*, and *Marketing Management*. He is a regularly featured analyst for BBC, UNIVISION, FOX NEWS,

and CNBC. He has been interviewed by more than 800 television and radio stations around the world. A successful global entrepreneur, Professor Thomas has traveled to and done business in more than 120 countries on all seven continents.

GARY E. ELPHINSTONE, adviser to the editor, is currently managing director of AVSEC AusAsia Pty Ltd., an international aviation security consultancy. Elphinstone's distinguished career in aviation began with the Royal Australian Air Force, where he specialized in signals intelligence and communications. During his service, he was promoted to serve at the British GCHQ, Hong Kong, for two and half years and, later, served as a fully rated flight services officer with the then Australian Department of Civil Aviation (DCA), working out of Sydney International Airport, Airways Operations. This was followed by an engagement with NASA at the deep space tracking station DSS 42, participating as electronics communications technician in a support role for the Apollo missions 8–13 and other NASA Deep Space Network programs. He rejoined the Federal Department of Aviation's Security Branch in 1978 and subsequently was chosen for an assignment with ICAO (the International Civil Aviation Organization) as aviation security adviser team leader with the aviation security project team, based in Thailand. The ICAO project (RAS 087/003) provided assistance to some 23 countries with the purpose of enhancing the capabilities of governments in the region to minimize acts of unlawful interference against civil aviation. This was the forerunner to the current ICAO USAP (Universal Security Audit Programme). Elphinstone retired from government service in 1997 as superintendent AVSEC Western Region, after 19 years. He resides with his family in Perth, Australia.

JAMES JAY CARAFANO is a leading expert in defense affairs, military operations and strategy, and homeland security at the Heritage Foundation. An accomplished historian and teacher, Carafano was an assistant professor at the U.S. Military Academy in West Point, NY, and served as director of military studies at the Army's Center of Military History. He also taught at Mount Saint Mary College in New York and served as a fleet professor at the U.S. Naval War College. He is a visiting professor at the National Defense University and Georgetown University. Carafano is the author of several military history books and studies. His latest is *GI Ingenuity: Improvisation, Technology and Winning World War II* (2006). Carafano also is the coauthor of *Winning the Long War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom* and the textbook, *Homeland Security*. Carafano was also a contributing author to the National Academies Army Science and Technology for Homeland Security 2004 report and codirector of the task force report, DHS 2.0: *Rethinking the Department of Homeland Security*. His other works include: *Waltzing into the Cold War*; published in 2002 by Texas A&M University; and *After D-Day*, a Military Book Club main selection published in 2000 by Lynne Rienner. As an expert on defense, intelligence,

and homeland security issues, he has testified before the U.S. Congress and has provided commentary for, among others, ABC, BBC, CBS, NBC, PBS, National Public Radio, the History Channel, Voice of America, Al Jazeera, Telemundo, and Al Arabiya. His editorials have appeared in newspapers nationwide, including the *Baltimore Sun*, the *Boston Globe*, the *New York Post*, the *Philadelphia Inquirer*, *USA Today*, and the *Washington Times*. Before becoming a policy expert, he served 25 years in the Army, rising to the rank of lieutenant colonel. His areas of expertise included military strategy, joint operations, future combat systems, postconflict operations, and nuclear weapons. Before retiring, he was executive editor of *Joint Force Quarterly*, the Defense Department's premier professional military journal. Carafano is a member of the National Academies Board on Army Science and Technology and the Department of the Army Historical Advisory Committee, and he is a senior fellow at the George Washington University's Homeland Security Policy Institute. A graduate of West Point, Carafano also has a master's degree and a doctorate from Georgetown University and a master's degree in strategy from the U.S. Army War College.

JEFFREY P. COHEN is an associate professor of economics in the Barney School of Business at the University of Hartford, in West Hartford, Connecticut. Professor Cohen has been a visiting scholar at the Federal Reserve Bank of St. Louis and is president-elect of the Transportation and Public Utilities Group (TPUG) of the Allied Social Sciences Association. He has published his research in leading economics journals on topics in urban and regional economics, public finance, and transportation. Professor Cohen is a member of the editorial board of the *Journal of Transportation Security*. He was a scholar-in-residence at New York University during the academic year 2007–8.

CLETUS C. COUGHLIN is a vice president and deputy director of research at the Federal Reserve Bank of St. Louis. He is also a policy associate with the Leverhulme Centre for Research on Globalisation and Economic Policy at the University of Nottingham, Nottingham, England. Dr. Coughlin has published numerous articles in leading economics journals and the bank's *Review* on topics in both international and regional economics.

FULVIO FASSONE is the vice president/commercial of SAGAT Turin Airport. He is also the Chairman of ATRI (the Association of Italian Travel Retail) and vice chairman of ETRC (the European Travel Retail Council).

DIANA HARDMEIER, MSc UZH, studied psychology, business management, and journalism at the University of Zurich and is a doctoral student with the Visual Cognition Research Group at the University of Zurich. Since 2006, she has also been research associate at Zurich State Police, Division of Airport Police, responsible for quality control.

ROSS RUDESCH HARLEY is an award-winning artist and writer. His video and sound work has been presented at the Pompidou Centre in Paris, New York's MoMA, Ars Electronica in Austria, and the Sydney Opera House.

His recent work includes Aviopolis (with Gillian Fuller), a multimedia project and book about airports, Black Dog Publications, London; Busface, a photo-media installation with the Ejecutivo Colectivo exhibited at ArtBasel, Miami; and the DVD installation Cloudscope in collaboration with Durbach | Block architects at Elizabeth Bay House, Sydney. He is a former editor of the journal *Art + Text*, and has written regular columns on design and popular culture for *Rolling Stone* and for the Australian national newspaper, *The Australian*. He has edited a number of anthologies, including *New Media Technologies* (1993), *Artists in Cyberculture* (1993) and *Before and After Cinema* (1999). Another, entitled *Parallel Histories in the Intermedia Age*, appeared in the summer of 2000. In 1992, he was the director of the influential International Symposium on Electronic Art (ISEA). He is currently senior lecturer in the School of English, Media and Performing Arts at the University of New South Wales, Sydney, Australia.

WILLIAM J. HAUSER is the associate director for the Taylor Institute of Direct Marketing and an assistant professor of marketing at the University of Akron. He received his PhD from the joint University of Akron/Kent State University PhD Sociology Program in 1979 and then completed a two year postdoctoral research fellowship at Washington University in St. Louis. Hauser has also served as a visiting assistant professor at West Virginia University and Washington University in St. Louis and taught part-time at the University of Akron from 1984 to 2003. He is currently an adjunct associate professor in the Department of Sociology. In 2001, Hauser received the Buchtel College of Arts and Sciences Part-time Teacher of the Year award. In 2003, he joined the Department of Marketing as a full-time, tenure-track faculty member. For over 20 years, he has served as the manager of market research and business development for Rubbermaid Incorporated and its Little Tikes subsidiary. During this time, he was responsible for all domestic and global market research and helped Rubbermaid introduce numerous new product categories and businesses. He also coordinated the annual strategic plan and coauthored the strategic market plans for Rubbermaid's entry into Europe and Japan. Most recently, Hauser was senior vice president and director of research and planning for KeyCorp in Cleveland, Ohio. He is also a member of the Marketing Institute of Ireland. He has also completed numerous consulting projects for small businesses and social agencies and was the recipient of the Summit County United Way's Community Builder Award in 2003.

ERIK HOFFER is a graduate of Northeastern University, holding a degree in industrial psychology. He also holds an associate's degree in transportation and traffic management from New York University. He recently retired from the company he founded in 1977, which is now a public corporation manufacturing his patented technologies in barrier and indicative sealing devices. After a short retirement of almost 1.5 hours, he began a new company in southwest Florida, manufacturing more of his patented antitheft devices for trucks and trailers as well as wide array of cargo seals and locks. Mr. Hoffer has over 20

original product technologies to his credit, along with many patents. He began his cargo security career in the military in 1965 and was trained in that area in 1966–67 in Viet Nam. He is the former chairman of educational events at the International Cargo Security Council, where he served in that capacity for five years. He has also chaired the council's Seal Committee. He is an active member of the Navy Lock and Seal engineering group, dealing in cargo security devices and new technology, and he has consulted regularly with the TSA, the DHS, and the Department of State on air, sea, and truck cargo security issues. He holds an active security clearance. He has taught cargo security at over 50 venues over the last 25 years and crafted the original master's program in cargo security for the GMATS (the Global Maritime and Transportation School at the Merchant Marine Academy, Kings Point, New York).

SHELDON H. JACOBSON, PhD, is a professor and director of the Simulation and Optimization Laboratory in the Department of Computer Science at the University of Illinois at Urbana–Champaign.

DAVID JARACH is a professor of marketing at Bocconi University, Milan, and senior professor of air transportation marketing at SDA Bocconi Business School, Milan. He is a visiting professor at Toulouse Business School, France, Aerospace MBA, and a member of the World Network Committee of Air Transport Research Society (ATRS). He sits on the editorial board of the *Journal of Air Transportation*, *Journal of Airport Management*, and *Journal of Transportation Security*. He acts as an advisor to the leading international players in the air transportation value chain through his own all-aviation consultancy.

Prof. Jarach has published four books (in Italian, English, and Chinese), dozens of academic articles, and hundreds of commentary articles in the international media about airline and airport marketing management practices. He is frequently interviewed by the main broadcasting media on aviation topics.

SAROSH R. KHAN is a graduate student in the Master of Public Administration in International Development (MPA/ID) program at the John F. Kennedy School of Government, Harvard University. His research interests include international development and the political economy of capital markets. Previously, Sarosh held positions at the International Monetary Fund, at the Federal Reserve Bank of St. Louis, and in the private sector.

ADRIAN J. LEE is a PhD candidate in the Department of Mechanical Sciences and Engineering at the University of Illinois at Urbana–Champaign.

JOHN J. NESTOR, PhD, is an operations research analyst in the Transportation Security Administration within the U.S. Department of Homeland Security.

ALEXANDER G. NIKOLAEV is a PhD candidate in the Department of Industrial and Enterprise Systems Engineering at the University of Illinois at Urbana–Champaign.

MARK B. SALTER is associate professor at the School of Political Studies, University of Ottawa. He received a master's degree from the London School of Economics and a doctorate from the University of British Columbia. He is currently associate editor of the *Journal of Transportation Security*, and has edited two books on airports, borders, and security: *Politics at the Airport* and *Global Policing and Surveillance* (with Elia Zureik). He is the author of *Rights of Passage: The Passport in International Relations*, and has also published articles in *International Political Sociology*, *Alternatives*, *Security Dialogue*, and the *Journal of Air Transport Management*. He has also acted as a consultant for the Canadian Air Transport Security Authority, Transport Canada, and the Canadian Human Rights Commission, and has presented at numerous conferences, including AVSEC World and the Canadian Aviation Security Conference. In 2007, he was the recipient of the National Capital Educator's Award and the Excellence in Education Prize at the University of Ottawa.

ANNEMARIE SCARISBRICK-HAUSER is currently an independent business intelligence consultant. She has spent 20 years as a research consultant in both the academic and business worlds, directing the design and implementation of business intelligence systems supported by robust governance processes. As a former senior vice president and manager of Enterprise Business Intelligence at KeyCorp in Cleveland, Ohio, she was responsible for enterprise information management for the nation's 13th largest banking institution. Prior to joining Key, she was the associate director of the Survey Research Center at the University of Akron. Scarisbrick-Hauser has earned a PhD in sociology and an MA in research methodology from the University of Akron, an MS in recreation management from Purdue University, and a BA in physical education from the University of Limerick, Ireland. She is a Six Sigma black belt and an adjunct professor at the University of Akron, where she teaches courses in research methods, assessing the social impact of disasters, collective behavior, emergency management, health policy, and digital marketing strategy. Over the past 20 years, Scarisbrick-Hauser has been integrally involved in all aspects of business intelligence, data governance, enterprise data management, data mining, and analytics. She has completed over 135 research projects for a diverse group of internal and external clients. She has presented at numerous domestic and international academic and professional conferences, in many cases as the keynote speaker. She has also published in numerous journals and has coauthored a book on applied sociology.

Prof. ADRIAN SCHWANINGER has lectured at the University of Zurich and at the Federal Institute of Technology (ETH) in Zurich since 1999 and at the University of Applied Sciences Northwestern Switzerland since 2008. He is a member of the Training and Technical Task Forces of the European Civil Aviation Conference (ECAC), the moderator of the ECAC Technical Task Force TIP Study Group, and the chairman of the InterTAG ad hoc Working Group on Competency Assessment. In 1999 he received the Young

Researcher Award in Psychology. In 2003 he received the ASI International Award of Excellence in Aviation Security: Enhancement of Human Factors. Together with his Visual Cognition Research Group (VICOREG), he is in charge of several aviation security projects in Belgium, Bulgaria, Canada, France, Germany, Greece, Norway, Romania, Sweden, Switzerland, the Netherlands, and the United States of America.

KATHLEEN SWEET is currently an associate professor of worldwide global intelligence and security at Embry Riddle Aeronautical University. She formerly taught courses in aviation security, terrorism, and strategic intelligence in the Department of Aviation Technology at Purdue University. She is CEO and president of Risk Management Security Group and is certified by the United Kingdom and Irish Department of Transport to teach air cargo security. Dr. Sweet received her undergraduate degree from Franklin and Marshall College in Lancaster, Pennsylvania, in Russian area studies, and she has a master's degree in history from Temple University. She also has been admitted to the bar in Pennsylvania and Texas after graduating from Beasley School of Law in Philadelphia. She is a graduate of many Air Force and civilian training programs. After graduating from law school, Dr. Sweet joined Wyeth International Pharmaceuticals as a legal specialist. She later joined the U.S. Air Force and initially was a member of the Judge Advocate General's Department. After 15 years as a JAG, and generally engaged in prosecuting cases on behalf of the military, she transferred to the 353rd Special Operations Wing as a military political affairs officer. She was later an intelligence officer assigned to HQ AMC as an executive officer and briefer. In 1995, she became an assistant air attaché to the Russian Federation. As an attaché, she was engaged in liaison work not only with the Russian Air Force but also the Federal Security Bureau. Her final assignment was as an instructor at the Air War College where she taught in the International Security Studies Division. She later became an associate professor at St. Cloud State University in the Department of Criminal Justice and an associate professor at Embry Riddle Aeronautical University, teaching security- and intelligence-related courses. She is the author of four books, *Terrorism and Airport Security*; *Aviation and Airport Security: Terrorism and Safety;* and *The Transportation Security Directory* Her fourth book, *Transportation and Cargo Security: Threats and Solutions*, was published in late 2005. She is considered an expert in the field of airport, aviation, and air cargo security and has been well published in the fields of international space programs and associated treaties, space-based offensive weapons, bioterrorism, and aviation security. Her company, Risk Management Security Group, doing business in Ireland as RMSG Ireland Ltd., engages in all aspects of consulting in transportation-related security, including the preparation of threat and vulnerability assessments and security awareness training.

*This page intentionally left blank*

# Aviation Security Management

# Aviation Security Management

## Volume 3

## Perspectives on Aviation Security Management

Edited by
Andrew R. Thomas

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

**Library of Congress Cataloging-in-Publication Data**

Aviation security management / edited by Andrew R. Thomas.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978–0–313–34652–1 ((set) : alk. paper)
ISBN-13: 978–0–313–34654–5 ((vol. 1) : alk. paper)
ISBN-13: 978–0–313–34656–9 ((vol. 2) : alk. paper)
ISBN-13: 978–0–313–34658–3 ((vol. 3) : alk. paper)
1. Airlines—Security measures. I. Thomas, Andrew R.
HE9776.A95 2008
363.28'76068—dc22 2008018728

British Library Cataloguing in Publication Data is available.



Library of Congress Catalog Card Number: 2008018728

ISBN-13: 978–0–313–34652–1 (set)
978–0–313–34654–5 (vol. 1)
978–0–313–34656–9 (vol. 2)
978–0–313–34658–3 (vol. 3)

First published in 2008

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the United States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48–1984).

10 9 8 7 6 5 4 3 2 1

# Contents

# Preface

Because of September 11, there is an almost universal recognition that aviation security is a deadly serious business. Yet, still, today around the world, the practice of aviation security is rooted in a hodgepodge of governmental rules, industry traditions, and local idiosyncrasies. In fact, seven years after the largest single attack involving the air transport industry, there remains no viable framework in place to lift aviation security practice out of the mish-mash that currently exists. The purpose of this three-volume set is to begin to change that. It is my sincere hope that this work, written from a truly global point of view, will be the first of many on this most important topic.

The fact that over half of the contributors to this set come from outside of the United States is no coincidence. Although roughly 40 percent of all air transport today takes place within the United States, the long-term trend is for dramatic increases in global system usage, driven by high-growth emerging markets like China, India, Russia, and Brazil. It is widely estimated that the total volume of passengers and cargo moved via the international air transport system will nearly triple in the next 25 years. Although America will remain the single largest player, the surge will come from emerging markets.

This evolving reality mandates that aviation security management be viewed not merely on a country by country basis, but as a global endeavor, where best practices—regardless of where they originate—are integrated into a new paradigm that is truly global in scope and scale. With that in mind, *Aviation Security Management* is intended to serve as a foundation for researchers, practitioners, and educators around the world who are looking to develop new knowledge and pass it along to the next generation of aviation security managers.

Dishearteningly, however, there id only a handful of academic programs—currently less than a dozen—where someone can actually study transportation security management. The number of schools where an aviation security management curriculum is available is even smaller. Such a lack of educational opportunities means that unless something is done quickly, the tens of thousands of new aviation security mangers who will join the profession in the coming years will not have had the opportunity to learn the best in transportation security management research and practice.

To professionalize the field of transportation security management, in general, and, aviation security management, in particular, several requirements need to be met. First and foremost, there must be a body of knowledge and a repertoire of behaviors and skills needed in the practice of the profession, knowledge, behavior, and skills that are not normally possessed by the nonprofessional. To date, very little of that body of knowledge and repertoire exists in a clear and cogent format. While many researchers and practitioners across multiple disciplines have been engaged in their own worthwhile pursuits, there remains a deficiency in the availability of clearinghouses for that knowledge. Bluntly asked, where does one go to learn about the emerging ideas, thoughts, technologies, and best practices in transportation and aviation security management?

Clearly there is neither the need nor the desire to provide those who seek to harm transportation networks with information they can use against us. As researchers, practitioners, and educators, we must be ever vigilant, striving to balance the need for open knowledge with the necessary parameters of sensitive information. I am certain we can do both—that is, provide cutting-edge knowledge to a growing body of well-intentioned researchers and practitioners while maintaining the integrity needed to ultimately make transportation more secure.

Which brings us back to those clearinghouses. This set of volumes and with the recently founded *Journal of Transportation Security* are intended to be some of the first building blocks of a much more extensive foundation, which will ultimately serve to prepare for the arrival of a true profession: transportation security management.

Having previously set the context and identified some of the key elements of aviation security management in the previous volumes, this third volume constitutes what is intended to serve as part of the foundation for the next generation of research in the area.

The first chapter, by Ruwantissa I. R. Abeyratne, details the efforts of the International Civil Aviation Organization (ICAO) to build and foster a working culture of security among the nations of the world. In the same light, Charles M. Bumstead argues that a global aviation security management crisis team would go a long way to resolving disputes between stakeholder groups.

As passenger screening becomes seemingly more cumbersome and widespread, Anthony T. H. Chin of the National University of Singapore discusses the possible uses of scientific content analysis (SCAN), a technique that

analyzes linguistic structure and content, in the aviation security realm. Terry Sheridan introduces the concept of emotive profiling. And, Adrian Schwaninger, Saskia M. Koller, and Anton Bolfing lay out principles and requirements for assessing X-ray image interpretation as it relates to the competency of aviation security screeners.

Challenging the status quo of current aviation security strategy, Professor Chien-tsung Lu puts forth his notion of constructing a comprehensive aviation security management model (ASMM). So does Jeffrey Ian Ross in his look at the growing pains faced by the U.S. Transportation Security Administration.

Looking at the cabin environment, two world-class experts lay out the future of this ever-changing area: David E. Forbes and Michael Tunnecliffe.

Reminding us that aviation security is a business component, Clinton V. Oster, Jr., and John S. Strong look at the associated funding and costs.

This volume and the entire set of volumes conclude with Mark B. Salter's analysis of the overall future of aviation security management.

The appendix contains a report from the U.S. Government Accountability Office that details progress made in aviation security since the September 11 attacks as well as the challenges that remain.

It is my heartfelt desire that this dynamic set should showcase the most current trends, issues, ideas, and practices in aviation security management, especially as the field evolves in the context of globalization and advances in technology, and address the salient issues concerning aviation security management so as to lay the foundation for the professionalization of this field of endeavor for future generations.

*Andrew R. Thomas, University of Akron*
*Editor*

*This page intentionally left blank*

# CHAPTER 1

# The Efforts of ICAO in Ensuring a Security Culture among States

*Ruwantissa I. R. Abeyratne*

## THE SECURITY CRISIS

Since the events of September 11, 2001, took place, the most critical challenge facing international civil aviation has been the compelling need to ensure that the air transport industry remains continuous in its operations, and that its consumer is assured of sustained regular, safe, and secure air transport services. The Air Transport Association (ATA), in its 2002 State of the United States Airline Industry Statement, advised that, in the United States, the combined impact of the 2001 economic downturn and the precipitous decline in air travel following the September 11, 2001, attacks on the United States had resulted in devastating losses for the airline industry that were likely to exceed $7 billion and continue through 2002.[1] Of course, the overall picture, which portended a certain inevitable gloom for the air transport industry, was not the exclusive legacy of United States' carriers. It applied worldwide, as was seen in the abrupt downturn of air traffic globally during 2001. The world community's retaliation against terrorism, which is an ongoing feature in world affairs, increased the airline passenger's fear of air transport and reluctance to use it. In most instances in commercial aircraft purchasing, air carriers canceled or postponed their new aircraft requisition orders. Many carriers, particularly in developing countries, were seen revisiting their cost structures and downsizing their human resource bases. It is incontrovertible

The author is coordinator, air transport programs, at the International Civil Aviation Organization in Montreal. He has written this article in his personal capacity and the views expressed herein do not necessarily reflect those of ICAO.

that another similar event or series of events will inevitably plunge the aviation industry into similar despair and destitution.

In order to arrive at where we are at the present time with regard to the results of the global measures taken by the International Civil Aviation Organization (ICAO), it is necessary to discuss the various steps taken from a regulatory perspective by ICAO, in its role as regulator and mentor of international civil aviation, in countering imminent threats to the sustainability of the air transport industry.

## The ICAO High-Level Ministerial Conference

At the 33rd Session of its ICAO Assembly, held from September 25 to October 5, 2001, ICAO adopted Resolution A33–1, entitled the *Declaration on Misuse of Civil Aircraft as Weapons of Destruction and Other Terrorist Acts Involving Civil Aviation*.[2] This resolution, while singling out for consideration the terrorist acts that occurred in the United States on September 11, 2001, and, inter alia, recognizing that the new type of threat posed by terrorist organizations requires new concerted efforts and policies of cooperation on the part of states, urged all contracting states to intensify their efforts to achieve the full implementation and enforcement of the multilateral conventions on aviation security, as well as the implementation and enforcement of the ICAO standards and recommended practices and procedures (SARPs) relating to aviation security, to monitor such implementation, and to take within their territories appropriate additional security measures commensurate to the level of threat, in order to prevent and eradicate terrorist acts involving civil aviation. The resolution also urged all contracting states to make contributions in the form of financial or human resources to ICAO's aviation security mechanism, in order to support and strengthen the combat against terrorism and unlawful interference in civil aviation; it called on contracting states to agree on special funding for urgent action by ICAO in the field of aviation security; and it directed the ICAO Council to develop proposals and take appropriate decisions for a more stable funding of ICAO action in the field of aviation security, including appropriate remedial action.

Resolution A33–1 also directed the ICAO Council to convene, at the earliest date, a high-level international ministerial conference on aviation security in Montreal with the objectives of preventing, combating, and eradicating acts of terrorism involving civil aviation; of strengthening ICAO's role in the adoption of SARPs in the field of security and the auditing of their implementation; and of ensuring the necessary financial means to strengthen ICAO's AVSEC mechanism, while providing special funding for urgent action by ICAO in the field of aviation security.

On February 19 and 20, 2002, in keeping with the requirement of Assembly Resolution A33, a high-level ministerial conference on aviation security was held in the headquarters of the International Civil Aviation Organization, Montreal. In the words of Dr. Assad Kotaite, president of the ICAO Council,

who opened the conference (and later served as its chairman), the conference was being held "at a critical juncture for civil aviation and for society at large . . . and would review and develop global strategy for strengthening aviation security with the aim of protecting lives both in the air and on the ground, restoring public confidence in air travel and promoting the health of air transport in order that it can renew its vital contribution to the world economy."[3] Dr. Kotaite stated that this was a historic moment in the evolution of civil aviation.

At this conference, attended by member states of the International Civil Aviation Organization, some 714 participants from 154 contracting states and observers from 24 international civil aviation organizations endorsed a global strategy for strengthening aviation security worldwide and issued a public declaration at the conclusion of their two-day meeting.

The conference came to several conclusions and adopted numerous recommendations containing guidance for follow-up action. The conference concluded that the events of September 11, 2001, had had a major negative impact on world economies and an impact on air transport that was unparalleled in history and that the restoration of consumer confidence in air transport and assurance of the long-term health of the air transport industry were both vital, and that many states had already initiated a range of measures to this effect. It was also the view of the conference that the effective application of enhanced uniform security measures, commensurate with the threat, would help to restore confidence in air transport, but these measures would need to be passenger and cargo user friendly and not overly costly for the industry and its consumers if traffic growth was to be regenerated. Accordingly, the conference recommended that consistent with Assembly Resolution A33-1, states should intensify their efforts to achieve the full implementation and enforcement of the multilateral conventions on aviation security as well as of the ICAO standards and recommended practices (SARPs) relating to aviation security, and take within their territories appropriate additional security measures that would be commensurate with the level of threat and cost effective. Since the restoration of confidence in air transport is a collective responsibility, the conference called upon states to enhance international cooperation in aviation security and assist developing countries to the extent that this was possible.

With regard to the compelling need to strengthen aviation security worldwide, the conference concluded that a strong and viable aviation security (AVSEC) program was indispensable and that a uniform global approach to the implementation of the international aviation security standards was essential, while leaving room for operational flexibility. It was also considered useful to establish regional and subregional approaches which could make a significant contribution to ICAO's aviation security activities. The conference concluded that aviation security was a responsibility of contracting states, and states that outsourced aviation security programs should therefore ensure that adequate governmental control and supervision were in place.

The conference also observed that, since gaps and inadequacies appeared to exist in international aviation security instruments with regard to new and emerging threats to civil aviation, further study was needed in this regard. There was a need for a comprehensive ICAO aviation security plan of action for strengthening aviation security, through a reinforced AVSEC mechanism, an ICAO aviation security audit program, technical cooperation projects, and the promotion of aviation security quality control functions and appropriate performance indicators.

Based on the above conclusions, the conference recommended that states should take immediate action to lock flight deck doors for aircraft operated internationally, while maintaining measures on the ground to provide the highest level of aviation security. States were also requested to actively share threat information in accordance with the standards in Annex 17, to employ suitable threat assessment and risk management methodologies appropriate to their circumstances, based on a template to be developed by ICAO, and to ensure that aviation security measures were implemented in an objective and nondiscriminatory manner.

As for ICAO's role in this process, the conference recommended that the organization should develop, as a matter of high priority, amendments to the appropriate annexes to require protection of the flight deck door from forcible intrusion; should continue its efforts to identify and analyze the new and emerging threats to civil aviation with the purpose of assisting in the development of security measures and to actively collaborate with other associated agencies; should carry out a detailed study of the adequacy of the existing aviation security conventions and other aviation security–related documentation with a view to proposing and developing measures to close the existing gaps and remove the inadequacies, including amendments where required, so as to deal effectively with the existing as well as the new and emerging threats to international civil aviation; and should develop and take action to deal with the problem of aviation war risk insurance; and develop and implement a comprehensive aviation security plan of action and take any additional actions approved by the council, including a clear identification of priorities.

One of the key conclusions of the conference was that, in order to further enhance safety and security and to ensure the systematic implementation of the critical elements of a state's aviation security system, there was an urgent need for a comprehensive ICAO program of aviation security audits and that such a program should audit national level and airport level compliance with Annex 17 and with aviation security–related provisions of other annexes on a regular, mandatory, systematic, and harmonized basis. It was the view of the conference that the ability to determine whether an airport or state is in compliance will require that auditors have a solid aviation security background and be sufficiently trained and certified by ICAO to ensure that auditing is conducted in a consistent and objective manner. The conference was strongly convinced that such an audit program should be undertaken under the auspices of ICAO's AVSEC mechanism, which could be guided by proven and

successful concepts used in viable programs already developed by the European Civil Aviation Conference (ECAC), the United States, and other states in the development of the framework for a security audit program.

It was considered that the regional approach would have many benefits and was to be considered as supplementary to local initiatives, in particular in promoting regional partnership and the activities of the ICAO regional AVSEC training centers. The AVSEC Panel, which is an instrumentality of the ICAO Council, should assist in the development of the technical requirements and guidance materials needed to administer the audits and assist in the development of an effective quality assurance program to maintain the standards of audit performance; and since an audit program could provide the security levels of audited airports only at the time of the audit, a permanent mechanism based on quality control and the regular conduct of exercises and inspections could guarantee the continuity and improvement of the security levels determined by the audits.

Arguably, the most significant and seminal recommendation of the conference was that ICAO should establish a comprehensive program of universal, regular, mandatory, systematic, and harmonized aviation security audits, with implementation beginning in 2003 based on the final work plan established by the council. It was also decided that, in order to be effective, the program should be based on an audit process that uses ICAO trained and certified audit teams, which are headed by an ICAO staff member and which consistently apply fair and objective methods to determine compliance with Annex 17 by observing measures at airports and assessing the state's capabilities to sustain those measures.

The conference was of the view that of singular importance to the audit process was the need for the audit program to be established under the auspices of ICAO's AVSEC mechanism. It recommended that, in developing the audit program, which should be transparent and autonomous, ICAO should ensure the greatest possible coordination and coherence with audit programs already established at a regional or subregional level, taking into account aviation security situation in these states. For this to become a reality, a compliance mechanism had to be built into the program, a mechanism that would delineate between minor and serious areas of improvement, ensure that immediate corrective action was taken for serious deficiencies and provide to developing states the necessary assistance to measurably improve security.

With regard to funding an aviation security audit program to be run by ICAO, an adequate and stable source of funding was to be sought for the AVSEC mechanism through increased voluntary contributions until such time that an allocation of funds could be sought through the regular program budget, which was envisioned to be as soon as possible. It was recommended that all states be notified of a completed audit, that ICAO headquarters be the repository for full audit reports, and that the sharing of audit reports between states take place on a bilateral or multilateral basis. States were required, under such a program, to commit to provide ICAO with national AVSEC findings

based on a harmonized procedure to be developed by ICAO as early as possible. Of course, those states—in particular developing countries—should be provided with technical and financial assistance under technical cooperation, so that they might take remedial actions to rectify the deficiencies identified during the audit. States should also utilize the ICAO audits to the maximum extent possible and could always approach ICAO with regard to the audit findings for other states.

The conference also concluded that, in order to execute the ICAO plan of action, an indicative additional funding requirement was for a minimum of US$ 5.4 million through voluntary contributions for the triennium 2002–2003–2004, these figures to be used as a basis for further study by the council. However, for the longer term a more stable means of funding the ICAO plan of action would be either through an increase of the assessment to the ICAO General Fund for the following triennia, or by a long-term commitment, on a voluntary basis, of systematic contributions according to an approved suggested level of contribution, to be determined by the council, by all states. With regard to the recouping policies of states, the conference observed and confirmed that ICAO's policy and guidance material on the cost recovery of security services at airports in ICAO's *Policies on Charges for Airports and Air Navigation Services* (Doc 9082/6) and the *Airport Economics Manual* (Doc 9562) remained valid, although there was a need for the development of additional policy and guidance material on the cost recovery of security measures with regard to air navigation services, complementary to that which already existed with respect to airport security charges. There was also a need for further improvement of human resources, utilizing the existing training centers and the standardization of instruction materials, where appropriate, based on ICAO's TRAINAIR methodology.

On this basis, states were called upon by the conference to commit to provide adequate resources, financial, human and/or otherwise in kind, for the time being on a voluntary basis through the AVSEC mechanism, for the ICAO plan of action for the triennium 2002–2003–2004 as a matter of priority, and to be aware of the continuing needs for subsequent triennia. They were also called upon to agree to remove the existing ties they individually imposed on the expenditures of AVSEC mechanism contributions in order for ICAO to immediately utilize all funds available in the AVSEC mechanism trust funds. The conference observed that states might wish to use ICAO's technical cooperation program as one of the main instruments to obtain assistance in advancing the implementation of their obligations under relevant international conventions, and the standards and recommended practices (SARPs) of 17—"Security" and related provisions of other annexes, as well as adherence to ICAO guidance material.

As for ICAO's involvement and contribution, the organization was requested to establish an ICAO aviation security follow-up program and seek additional resources, as with the USOAP follow-up program of the Technical Co-operation Bureau, to enable states to obtain technical cooperation in the

preparation of necessary documentation and in resource mobilization for aviation security. It was felt that one of the ways in which this could be achieved was by ICAO's promoting the use of the ICAO objectives implementation mechanism as a means for states to obtain technical cooperation, as required for the rectification of deficiencies identified during aviation security evaluations and audits and urgently pursuing the development and implementation of an international financial facility for aviation safety (IFFAS), to encompass not only safety but also security.[4] Another significant function of ICAO was to elaborate on its policy and guidance material on cost recovery of security services, notably to include the development of policy and guidance material on cost recovery, through charges, of security measures with regard to air navigation services and to explore the issue of using security charges as a means of recovering the cost of ICAO assistance provided to states for security development projects.

## Postconference Work

In furtherance of the recommendations of the Conference, the ICAO Secretariat initiated an aviation security plan of action which was aimed at reviewing legal instruments, in particular the enhancement of Annex 17—"Security—Safeguarding International Civil Aviation against Acts of Unlawful Interference to the Convention on International Civil Aviation" (the work undertaken by the AVSEC panel and amendment 1010 to Annex 17) and the introduction or strengthening of security-related provisions in other annexes to the convention (Annex 1—"Personnel Licensing," Annex 6—"Operation of Aircraft," Annex 8—"Airworthiness of Aircraft," Annex 9—"Facilitation," Annex 11—"Air Traffic Services," Annex 14—"Aerodromes," and Annex 18—"The Safe Transport of Dangerous Goods by Air"). The plan of action also envisioned reinforcing AVSEC mechanism activities, notably in the preparation of security audits and in undertaking immediate/urgent assistance to states, and expediting work on improving technical specifications relating to and further implementing the use of machine readable travel documents (MRTDs), biometric identification, travel document security, and the improvement of border security systems. The reviewing of certain procedures for air navigation services (PANS) and revision of relevant ICAO manuals and other guidance material including further development of aviation security training packages (ASTPs), training programs, workshops, seminars, and assistance to states through ICAO's technical cooperation program were also on the program of implementation.

At that time, ICAO considered the development and execution of a comprehensive and integrated ICAO AVSEC plan of action as its highest priority. It is no less important to ICAO at the present time. The success of this plan of action was to be measured over a long period as the improvements expected in contracting would require an intensive and continuous worldwide commitment. It was expected that the full and active participation of all contracting states, as

well as all technical and deliberative bodies of ICAO, would be essential for the achievement of concrete results within an acceptable period of time.

The aviation security plan of action of ICAO was to focus on the development of new training and guidance material on national quality control (NQC), system testing, auditors, and audit guidelines and forms, with urgent distribution to all states, including the training and certification of international auditors through the existing ICAO aviation security training centers (ASTCs) network, which was to be reinforced and expanded where required. It was also expected to include undertaking universal, mandatory, and regular AVSEC audits to assess the level of implementation and enforcement by states of the SARPs contained in Annex 17, together with the assessment of security measures undertaken, on a sample basis, at airport level for each state. ICAO would maintain an ICAO AVSEC findings database. The creation of aviation security regional units (ASRUs) functionally linked to the AVSEC mechanism, to be urgently implemented in Africa, the Middle East, Eastern Europe, the Americas, and Asia and the Pacific, in order to coordinate the execution of AVSEC mechanism activities and provide direct assistance to states, was also be a feature of the plan.

The seminal consideration regarding ICAO's role in sustaining the aviation industry lies in the mandate of the organization, as contained in Article 44 of the Convention on International Civil Aviation.[5] In this context, ICAO's role throughout the past 63 years has been one of adapting to the trends as civil aviation has gone through three distinct phases of metamorphosis. The first phase was the modernist era that prevailed when the Convention on International Civil Aviation was signed at Chicago on December 7, 1944, an era centered on state sovereignty[6] and the widely accepted postwar view that the development of international civil aviation could greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet that its abuse could become a threat to general security.[7] This essentially modernist philosophy focused on the importance of the state as the ultimate sovereign authority, which could overrule considerations of international community welfare if they clashed with the domestic interests of the state. This gave way, in the 1960s and 1970s, to a postmodernist era of recognition of the individual as a global citizen whose interests in public international law were considered paramount over considerations of individual state interests.

The September 11, 2001, events led to a new era that calls for a neopostmodernist approach. This approach, as has been demonstrably seen after the events of September 11, 2001, admits of social elements and corporate interests being involved with states in an overall effort at securing world peace and security. The role of ICAO in this process is critical, since the organization is charged with regulating for safe and economic air transportation within the broad parameters of the air transport industry. The industry remains an integral element of commercial and social interactivity and a tool that could be used by the world community to forge closer interactivity between the people of the world.

In the above sense, ICAO's initiatives in the fields of aviation security in the immediate aftermath of the September 11 events have not been mere reactive responses but a visionary striving to ensure the future sustainability of the industry. Of course, this responsibility should not devolve upon ICAO alone. ICAO's regulatory responsibility can only be fulfilled through active regulatory participation by states.

## SECURITY MEASURES AND SECURITY CULTURE

### A Risk-Based Approach to Security

It must also be noted that a new dimension in the sabotage of aviation is damage caused by the hostile use of dirty bombs, electromagnetic pulse devices, or biochemical materials. Dirty bombs are devices that cause damage through nuclear detonation involving the spread of radioactivity to undetermined areas.[8] In recent years, man-portable air defense systems (MANPADS) have posed a serious threat to aviation security.

Studies have shown that stringent measures, when adopted against a particular type of crime belonging to a generic group (such as hijacking in the spectrum of unlawful interference against civil aviation), would be effective enough to reduce that particular type of crime. However, such measures might give rise to increase in other forms of crime belonging to that generic group. Called the spillover effect, this pattern has applied to civil aviation, as seen in the decrease in offences against aircraft after the events of September 11, 2001.

In order for basic strategies to be employed to prevent crime and to combat crime when prevention is impossible, crime prevention strategies adopt two methods of combating crime. The first method is to prevent or stop potential criminal acts. The second method is to apprehend and punish anyone who commits a criminal act. These methods follow the philosophy that the prevention of crime can be achieved by increasing the probability of apprehension and applying severe penal sanction to a crime. For example, the installation of metal detectors at airports increases the probability of detecting and apprehending potential hijackers or saboteurs. Theoretically the high risk of being apprehended decreases the potential threat, and the stringent penal sanction that may apply consequent to such apprehension compounds the ominous quality of the preventive means taken.

At the 36th Session of the ICAO Assembly ( Montreal, September 18–28, 2007), a resolution. was adopted, addressing a consolidated statement of continuing ICAO policies related to the safeguarding of international civil aviation against acts of unlawful interference. The assembly took note, inter alia, of the August 2006 threat to civil aviation operations posed by an alleged terrorist plot against civil aircraft over the North Atlantic that would have involved the component parts of an improvised explosive device including a homemade liquid explosive, being taken through the passenger and cabin baggage security checkpoint for assembly airside, probably on the aircraft. The resolution

recognizes new and emerging threats posed to aviation security, including those posed by the use of aircraft as a weapon of destruction, the targeting of aircraft by MANPADS, and other surface-to-air missile systems, light weapons and rocket-propelled grenades, unlawful seizure of aircraft, attacks on facilities and other acts of unlawful interference against civil aviation, acts aimed at the destruction of aircraft by carrying on board liquids, gels, and aerosols as component parts of an improvised explosive device, acts aimed at using the aircraft as a weapon of destruction, and the unlawful seizure of aircraft.

The resolution also notes that attacks on aviation facilities and other acts of unlawful interference against civil aviation have a serious adverse effect on the safety, efficiency, and regularity of international civil aviation, endangering the lives of persons on board and on the ground and undermining the confidence of the peoples of the world in the safety of international civil aviation.

It therefore concludes that all acts of unlawful interference against international civil aviation constitute a grave offence in violation of international law.

## MANPADS

It is evident that various global security measures have been taken since 2001. It is also clear that, in general terms, aviation security should be centered on identifying new and emergent threats to aviation and the attendant adoption of a risk-based approach. One of the ominous threats is the use MANPADS to destroy or damage aircraft in flight. As a result of the various security measures taken by the international community following the events of September 11, 2001. to strengthen aircraft against attacks on them,[9] attacks against aircraft, although still posing a threat, are not as prolific, having given way to attacks against facilities such as airports and allied service providers.[10] Generally, however, perceived threats to civil aviation remain hijacking of aircraft; aviation sabotage, such as the causing of explosions in aircraft on the ground and in flight; missile attacks against aircraft; armed attacks on passengers, airports, and other aviation-related property; and the illegal carriage of narcotics by air and its criminal ramifications. These threats are by no means new.[11]

MANPADS are extremely effective weapons that are widely available worldwide. Introduced in the 1950s and originally meant to deter terror attacks from air to ground and meant to be used by state authorities and other protection agencies, these weapons have gotten into the wrong hands and are being used against civil and military aviation. The surface-to-air MANPAD is a light weapon that offers very little warning before impact, and is often destructive and lethal.[12] MANPADS are cheap, and easily carried, handled, and concealed. It is claimed that there are at least 100,000 and possibly in excess of 500,000 systems in inventories around the world, and several thousands of these are vulnerable to theft from state authorities.[13] It is also claimed that there is a 70 percent chance that a civil aircraft will be destroyed if hit by a MANPAD.[14] A study conducted and published in early 2005 by

the Rand Corporation concludes that, based on the effects of the attacks of September 11, 2001, it is likely for air travel in the United States to fall by 15 to 20 percent after a successful MANPADS attack on a commercial airliner in the United States.[15] The international aviation community is aware that civil aircraft are particularly vulnerable to handheld ground-to-air missiles and that susceptibility avoidance techniques (calculated to avoid being hit) and vulnerability avoidance (survival after being hit) systems must be in place. This is particularly so since tracking the proliferation of MANPADS is difficult, as any intelligence gathered on this particular threat is usually ex post facto, through the recovery of launchers or fragments from expended missiles. Contrary to popular belief, the MANPAD is highly durable and can be used several years after inactivity, with recharged batteries.

The world's attention was further drawn to the deadly threat posed by MANPADS in November 2002, when there was an unsuccessful attempt to bring down a civilian aircraft leaving Mombasa, Kenya. Over the past 35 years, significant developments have taken place in dangerous weapons systems, creating more opportunities for terrorists. The ready acceptance of new technologies by the international community and our growing dependence on them have created many targets, such as nuclear and civil aircraft in flight. Similarly, developments in electronics and microelectronics, and the trend toward miniaturization and simplification have resulted in a greater availability of tactical weapons with longer ranges and more accuracy that are also simpler to operate. One of the most effective developments in individual weaponry is portable, precision-guided munitions (PGMs), which are lightweight and easy to operate. They can usually be carried and operated by a single person. The U.S.-made Stinger, the British-made Blowpipe, and the Russian-made SA-7 missiles are examples of these smaller weapons. These are shoulder-fired, antiaircraft missiles with infrared, heat-seeking sensors that guide the projectile to the heat emitted from an aircraft engine. It is known that more than 60 states possess SA-7 missiles and there is no doubt that most of them maintain strict security measures to prevent the outflow of the weapons. However, it has been alleged that some states, including Libya, have supplied PGMs to terrorist organizations. It is incontrovertible that in the hands of terrorists these missiles are not likely to be used against conventional targets such as tanks and military fighter aircraft. Of particular concern is the prospect of civilian airliners being shot at by surface-to-air missiles (SAMs) and antitank rockets as they land at or take off from airports.[16] Dr. Richard Clutterbuck summarizes the great threat of missile attacks:

> Recent years have seen increasing use of expensive and sophisticated surface-to-surface and surface-to-air missiles (SSM and SAM) by terrorists, generally of Russian or East European origin and redirected by Arab Governments, notably Colonel Gadafi's. Continuing development of these weapons for use by regular armies will ensure that new and more efficient versions will become available for terrorists.[17]

With increased airport security, placing explosive devices on civil aircraft is becoming more difficult, but now the same destructive result can be achieved far more easily by using modern missiles or rockets.

United Nations (UN) General Assembly Resolution 58/241, on the illicit trade in small arms and light weapons in all its aspects, started the process that led to the adoption, on December 8, 2005, of the International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons. For the purpose of this instrument, "small arms and light weapons" mean any man-portable lethal weapon that expels or launches, is designed to expel or launch, or may be readily converted to expel or launch a shot, bullet or projectile by the action of an explosive, excluding antique small arms and light weapons or other replicas.

The purpose of this instrument is to enable states to identify and trace, in a timely and reliable manner, illicit small arms and light weapons. The purpose is also to promote and facilitate international cooperation and assistance in marking and tracing the illicit trade in small arms and light weapons, and to enhance the effectiveness of, and complement, existing bilateral, regional, and international agreements to prevent, combat, and eradicate this trade in all its aspects.

For the purpose of identifying and tracing illicit small arms and light weapons, at the time of manufacture of each small arm or light weapon under their jurisdiction or control, states will be required to maintain a unique marking, in order to permit identification by all states of the country of manufacture. States will also ensure that accurate and comprehensive records are established for all marked small arms and light weapons within their territory. States should also maintain the manufacturing records for at least 30 years, and all other records, including records of import and export, for at least 20 years.

The instrument contains a number of provisions relating to cooperation in tracing, which is defined as "systematic tracking of illicit small arms and light weapons found or seized on the territory of a State from the point of manufacture or the point of importation through the lines of supply to the point at which they became illicit." The instrument calls upon contracting states to consider rendering technical, financial, and other assistance in building national capacity in the areas of marking, record keeping, and tracing in order to support the effective implementation of this instrument by states. It also encourages initiatives, within the framework of the United Nations Program of Action to Prevent and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, that mobilize the resources and expertise of, and where appropriate cooperation with, relevant regional and international organizations to promote the implementation of this instrument by states.

The United Nations General Assembly, on September 8, 2006, adopted a counterterrorism strategy that is , a unique global instrument to enhance national, regional, and international efforts to counter terrorism. The strategy emphasizes the need to combat the illicit arms trade, in particular the trade in small arms and light weapons, including MANPADS. Member states

have agreed to a common strategic approach to fighting terrorism, not only by sending a clear message that terrorism is unacceptable but also resolving to take practical steps individually and collectively to prevent and combat it. These steps include a wide range of measures ranging from strengthening state capacity to counter terrorist threats to better coordinating the UN system's counterterrorism activities.

In order to strengthen joint efforts to counter the threat to civil aviation operations posed by MANPADS, the Asia-Pacific Economic Cooperation (APEC) organization, the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), and individual states have taken a number of initiatives such as the holding of seminars, workshops, and special meetings, the development of guidelines on control and security of MANPADS, and the exchange of information.

## The Diverse Nature of Missile Attacks

The use of SAMs and antitank rockets by terrorists goes back to 1973. On September 5, 1973 Italian police arrested five Middle Eastern terrorists armed with SA-7s. The terrorists had rented an apartment under the flight path leading to Rome's Fiumicino Airport and were planning to shoot down an El Al airliner coming in to land at the airport.[18] These arrests proved a considerable embarrassment to Egypt, because the SA-7s were later traced back to a batch supplied to that country by the USSR. It was alleged that the Egyptian government was supplying some missiles to the Libyan army but inexplicably, the SA-7s had been directly rerouted to the terrorists. This incident also placed the USSR in an awkward position because its new missile and its proxy use of surrogate warfare against democratic states were revealed to the West.[19]

The plot of the missile attack on El Al derived from an appalling incident on February 21, 1973, when a Libyan B-727 was shot down over the Sinai Desert by an Israeli fighter, killing the 108 innocent people on board.[20] The Libyan people called for vengeance against Israel. Libya urged the other Arab states to send their warplanes against Israel's major cities and to destroy Israeli airliners wherever they could be found.[21]

On January 5, 1974, 220 soldiers and 200 police officers sealed off five square miles around Heathrow International airport in London after receiving reports that terrorists had smuggled SA-7s into Britain in the diplomatic pouches of Middle Eastern embassies and were planning to shoot down an El Al airliner.[22]

Another significant incident occurred on January 13, 1975, when an attempt by terrorists to shoot down an El Al plane with a missile was believed to have brought civil aviation to the brink of disaster. Two terrorists drove their car onto the apron at Orly Airport, where they set up a rocket launcher and fired at an El Al airliner that was about to take off for New York with 136 passengers. The first round missed the target, thanks to the pilot's evasive action,

and hit the fuselage of a Yugoslav DC-9 airplane waiting nearby to embark passengers for Zagreb. The rocket failed to explode and no serious casualties were reported. After firing again and hitting an administration building, which caused some damage, the terrorists escaped by car. A phone call from an individual claiming responsibility for the attack was received by Reuters. The caller clearly implied that there would be another such operation, saying, "Next time we will hit the target."

In fact, six days later another dramatic though unsuccessful attempt did occur at Orly airport. The French authorities traced the attack to Carlos, the Venezuelan PFLP terrorist and leader of the PFLP group in Europe.[23] It is also known that once again an El Al airliner had been deliberately chosen as a target by Gadafi in an attempt to avenge the loss of the Libyan airliner shot down by Israel over the Sinai Desert.[24]

Despite there failures, on January 25, 1976 another abortive attempt made by three PFLP terrorists, who were arrested by Kenyan police at Nairobi Airport—following a tip-off by Israeli intelligence to the Kenyan General Service Unit—before they had time to fire SA-7 missiles at an El Al aircraft carrying 100 passengers. In connection with this operation, two members of the German Baader-Meinhoff Faction, Thomas Reuter and Brigitte Schultz, were also arrested. After 10 days of interrogation, the terrorists were handed over to Israel by the Kenyan government. However, it was not until March 1977, 14 months after the arrests in Kenya, that the Israelis officially announced that they were holding the three Palestinian and two German terrorists. During this period, an unsuccessful attempt to gain their release was undertaken by the PFLP in June 1976, when Palestinian terrorists hijacked an Air France aircraft to Entebbe. The names of the five being held in Israel were included on the list of prisoners whose release was demanded in exchange for the hostages. The three Palestinians were released by the Israeli government in 1985.[25]

There has been a marked increase in missile attacks since 1984. On September 21, 1984, Afghan counterrevolutionaries fired a surface-to-air missile and hit a DC-10 Ariana Airliner carrying 308 passengers. The explosion tore through the aircraft's left engine, damaging its hydraulic system and a wing containing a fuel tank. The captain of the aircraft, however, managed to land the aircraft safely at Kabul International Airport.[26] Another significant incident took place on April 4, 1985, when a member of the Abu Nidal group fired an RPG rocket at an Alia airliner as it took off from Athens Airport. Although the rocket did not explode, it left a hole in the fuselage.[27]

Advanced missiles and rockets can be found in many terrorist and insurgent armories. It is suspected that some terrorist organizations, including Iranian militia in Lebanon, the Provisional Irish Republican Army, and various African and Latin American insurgents, possess the sophisticated Russian-made RPG-7 portable rocket launcher, but it is disturbing to note that some terrorist organizations, most notably Palestinian groups, have their own RPG-7-manufacturing facilities. In addition, more than a dozen

other terrorist and insurgent groups are known to possess portable surface-to-air missiles, These groups include various Cuban surrogates, Colombian drug dealers, and a number of African, European, and Palestinian terrorist organizations.[28]

The possibility of the undeterred use of missiles may be encouraged by the rapid proliferation of such weapons and the publicity to be gained by using them. The enhanced effectiveness of missiles against aircraft makes the threat of such attacks real.

### Installation of an Antimissile System

The installation of a sophisticated antimissile system similar to that employed on military aircraft to divert surface-to-air missiles is an effective deterrent. One good example is the measure taken by the British government, which, immediately after the discovery of 20 SA-7s in the coaster *Eksund*, which was intercepted by French authorities off the coast of Brittany in November 1987 when bound for a rendezvous with the IRA, fitted all British Army helicopters flying in Northern Ireland with electronic and other decoy systems to confuse the missile's heat-seeking guidance system. These systems included the U.S.-made Saunders, AN/ALG 144. This system, when linked to the Tracor AN/ALE 40 chaff dispenser, works by jamming the missile's homing radar and sending infrared flares and chaff to act as a decoy for the heat-seeking device.[29] The system is used by both the U.S. and the Israeli armies, which have been well pleased with its performance. Until the British realized that the IRA might be in possession of SAMs, the Ministry of Defence hesitated to install such a system because of the high cost involved, and its decision to do so shows the seriousness of the threat. Another example of a good countermeasure is the response of El Al to the threat of such an attack, which included the installation of electronic countermeasure equipment similar to that employed on military aircraft to divert surface-to-air missiles.[30] However, the problem is that these countermeasures are not yet fully effective, although they could minimize the threat. Hence there is a need to proceed diligently with the development of systems that are guaranteed to prevent this type of attack against civil aviation.

### The Perimeter Guard

For a successful missile attack against aircraft, the firing position has to be located within range of the flight path. A missile's guidance system is such that the weapon has to be fired within a few degrees of the flight path if the infrared sensor is to locate the target. Accordingly, a possible preventive measure would be to prevent terrorists from getting into a firing position with their missiles. However, it would be very difficult to cut off areas of up to 6 km wide that lie in the paths of aircraft as they land and take off. This measure is therefore impracticable if not impossible.[31] This difficulty can be overcome to an extent by patrolling the outer areas of airports in times of stringent

security conditions. Even in times when no specific threat has been received, it is within the capacity of most states to monitor those strips of land from which a SAM could be launched and thus minimize the risk. At the same time, these security operations would deter terrorists from spending vital resources on buying SAMs given the limited possibilities for their use.

Although the success rate so far of Western states in preventing terrorist missile attacks against civil aviation is satisfactory, and security forces, with the help of good intelligence, have been successful in tracking down and capturing missiles before they could be used, it is not unlikely that there will be attempts to use surface-to-air missiles to attack civil aviation in the near future. As some targets are becoming more difficult for terrorists to attack, it can be anticipated that they will make efforts to overcome the enhanced security systems as well as redirecting their efforts toward less secure targets. The displacement of the increasingly ineffective system of hijacking by missile attacks against civil aviation is a real threat.

## INTERNATIONAL ACCORD

In April 1996 in Vienna, state representatives of the "New Forum" held a plenary meetingto confirm the Wassenaar Arrangement,[32] earlier agreed upon in the city of Wassenaar, the Netherlands, which addresses the risks to regional and international security related to the spread of conventional weapons and dual-use goods and technologies while preventing destabilizing accumulations of weapons such as MANPADS. The Wassenaar Arrangement complements and reinforces, without duplicating, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognized measures designed to promote transparency and greater responsibility, by focusing on the threats to international and regional peace and security that may arise from transfers of armaments and sensitive dual-use goods and technologies where the risks are judged greatest. It is also calculated to enhance cooperation in order to prevent the acquisition of armaments and sensitive dual-use items for military end uses, if the situation in a region or the conduct of a state is or becomes a cause for serious concern to the participating states. It is not the intent and purpose of the arrangement to be directed against any state or group of states, nor will it impede bona fide civil transactions. Furthermore, it will not interfere with the rights of states to acquire legitimate means with which to defend themselves pursuant to Article 51 of the Charter of the United Nations.[33] The arrangement allows for participating states to control all the items set forth in a list of dual-use goods and technologies with the objective of preventing unauthorized transfers or retransfers of those items. Participating states also agree to exchange general information on the risks associated with transfers of conventional arms and dual-use goods and technologies in order to consider, where necessary, the scope for coordinating national control policies to combat the risks involved. At the tenth plenary meeting of the Wassenaar Arrangement, held in Vienna

on December 8–9, 2004, participating states reaffirmed their intent and resolve to prevent the acquisition by unauthorized persons of conventional arms and dual-use goods and technologies, in particular by terrorist groups and organizations. States also exchanged information on various national measures adopted to implement the provisions of the arrangement.

The Wassenaar Arrangement is the first global multilateral arrangement on export controls concerning conventional weapons and sensitive dual-use goods and technologies. It has not been given the conventional term, "convention" or "agreement," but nonetheless carries the agreement of participating states to collaborate in complementing, without duplicating, existing regimes on the nonproliferation of weapons of mass destruction and their delivery systems. The Wassenaar Arrangement is not a treaty in the sense of Article 102 of the United Nations Charter,[34] nor is it a treaty as defined by the Vienna Convention on the Law of Treaties of 1969, Article 2 of which defines a treaty inter alia as an international agreement concluded between states in written form and governed by international law. However, it remains an agreement between sovereign states concerning the implementation of the internal law of each participating state. This does not, however, mean that the Wassenaar Arrangement cannot be considered an international agreement or that it is invalid. It merely means that the arrangement does not come within the purview of the Vienna Convention. It is worthy of note that Article 3 of that convention explicitly recognizes that international agreements between states do not lose their validity merely because they do not come within the ambit of the convention.[35]

As mentioned earlier, the ICAO Assembly,[36] at its 36th Session (Montreal, September 18–28, 2007), adopted Resolution A36, in which the assembly expressed its deep concern regarding the global threat posed to civil aviation by terrorist acts, in particular the threat posed by MANPADS, other surface-to-air missiles systems, light weapons, and rocket propelled grenades.

The assembly noted that the United Nations General Assembly, on September 8, 2006, adopted a counterterrorism strategy.The Assembly recalled United Nations General Assembly resolutions 61/66 on the illicit trade in small arms and light weapons in all its aspects, 60/77 on the prevention of the illicit transfer and unauthorized access to and use of man-portable air defense systems, 61/71 on assistance to states for curbing the illicit traffic in small arms and light weapons and collecting them and 60/288 on the UN's global counterterrorism strategy. It also noted the International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons (A/60/88) and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Elements for Export Controls of MANPADS, and the Inter-American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and other Related Material:

*Noting* with satisfaction the ongoing efforts of other international and regional organizations aimed at developing a more comprehensive and coherent response to the

threat to civil aviation posed by MANPADS; and [recognizing] that the specific threat posed by MANPADS requires a comprehensive approach and responsible policies on the part of States.

The assembly urged all contracting states to take the necessary measures to exercise strict and effective controls on the import, export, transfer or retransfer, and stockpile management of MANPADS and associated training and technologies, as well as limiting the transfer of MANPADS production capabilities. It called upon all contracting states to cooperate at the international, regional, and subregional levels with a view to enhancing and coordinating international efforts aimed at implementing countermeasures carefully chosen with regard to their effectiveness and cost, and combating the threat posed by MANPADS. Furthermore, the assembly called upon all contracting states to take the necessary measures to ensure the destruction of nonauthorized MANPADS in their territory as soon as possible, while urging all contracting states to implement the international instruments to enable states to identify and trace, in a timely and reliable manner, illicit small arms and light weapons as referred to in United Nations General Assembly Resolution 61/66. All contracting states were urged to apply the principles defined in the Elements for Export Controls of MANPADS of the Wassenaar Arrangement. Finally, the assembly directed the ICAO Council to request the secretary general to monitor on an ongoing basis the threat to civil aviation posed by MANPADS and to continuously develop appropriate countermeasures to this threat and periodically request contracting states to inform the organization regarding the status of implementation of the resolution and the measures taken to meet its requirements.

### Other Current Threats

Security restrictions on the carriage of liquids, aerosols, and gels (LAGs) in hand baggage were introduced on August 10, 2006, in response to the foiling of an alleged terrorist plot in the United Kingdom against aviation using improvised explosive devices containing homemade liquid explosives. An initial ban on the carriage of all hand baggage on flights leaving the United Kingdom was subsequently modified to a restriction on the amounts of LAGs that were permitted to be carried by passengers through screening points. These restrictions were adopted elsewhere in Europe and in North America. They were subsequently harmonized within the European Union by an amendment to the European Commission regulations, which came into effect on November 6, 2006.

As a global follow-up to these measures, ICAO recommended their universal adoption (no later than March 1, 2007) in a state letter. ICAO also reacted to the new threat with urgency and efficiency, calling a special meeting of the council on August 17, 2006 to explore ways of countering the new threat. As the international civil aviation industry attaches great importance to the

security screening of liquids, many countries have made great efforts to study methods to detect liquids. At present and for the near future, the most effective and the safest method is a combination of regular measures, such as X-ray screening, visual examination, inspection by removing bottle lids, restrictions on carrying liquids, and so forth. ICAO temporary security control guidelines provide a uniform operation mode for liquids screening, which is helpful to the unification of international civil aviation security standards.

### Bioterrorism

A bioterrorism attack is the deliberate release of viruses, bacteria, or other agents used to cause illness or death in people, animals, or plants. These agents are typically found in nature, but it is possible that they could be changed to increase their ability to cause disease, make them resistant to current medicines, or increase their ability to be spread into the environment. Biological agents can be spread through the air, through water, or in food. Terrorists may use biological agents because they can be extremely difficult to detect and do not cause illness for several hours to several days. While some bioterrorism agents, such as the smallpox virus, can be spread from person to person, some agents such as anthrax are incapable of being so spread.

There have been several noteworthy instances of bioterrorism in the past,[37] even as early as 1915,[38] which send an ominous message that it is a distinct possibility in the aviation context. Until recently in the United States, most biological defense strategies have been geared to protecting soldiers on the battlefield rather than looking after ordinary people in cities. In 1999, the University of Pittsburgh's Center for Biomedical Informatics deployed the first automated bioterrorism detection system, called RODS (Real-Time Outbreak Disease Surveillance). RODS is designed to draw collect data from many data sources and use them to perform signal detection, that is, to detect a possible bioterrorism event at the earliest possible moment. RODS, and other similar systems, collect data from various sources including clinical data, laboratory data, and data from over-the-counter drug sales. In 2000, Michael Wagner, the codirector of the RODS laboratory, and Ron Aryel, a subcontractor, conceived of the idea of obtaining live data feeds from "nontraditional" (non–health care) data sources. The RODS laboratory's efforts eventually led to the establishment of the National Retail Data Monitor, a system that collects data from 20,000 retail locations nationwide.

On February 5, 2002, President Bush visited the RODS laboratory and used it as a model for a $300 million spending proposal to equip all 50 states with biosurveillance systems. In a speech, Bush compared the RODS system to a modern "DEW" line (referring to the Cold War ballistic missile early warning system).

The principles and practices of biosurveillance, a new interdisciplinary science, were defined and described in a handbook published in 2006.[39] Data that

could potentially assist in the early detection of a bioterrorism event include many categories of information. Health-related data such as those collected from hospital computer systems, clinical laboratories, electronic health record systems, medical examiner record-keeping systems, 911 call center computers, and veterinary medical record systems could be of help in the fight against bioterrorism. Researchers are also considering the utility of data generated by ranching and feedlot operations, food processors, drinking water systems, school attendance recording, and physiological monitors, among others. Intuitively, one would expect systems that collect more than one type of data to be more useful than systems that collect only one type of information (such as single-purpose laboratory or 911 call-center based systems) and be less prone to false alarms. This indeed appears to be the case.

The inherently uncontrollable nature of dangerous pathogens makes bioterrorism unattractive as a warfare strategy. However, the potential power of genetic engineering cannot be marginalized or underestimated, and the compelling need for continuing vigilance cannot be ignored.

### Intelligence Gathering

The gathering of reliable intelligence remains the first line of defense. Although modern technologies clearly aid terrorists in terms of weapons and targets, technology can also be used against terrorists. Governments that are endowed with the necessary technology can keep track of terrorist organizations and their movements with the aid of computers. At the same time, electronic collection methods and signals intelligence afford the possibility of eavesdropping on and intercepting terrorist communications, leading to better predictions of their operations. One of the instances in which intelligence gathering has worked well to prevent terrorism occurred in September 1984, when the Provisional IRA spent an estimated £1.5 million in the United States on a massive shipment of seven tons of arms. With the help of an informer who warned about a forthcoming shipment of weapons, including rockets, to the Provisional IRA from the United States, the FBI informed British intelligence, which in turn contacted the Irish, and the ship carrying the arms was tracked by a U.S. satellite orbiting 300 km above the earth. The satellite photographed the transfer of the arms to a trawler. Finally, two Irish naval vessels intercepted the trawler, and British security forces arrested the crew.[40] This incident shows that intelligence gathering with the help of high technology can cut off the transfer of missiles and other weapons to terrorists.

### A Risk-Based Approach?

Intelligence and the likelihood of an attack are central elements of risk management. However, the need to introduce more risk assessment is driven in part by the passenger hassle factor. The hassle factor is making air travel increasingly unpopular and contradicting the very aim of Article 22 of the

Chicago Convention, which aims to preserve the speed and convenience of air travel ("to prevent unnecessary delays to aircraft, crews, passengers, and cargo"). The need to introduce more risk assessment is also driven by increased costs for security measures and for related equipment and technology. In this context, all stakeholders in the system, that is, governments, airlines, airports, and passengers, have an interest in reflecting on how best to decide which possible measures can be introduced, and what their respective impacts, both positive and negative, are likely to be across the board.

A key principle leading toward more risk-based security is the idea that addressing all risks at the same level, regardless of their severity, is actually less efficient than concentrating the bigger part of one's resources on the most severe risks. Like everything, air transport operates in a context of limited resources, be they financial, infrastructural, or other (availability of trained staff, and so forth). In this context, and in the interest of better security, governments must carefully weigh the options that present themselves to them, and make the right decisions. The primary role of the authorities must be to centralize intelligence and threat information. Airlines are major interested parties and need to be informed in good time. Assessing and prioritizing the different risks is a typical government duty. A certain risk can be addressed or mitigated by a number of possible measures. Here the role of governments should be to assess which of these options will have the least impact on industry and passengers. This impact can be operational as well as financial.

Security management systems, particularly when applied to air carriers, provide an effective tool that would ensure a risk-based approach to aviation security. Within a security risk management environment, consideration is given to threats that are often ill defined, constantly evolving, and the result of deliberate and intentional actions. In addition, specific security threats must be considered unpredictable and likely to be indiscriminate in nature. For example, while the intelligence and law enforcement agencies involved in preventing terrorist activity may uncover information suggesting pending attacks, it is necessary and prudent to assume that they may not be able to identify and stop all possible threats all of the time.

Security measures must also be capable of being strengthened quickly at any time as a result of increased levels of security risk. In addition, by virtue of their nature, they are usually highly visible and intrusive and often conflict with passenger and air cargo facilitation needs that require ready access to facilities and services to expedite the process of air transportation. This is not the case with the vast majority of controls in a safety environment. These factors require recognition and assessment when specific preventative security controls and associated regulatory standards are considered and developed. Recognizing these factors, the need exists for an integrated systems managed approach within various organizations, at both regulatory and industry levels, that have responsibilities relating to the delivery of safety and security outcomes. Such an approach has the ability to offer a range of benefits, including the integration of existing organizational quality management systems into a

comprehensive and aligned organizational structure and culture that ensures a more cohesive and standardized approach to how security processes should be implemented with overall better and more uniform standards of service delivery.

The introduction into existing processes, at both regulatory and industry levels, of effective risk assessment activity that can contribute to making security processes proactive and targeted, and therefore potentially more efficient and effective without unduly impacting on export trade and passenger movements, is certainly a proactive measure in a risk-based approach. Additionally, in order for air carriers to successfully implement security event management systems (SEMS) within their operations, it is paramount that states endorse this approach as being in compliance with the security requirements of ICAO Annex 17—"Security" as well as with individual regulators. States are also encouraged to draft regulations based on the desired outcome or standard rather than prescribe actual procedures that are necessary to be in compliance. Allowing flexibility to those entities responsible for the implementation of security measures to meet the stated standards in the best possible way will lead to a more effective and efficient use of resources.

Outcome- or performance-based regulations also facilitate the quality control oversight that a state needs to exercise on various stakeholders by limiting the oversight responsibility to ensuring that the security standards are met, without focusing on the particulars of the procedures. Finally, in order to ensure better co-operation, it is paramount that contracting states recognize various methods by which to meet security standards if an overall improved security environment is to be achieved. Mutual acceptability of security procedures prevents the mandating of security procedures extraterritorially, all the while ensuring that the same level of security is achieved globally.

## The ICAO Security Audits

On the basis of Assembly Resolution A33–1 adopted in 2001 and the recommendations of the high-level ministerial conference on aviation security (Montreal, February 2002), the council adopted in June 2002 its Aviation Security Plan of Action, which included the establishment of a comprehensive program of regular, mandatory, systematic, and harmonized audits to be carried out by ICAO in all contracting states. The ICAO Universal Security Audit Program (USAP) was subsequently launched, with the objective that all contracting states should have benefited from an initial audit by the end of 2007.

Since the launch of the USAP in 2002, 169 aviation security audits and 77 follow-up missions have been conducted.[41] The audits have proven to be instrumental in the ongoing identification and resolution of aviation security concerns, and analysis reveals that the average implementation rate of Annex 17 standards in most states has increased markedly between the period of the initial audit and the follow-up mission.

A critical part of the audit process is the requirement that all audited states submit a corrective action plan to address deficiencies identified during an audit. As directed by the council, all states are notified (by state letter and on the USAP secure Web site) of those states that are more than 60 days late in submitting a corrective action plan. As of July 31, 2007, there were seven states that were more than 60 days late. In the case of late corrective action plans, repeated reminders are sent to states, including reminders at the level of the secretary general and with the involvement of the applicable regional office, and ICAO assistance is offered should the state require advice or support in the preparation of its action plan. Extensive feedback is provided to each audited state on the adequacy of its corrective action plan, and an ongoing dialogue is maintained where necessary to provide support in the implementation of proposed actions.

ICAO performs comprehensive analysis of audit results on levels of compliance with Annex 17—"Security" standards on an ongoing basis (globally, by region, and by subject matter). This statistical data is made available to authorized users on the USAP secure Web site and is shared with other relevant ICAO offices as a basis for prioritizing training and remedial assistance projects. As of July 31, 2007, 77 follow-up missions had been conducted. These missions take place two years after the initial audit with the purpose of validating the implementation of state corrective action plans and providing support to states in remedying deficiencies. These missions are normally conducted by the applicable regional office, with close coordination through headquarters. The results of the follow-up visits indicate that the majority of states have made significant progress in the implementation of their corrective action plans.

A high-level ICAO Secretariat Audit Results Review Board (ARRB) has been established as part of a coordinated strategy for working with states that are found to have significant compliance shortcomings with respect to ICAO standards and recommended practices (SARPs). The ARRB both examines the safety and security histories of specific states and also provides an internal advisory forum for coordination among ICAO's safety, security, and assistance programs.

As future measures in the audit program of ICAO, the ICAO Council in 2007 approved the practice that not all states need to be audited at the same frequency, although the USAP should always preserve the principle of universality. The council was of the view that, with a solid baseline of audit results established for all states by the end of 2007, a more effective use of resources could be achieved by developing an appropriate scheduling/frequency model to determine the priority of future audits and frequency of visits to states. It remains a requirement, however, that the principle of universality will be maintained, with all states audited at least once within a six-year period.

Another decision of the council was that future audits under the USAP should be expanded to include relevant security-related provisions of Annex 9–"Facilitation." With the recent expansion of the universal audit program to

a comprehensive systems approach covering all safety-related annexes, Annex 9 is currently the only annex not included in either of ICAO's two audit programs. There are a number of security-related provisions contained in Annex 9, particularly as related to the security and integrity of travel documentation, which can be audited under the USAP along with the related standards of Annex 17.

The council also decided that wherever possible, ICAO aviation security audits should be focused on a state's capability to provide appropriate national oversight of its aviation security activities. Using the results of the initial audits and follow-up visits, the scope of future ICAO audits should be adjusted to the prevailing situation in each audited state. Those states that have demonstrated the national infrastructure necessary to oversee security activities at their airports may undergo a targeted oversight audit to verify adequate implementation of the state's national quality control program. Such oversight audits would continue to include a verification of the implementation of ICAO provisions through spot checks at the airport level.

The ICAO USAP has been implemented on schedule and within its budget allocation. The audits have proven to be instrumental in the identification of aviation security concerns and in providing recommendations for their resolution. From its inception, the USAP has enjoyed the support of contracting states and is promoting positive change as states become increasingly sensitized to the international requirements. The USAP follow-up missions have shown a markedly increased level of implementation of ICAO security standards, attesting to states' commitment to achieving the objective of the USAP, to strengthen aviation security worldwide.

## CONCLUSION

A security culture, if such were to exist among ICAO's member states, would mean that the states would be aware of their rights and duties and, more importantly, assert them. Those who belong to a security culture know which conduct would compromise security and they are quick to educate and caution those who, out of ignorance, forgetfulness, or personal weakness, partake in insecure conduct. Security consciousness becomes a "culture" when all the 190 member states working together make security violations socially and morally unacceptable within the group.

All ICAO member states were to have been successfully audited by the end of 2007, with strengths and weaknesses identified, regional and global trends tracked, and recommendations made to states for improving their security regimes. However, there remains a small number of states that have made little or no progress in implementing the ICAO recommendations to correct the deficiencies identified through the audits. Although security audit information has been restricted in the past, steps should be taken to increase the transparency of the audit program and ensure that the global aviation network remain protected. It is therefore proposed that, in addition to a review

of deficiencies by the Audit Results Review Board, consideration be given to the development of a process that will notify all member states when deficiencies identified during the course of a USAP audit remain unaddressed for a sustained period. A notification process could involve the use of information that does not divulge specific vulnerabilities but enables states to initiate consultations with the state of interest to ensure the continued protection of aviation assets on a bilateral basis.

Upon completion of a USAP audit, states are required to submit a corrective action plan addressing deficiencies and schedule a follow-up visit. Audit follow-up visits were initiated in mid-2005 in order to check the implementation of states' corrective action plans and to provide support in remedying identified deficiencies. These visits are normally conducted in the second year following a state's audit. According to USAP reports, follow-up visits have shown that the majority of states have made progress in the implementation of their corrective action plans. At the same time, however, follow-up visits have also revealed that a small number of states that have made little or no progress in correcting their deficiencies.

According to a progress report submitted to the ICAO Council in 2006, the ICAO Secretariat advised that in the case of states that are demonstrating little or no progress by the time of the follow-up visit, a cross analysis of the USAP audit results with those of the USOAP reveals that generally, states that have difficulty in implementing the safety-related SARPs are also experiencing difficulties with the implementation of the Annex provisions on the security side. Certain contributing factors have been identified. These often include a lack of financial and/or suitably qualified human resources, as well as frequent changes in key personnel within a state's appropriate authority. In some cases, there also appears to be a certain complacency and general lack of interest in implementing the ICAO recommendations."

In order to address the issue of states that are not responding effectively to the ICAO audit process, a high-level Secretariat Audit Results Review Board has recently been established for the purpose of examining both the safety and security histories of specific states brought to its attention by either USOAP or USAP. The objective is to highlight or raise the profile of these states within the system, in order to encourage them to take responsible actions in a measured and timely manner.

The Committee on Unlawful Interference of the ICAO Council has recommended to the council that these data and trends be made public at the assembly. Although such information has been restricted in the past, the committee believes all states and the public should be aware of the areas needing improvement without identifying specific states or vulnerabilities. Further, the council has been discussing with the Secretariat ways in which it can most effectively exercise its oversight responsibilities with respect to states that do not comply with their responsibilities under the convention and its annexes.

For those states that lack the resources to improve their security systems, new mechanisms such as ICAO's Coordinated Assistance and Development

(CAD) Program are in place to assist in directing longer-term attention to problems. For those states that remain unable to improve their security systems, bringing such problems before the Audit Results Review Board, and possibly the council, for consideration are valuable steps toward addressing the deficiencies in the longer term. However, the vulnerabilities presented by unresolved and sustained issues represent a significant weakness in the global protective network and a possible critical or urgent area of vulnerability for other member states with air carrier service at the airport of interest, particularly when combined with indications of a heightened threat.

In building a security culture within ICAO member states, it is imperative that consideration should also be given to the development of a process for ensuring that all member states are notified when deficiencies identified during the course of a USAP audit remain unaddressed for a sustained period of time. A notification process could involve the use of information that does not divulge specific vulnerabilities but enables states to initiate consultations with the state of interest. Such a notification process may result in a strengthened ability on the part of ICAO to ensure that states unwilling to meet basic security standards will be held accountable and allow for a limited amount of transparency in the security audit program without divulging specific potential security vulnerabilities.

## NOTES

1. Carol B. Hallett, President and CEO, Air Transport Association, *State of the United States Airline Industry, A Report on Recent Trends for United States Carriers*, statement, 2002, www.airlines.org/news/speeches.

2. *Assembly Resolutions in Force* (as of October 5, 2001), ICAO Doc. 9790, VII-1. Also of general interest is UN General Assembly Resolution 56/88, *Measures to Eliminate International Terrorism*, adopted at the Fifty-Sixth Session of the United Nations, which calls upon states to take every possible measure in eliminating international terrorism.

3. ICAO News Release, "High-Level Ministerial Conference Approves Worldwide Manditory Aviation Security Audit Programme," February 21, 2002, PIO 02/2002.

4. For detailed information on the proposed international facility for aviation safety, see Ruwantissa I. R. Abeyratne, "Funding an International Financial Facility for Aviation Safety," *Journal of World Investment* 1, no. 2 (December 2000): 383–407.

5. Convention on International Civil Aviation (also called the Chicago Convention), signed at Chicago on December 7, 1944. See ICAO Doc. 7300/9, 9th ed., 2006.

6. Article 1 of the Chicago Convention provides that the contracting states recognize that every state has complete and exclusive sovereignty over the airspace above its territory.

7. Preamble to the Chicago Convention.

8. At the 35th Session of the ICAO Assembly (Montreal, September 28–October 8, 2004), the International Air Transport Association (IATA) brought to the attention of the assembly the fact that the aviation underwriting community had formally announced its intention to exclude all hull, spares, passenger, and third party liability claims resulting from damage caused by the hostile use of dirty bombs, electromagnetic pulse devices, or biochemical materials. For a discussion of this subject, see Ruwantissa

I. R. Abeyratne, "Emergent Trends in Aviation War Risk Insurance," *Air and Space Law* 30, no. 2 (April 2005): 117–29.

9. As has already been discussed in the first part of this chapter, at the 33rd Session of the Assembly, ICAO adopted Resolution 13/1, entitled *Declaration on Misuse of Civil Aircraft as Weapons of Destruction and Other Terrorist Acts Involving Civil Aviation*. This resolution, while singling out for consideration the terrorist acts that occurred in the United States on September 11, 2001, and, inter alia, recognizing that the new types of threat posed by terrorist organizations require new concerted efforts and policies of cooperation on the part of states, urges all contracting states to intensify their efforts in order to achieve the full implementation and enforcement of the multilateral conventions on aviation security, as well as of the ICAO standards and recommended practices and procedures (SARPs) relating to aviation security. The resolution also calls upon states to monitor such implementation, and to take within their territories appropriate additional security measures commensurate to the level of threat, in order to prevent and eradicate terrorist acts involving civil aviation. Stemming from this resolution, and subsequent ICAO action such as was contained in Resolution A35–1 (on the destruction of Russian civil aircraft on August 24, 2004), various security and facilitation measures such as biometric identification, strengthening of cockpit doors, and issuance of passenger name records have succeeded in reducing the incidents of physical human action on board, such as hijacking, over the past few years.

10. In the period from 1947 to 1996, hijacking was the most common offense against civil aviation, recording 959 incidents. During this period, hijacking constituted 87 percent of all attacks on aircraft. see Paul Wilkinson and Brian M. Jenkins, eds., *Aviation Terrorism and Security* (Frank Cass: London, 1999), 12.

11. Hijacking in the late 1960s started an irreversible trend, which was later dramatized by such incidents as the skyjacking by Shia terrorists of TWA Flight 847 in June 1985. The skyjacking of Egypt Air Flight 648 in November of the same year and the skyjacking of a Kuwait Airways Airbus in 1984 are other early examples of skyjacking. Aviation sabotage, in which explosions on the ground or in midair destroy whole aircraft, their passengers, and their crew, has also been a continuing threat in past decades. The explosion of Air India Flight 182 over the Irish Sea in June 1985 and Pan Am Flight 103 over Lockerbie, Scotland, in 1988, and the UTA explosion over Niger in 1989 are examples. Missile attacks, in which aircraft are destroyed by surface-to-air missiles (SAMs) also occurred as early as the 1970s. The destruction of the two Viscount aircraft of Air Rhodesia in late 1978/early 1979 provides two examples. Armed attacks at airports, now a reemerging threat, occurred early on in instances where terrorists opened fire in congested areas of airport terminals. Examples of this type of terrorism include the June 1972 attack by the Seikigunha (Japanese Red Army) at Ben Gurion Airport, Tel Aviv; the August 1973 attack by Arab gunmen on Athens Airport; and the 1985 attacks on the Rome and Vienna airports; Finally, the illegal carriage by air of narcotics and other psychotropic substances and crimes related to this, such as the seizure of or damage to aircraft, persons, and property, also constitute a threat that cannot be ignored in the present context. For an extensive study of the carriage of narcotics by air, see Ruwantissa I. R. Abeyratne, *Aviation Security* (London: Ashgate, 1998), 197–296.

12. The lethality of the weapon can be illustrated by the 340 MANPADS used by Afghan Mujahedeen rebels to successfully hit 269 Soviet aircraft. See http://www.janes.com/security/international_security/news/.

13. "MANPADS," *Ploughshares Monitor*, Autumn 2004, 83.

14. Ibid. The deadly accuracy and ease of handling of MANPADS were demonstrated when Somali gunmen shot down two U.S. MH-60 Black Hawk helicopters in October 1993.

15. *Infrastructure Safety and the Environment*, *Protecting Commercial Aviation against the Shoulder-Fired Missile Threat* (Santa Monica, CA: Rand Corporation, 2005), 9.

16. Donald J. Hanle, *Terrorism: The Newest Face of Warfare* (New York: Pergamon-Brassey's, 1989), 185; Arie Ofri, "Intelligence and Counterterrorism," *ORBIS* 28 (Spring 1984): 49; Andrew J. Pierre, "The Politics of International Terrorism," *ORBIS* 19 (1975–76): 1256; Frederick C. Dorey, *Aviation Security* (London: Granada, 1983): 142.

17. Richard Clutterbuck, *Living with Terrorism* (London: Butterworths, 1991), 175.

18. Christopher Dobson and Ronald Payne, Appendix B, "The Chronology of Terror: 1968–1987," in *War without End: The Terrorists: An Intelligence Dossier* (London: Sphere Books, 1987), 366.

19. Christopher Dobson and Ronald Payne, *The Carlos Complex: A Pattern of Violence* (London: Hodder and Stoughton, 1977), 134.

20. *Keesing's Contemporary Archives*, March 5–11, 1973, 25757.

21. Ibid.

22. Edward F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1969–1979* (London: Aldwych Press, 1980), 428.

23. Dobson and Payne, *The Carlos Complex*, 53.

24. Ibid.

25. Mickolus, *Transnational Terrorism*, 581; *Al-Hadaf, Al-Hadaf mao Al-Babtal al-Muharrarin: Al-Muo taqilun hawwalu Dhallam al-Asr ila Nidhal Mushriq* (Al-Hadaf with the Liberated Heroes: The Detainees Transformed the Gloom of Imprisonment into a Shining Struggle), June 1985, 35–41.

26. U.S. Department of Transportation (FAA), *Worldwide Significant Acts Involving Civil Aviation* (Washington, DC: Federal Aviation Administration, 1984), 14.

27. U.S. Department of Defense, *Terrorist Group Profiles* (Washington, DC: U.S. GPO, 1989), 7.

28. James Adams, *Trading in Death: Weapons, Warfare and the Modern Arms Race* (London: Hutchinson, 1990), 60–61; Paul Wilkinson, "Terrorism: International Dimensions" in *The New Terrorism*, ed. William Gutteridge (London: Institute for the Study of Conflict and Terrorism, 1986), 39–40; Christopher Dobson and Ronald Payne, *The Terrorists: Their Weapons, Leaders and Tactics* (New York: Facts on File, 1982), 119.

29. *Daily Telegraph* (London), January 7, 1988.

30. Aryeh Lewis and Meir Kaplan, eds., *Terror in the Skies: Aviation Security* (Tel Aviv, Israel: ISAS, 1990), 226; William Alva Crenshaw, "Terrorism and the Threat to Civil Aviation" (PhD diss., University of Miami, 1987): 126.

31. Dorey, *Aviation Security*, 142.

32. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Elements for Export Controls of MANPADS and the Inter-American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Material, available at www.wassenaar.org.

The participating states were Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, the

Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States.

33. Article 51 of the United Nations Charter provides, inter alia, that nothing in the charter will impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.

34. Infrastructure Safety and the Environment, Article 102 of the UN Charter, stipulates that every treaty and every international agreement entered into by any member of the United Nations after the charter comes into force shall be registered with the UN Secretariat as soon as possible.

35. Malcolm N. Shaw, *International Law*, 5th ed. (Cambridge: Cambridge University Press, 2003), 812.

36. The ICAO's triennial assembly, at which its 190 member states gather to evaluate policy and make new policy as necessary through resolutions, is the supreme governing body of the organization.

37. In 1984, followers of the Bhagwan Shree Rajneesh attempted to control a local election by incapacitating the local population through infecting salad bars in restaurants, doorknobs, produce in grocery stores, and items in other public areas with salmonella typhimurium in the city of The Dalles, Oregon. The attack caused about 751 people to become sick (there were no fatalities). This incident was the first known bioterrorist attack in the United States in the twentieth century. In September and October of 2001, several cases of anthrax occurred in the United States; these were reportedly caused deliberately. This was a well-publicized act of bioterrorism. It motivated efforts to define biodefense and biosecurity.

38. In 1915 and 1916, Dr. Anton Dilger, a German-American physician, used cultures of anthrax and glanders with the intention of committing biological sabotage on behalf of the German government. Other German agents are known to have undertaken similar sabotage efforts during World War I in Norway, Spain, Romania, and Argentina.

39. Michael Wagner, Andrew Moore and Ron Aryel, eds., *Handbook of Bio Surveillance* (New York: Elsevier, 2006). Bio surveillance is the science of real-time disease outbreak detection. Its principles apply to both natural and man-made (bioterrorist) epidemics. In addition to activity in this field in the United States, work is also being done in Europe, where disease surveillance is beginning to be organized on a continent-wide scale, which is needed to track biological emergencies. The system not only monitors infected persons but also attempts to discern the origin of the outbreak.

40. *Daily Telegraph*, October 16, 1984; *Times* (London), December 12, 1984.

41. The 36th Session of the ICAO Assembly was informed that there are some 150 certified auditors on the Universal Security Audit Program (USAP) roster, from 59 states in all ICAO regions. The participation of certified national experts in the audits under the guidance of an ICAO team leader has permitted the program to be implemented in a cost-effective manner while allowing for a valuable interchange of expertise.

# CHAPTER 2

# The Case for an Aviation Security Crisis Management Team

*Charles M. Bumstead*

The new wave of political violence in the Middle East and South Asia, where religious sectarianism has added a dangerous and potent factor to the problem of international terrorism, has focused attention on the real danger this brand of terrorism could pose to Western civilization and international order.

Terrorism, political or religious, can be briefly defined as "A special form of clandestine, undeclared, and unconventional warfare waged without benefit of humanitarian restraints or rules."[1] Terrorist attacks on the Western international airline industry strike at the very heart of the global economy as well as affecting individual states. The major threat at this time is *organized international terrorism.*

There has been a remarkable increase in the number and intensity of incidents in the past few years. Since the attack on the World Trade Center in September of 2001, the growing threat of extremist violence involving civil aircraft in the air and the industry's infrastructure and buildings on the ground has been looming over the international civil aviation industry. No state, it seems, is safe from this type of threat, as it appears to be ideological rather than political in nature. There are still random, individual threats to international civil aviation that do not fall into the category of international terrorism. However, organized international terrorism is the major threat facing the industry today. There is not, currently, a way to prevent all such attacks.

During the past few years, the aviation community has attempted to address the complicated issues related to preventing unlawful interference with international civil aviation. Early on, incidents in which an aircraft was destroyed were relatively rare. Usually, it was a hostage situation and the

aircraft was on the ground. That scenario has changed, and the threat has grown to include devastating property damage, including the loss of aircraft and human lives, such as when an aircraft is used as a destructive missile. The other aspect of the current threat is risk of damage to the infrastructure: terminal buildings, rail transportation, and other structures. These types of attacks, even though some are directed toward the ground transportation industry, have a deleterious effect on all segments of transportation including that of the air domain.

States and international organizations have historically limited their responses and their actions to individual incidents. There was little or no recognition of the growing unrest in certain areas of the Middle East, where the roots of organized international terrorism were growing. Therefore, the actions taken by states and by international organizations tended to be reactive rather than proactive. Subsequently, actions treated only the issues specific to each individual incident. The term "incremental" can be applied to their processes. The international organizations did not recognize the growing threat posed by organized ideological entities. As a result, little or no effort was expended by the international organizations to organize a concerted effort to develop an aggressive program to forecast, prevent, or provide an emergency response during an incident or to seek measures to amend the aviation security system. That task has primarily been left to individual states. This failure to see into the future is fundamental to the problems connected with the prevention and treatment of incidents of terrorism.

Due to the increased number of incidents and the severity of the attacks, it is time to rethink the entire international aviation security management process; and that includes examining the role played by international organizations in the aviation security milieu.

## A FRESH PERSPECTIVE

The international aviation organizations must take a fresh look at the problems they are now facing. There are some problems that need to be addressed on a priority basis. First; there's the inability of international aviation organizations, specifically the International Civil Aviation Organization (ICAO), to effectively deal with incidents of unlawful interference. The role of the ICAO is limited by international law to rule making and assistance to the various contracting states. There is no apparent vehicle within the ICAO to deal with an ongoing incident or to play any role in the development of preventive measures to avoid or minimize the effects of such incidents. ICAO has provided documents that provide general guidelines to the contracting states concerning aviation security. Within the documents provided by ICAO there are regulations that place the responsibility on ICAO to develop standards and recommended practices (SARPs) to govern the establishment of aviation security regulations in each contracting state.[2] It is imperative that the ICAO documents be examined with an eye to providing

a more aggressive posture toward security, perhaps to include preventive measures and the ability to coordinate with the contracting states' intelligence agencies.

Second, existing regulations concerning aviation security are stated by ICAO in Annex 17, Standards and Recommended Practices, "Safeguarding International Civil Aviation against Acts of Unlawful Interference," and are expressed in very general terms.[3] The states have a great deal of leeway as to the type and kind of security regulations they promulgate. Some states have very stringent security requirements for their international and domestic air carriers. Other states do not have strict security procedures, because of the lack of a perceived threat.

There are occasions when the threat assessment organ of a contracting state may determine that a heightened security level is required, due to intelligence reports indicating a credible threat to the state or its aircraft. The security requirements may be perceived as serious enough to require the state to seek a higher level of security at an airport in another state's sovereign territory. It would be helpful to have a means provided in the ICAO documents through which such problems can be sorted out ahead of time, rather than during an incident. Such a vehicle could be made available to the international community.

In April 1996, the U.S. Congress passed the Hatch Act. This was antiterrorism legislation, requiring all airlines flying to the United States, no matter from which sovereign nation, to apply security measures similar to those imposed by the Federal Aviation Administration (FAA) on U.S. airlines. There was an adverse reaction on the part of many contracting states in ICAO over the proposed legislation. Several states alleged that the act attempted to apply U.S. law outside the territorial limits of the United States, and further, that the Hatch Act infringed upon the sovereignty of contracting states.[4] It was considered objectionable by almost the entire international aviation community. States said that the Hatch Act flew in the face of the "host state responsibility" set out in the Chicago Convention, to which the United States is a contracting party.

The Hatch Act created a firestorm of opinions from almost all of the contracting states in ICAO that operated civil aviation flights into or out of the United States. The conclusion drawn by several states was that the move was more of an economic strategy by the United States to force other states into investing large amounts of cash to help cover the cost of providing a specified level of safety. Additionally, the majority of states felt that the increased security measures required by the act would not enhance safety but, rather, would decrease the safety component by not allowing contracting states to utilize the precepts of the risk management concept.[5]

An example will illustrate the way in which the U.S. requirement for heightened security could affect the international aviation community and help to clarify the issues involved. The United States receivs information that a specific flight, departing from the United Kingdom with a destination in the

United States, has been threatened with a bomb; the United States requests that United Kingdom security should not allow curbside baggage checks but should match passengers with baggage prior to departure. The United Kingdom, not being able to comply with the request, reports this to the United States. The United States finds this position unacceptable because it considered the threat to be very credible. The United States informs the United Kingdom that the aircraft can not land in the United States. The United Kingdom is left with the option of canceling the flight or delaying it until the request from the United States could be met. Since there are no resources at the United Kingdom airport to perform the required functions, the flight is canceled by the United States. The United Kingdom objects because the United States, in effect, attempted to take U.S. security actions in the United Kingdom's sovereign airspace.

The position of the United Kingdom, as presented here, is supported in the ICAO SARPs, as the SARPs forbid a state from requiring a higher level of security than that provided for in the SARPs. It is evident that there is a major problem. No state, under threat of a potential bomb aboard an aircraft landing in its territory, is going to pay much attention to the Chicago Convention or to the ICAO SARPs. Nationalism and protection of citizens and property will be the primary motivation for the affected state. It is quite obvious that such a situation in the international arena cannot be allowed to exist. There must be provisions in current ICAO documents for states to require increased security standards, above those required by the SARPs, when a high-security situation arises.

After an initial flurry of activity, ICAO and other international organizations took action to criticize the United States for its precipitate action in passing the Hatch Act. The ensuing months led to strong comments from around the world. States were adamant in their criticism of the act, and ICAO published an official response to the United States—the "Notice of Proposed Rule Making" (NPRM)—in 1999, objecting to the stringent terms of the act, and adding a specific complaint concerning the requirement for contracting states to provide a level of security similar to that provided by the United States.[6]

All of the objections made by ICAO and the contracting states had a measure of validity, as the required standards would, in fact, cause many problems for other states. For instance, the problems of baggage handling outside of the terminal area and of matching passengers with baggage could cause problems in the United Kingdom and many other states in Europe.

While the provisions of the Hatch Act had concrete effects on the sovereign airspace of many of the contracting states, international organizations such as the International Air Transport Association (IATA) and ICAO were quick to suggest to the United States other methods of improving security standards. Unfortunately, most of the suggestions were for the United States to conform to the provisions of Annex 17 and to the language of the annex in the formulation of U.S. security regulations.

## CONSIDERATION OF ICAO ACTIONS

Throughout the years, the ICAO instituted a number or measures to meet with the increased threat of "unlawful interference with civil aviation." Among those measures were the following:

Establishment of the Aviation Security Cooperation and Development Unit (ASCAD). The unit will be the focal point for assistance and for the funding of programs in the aviation security field.

- Certification of ICAO instructors. A new certification program for instructors in aviation security has been implemented.
- Aviation security training centers (ASTCs). A total of 15 facilities, at least one in each of the regional and subregional areas of ICAO were to be established.
- AVSEC training courses. Over 50 training package programs per year are being conducted in the 15 ICAO ASTCs.
- Aviation security training packages (ASTPs). A new package, ASTP/AIRLINE, has been developed jointly with the International Air Transport Association (IATA). Other ASTPs have been developed by ICAO.
- Establishment of a secure Web site to deal with man-portable air defense systems (MANPADs).
- Establishment of an aviation security regional officer (ASRO) position in three of the ICAO regional offices.

ICAO has also established an audit system called the Universal Security Audit Program (USAP). The program allows for the analysis of client states' aviation security programs with regard to Annex 17 to the Convention on International Civil Aviation Standards.[7]

Finally, one of the more important programs established by ICAO is the requirement for contacting states to develop and utilize machine readable travel documents (MRTDs). This includes new standards stating that all contracting states should begin issuing only machine readable passports (MRPs) by April 1, 2010, and that any non–machine readable passport issued before that date should have an expiration date before November, 24. 2015; and a recommended practice that all client states should incorporate biometric identification in their travel documents. The dates established for compliance seem to be quite a distance down the road (3–8 years) for the effective countering of a current terrorist threat. It becomes increasingly obvious that the steps taken by ICAO, while helpful, do not address the fundamental problem of incident prevention and mitigation, nor do they identify the SARPs, or other ICAO documents, as being deficient in providing quality security direction or procedures to the contracting states.[8]

## CONSIDERATION OF ACTIONS TAKEN BY IATA

A major part of the fallout after the September 2001 attack on the World Trade Center was a marked increase in antiterrorist legislation and

preventive measures initiated by the various states and by ICAO and IATA, as well as by other international organizations associated with international civil aviation. IATA, as always, was in the forefront in seeking to ensure the viability of the international aviation industry. It took very positive steps to improve safety; among the measures taken by IATA was the establishment of the security management systems (SEMS) for air transport operators.[9]

SEMS is a standardized approach to implementing the security processes outlined in IATA's air carrier security program. It is a businesslike approach to the way in which security processes should be implemented and will provide better and more uniform standards throughout the aviation industry. Essentially, SEMS is an element of corporate management responsibility, which sets out a company's security policy for the management of security as an integral part of its overall business, making security one of the company's core values by developing a security culture within the organization.

SEMS is based on ICAO Annex 17 standards and IATA operational safety audit security standards (IOSA). A major responsibility of management in SEMS is the establishment of an effective and focused threat assessment process that will contribute to making security processes proactive. SEMS provides a businesslike approach to security: goals are set and levels of authority are established, thereby ensuring that effective security matters are mandated by IATA.

IATA has established a series of training packages covering most aspects of security within its domain. The overall program is called the Aviation Security Training Package (ASTP). ICAO and IATA have partnered to provide international airlines with the most up-to-date and comprehensive security training packages available worldwide. This package is claimed to be "the answer to your aviation security training challenges." The package is designed for senior managers, middle managers, managers/supervisors, and technical staff.

The disadvantages are few but relatively important, as the package focuses only on those items that are directly associated with IATA's responsibilities to its client states. First, the package does not deal with the ground-associated infrastructure that accompanies all aviation-oriented activity—fuel storage depots, terminal buildings, airport ground transportation, visitor and passenger automobile parking, public transportation access, airport secure areas, and so forth. The fact that various states may have different security requirements makes this program less efficient than it could be. The effort is commendable, but, given the states' own security regulations and the additional requirements of ICAO, it will be very difficult for an individual state to incorporate this program into other security programs. Second, the course costs a considerable amount of money and includes over 900 slides. This constitutes an incredible amount of material for the average employee to assimilate. This criticism is not meant to cast aspersions on the program. It is merely meant to point out areas that can be modified or altered to make it easier and simpler for the average employee to assimilate the information. The greatest advantage is that it is not a correspondence course but one that is taught by ICAO and IATA personnel. For this reason alone, the program is highly recommended and applauded.

IATA did not stop with the establishment of SEMS and ASTP but took further steps to provide training for employees of the aviation community by providing for a course leading to a diploma in aviation security.[10] It is required that participants be graduates of the Senior Management of Civil Aviation Security Course and three other courses over a three-year period. Stringent grading requirements are applied to ensure that participants demonstrate knowledge of the subject.

All of the efforts on the part of ICAO and IATA serve to reinforce the perception that security education is no longer just a course of study to add to a person's resume but now requires a university level course (or the equivalent) of study that will lead to a degree in aviation security management. The education of security specialists can no longer be relegated to the sphere of supplementary education but should now be required. An airline pilot requires specialized education to do her or his job, and so does a security specialist. There is no more important job in the international aviation community than that of aviation security management, and it should be the responsibility of well-trained and educated security professionals.

## THE UNITED NATIONS' APPROACH TO INTERNATIONAL TERRORISM

The United Nations (UN), as the leading international organization, embraced the challenge of international terrorism following the attack on the World Trade Center. The UN made great strides in developing a progressive program to deal with the threat of terrorism. One of the major problems with the UN effort, however, is the political ramifications of dealing with contracting states; the UN charter demands consensus in all of its decisions. The entire international community has had difficulty even in reaching a consensus on the definition of "terrorism." As an international organization, the UN could not and did not permit a definition that equates terrorism with "national liberation movements."

A challenge to the UN is that it must convince the major powers, and especially the United States, as its largest contributor, that security information will not be leaked and used for terrorist activities. The various state intelligence organs must feel secure that information shared with the UN does not warn terrorist organizations of potential operations against them.[11]

When dealing with terrorism, the international community cannot show any weakness or vacillation, because this feeds the terrorist movement, especially as the proponents of terrorism ignore the rules governing the conduct of a civilized society. Any effort against international terrorism requires total commitment if it is to be successful, which explains the U.S. position that recognizes the value of stern preventive/preemptive security measures.

The United Nations must lead the free world against terrorism, and it can only do this by adopting a very strong position against any state or group of states that support, sponsor, encourage, or abet terrorism. A strong position

adopted by the UN will go a long way toward convincing the free world of its determination to join in the battle against unlawful interference in international civil aviation. Such a position would alleviate international concerns and encourage cooperation. Terrorism is an international problem, which can only be defeated with complete cooperation between all contracted states.

## RAMIFICATIONS OF THE HATCH ACT

Since 1999, when the National Proposal for Rulemaking (NPRM) was published by the United States, there have been several major terrorist attacks against the United States, the United Kingdom, Spain, Indonesia, and other states; so severe were the attacks, in fact, that aviation security management has now assumed a position it has never enjoyed, that of being a primary concern in the international struggle against unlawful interference with civil aviation.

When an international organization such as ICAO is expected to provide standards for the entire international aviation community, a major problem for all of the contracting states is created, that is, the time frame associated with rule making. The contracting states must all be appraised of the proposed changes, additions, amendments, or supplements to the appropriate regional air navigation plan. This is an extremely time-consuming process and often takes literally years to go from the initial proposal to final rule making.

When technological changes are proposed to the contracting states, it must be recognized that some of the states do not have the financial or technological expertise available to implement all of the changes proposed. Some changes involve a large outlay of money or require that advanced technology be implemented immediately due to international security concerns. One example is machine readable passports. The less affluent states may not be able to comply with the standards or the time constraints required by ICAO.

ICAO has, in the past, provided the opportunity for the less affluent states to delay compliance with the standards until such time as a state can reasonably be expected to adopt the standards. The delay, however, would not just apply to the less affluent states but to all of the contracting states, as specified in Annex 17. It may well be that a particular technology has become available and the more affluent states want the standards amended to include the new technology. These states, because of the heightened international threat, will want the new technology applied immediately. The problems associated with different states having a different perceived threat level and different abilities to put into effect security measures add to the already complex problem of handling an international incident.

In order to assist in minimizing the effects of such a situation, it is suggested that some method be developed that will allow interstate coordination to take place in a much quicker and more efficient manner in order to handle security problems between states when an international incident occurs.

One step that can be taken is that a *minimum standard of aviation security* be established, and *all* contracting states be required to be in compliance, in

order to receive the sponsorship of the other members of the international aviation community or to enter into interstate letters of understanding concerning state to state aircraft operations.

The most important issue is the fact that aviation security management has come into its own because of the increased security threats that now exist worldwide. In every job description in the aviation industry there appears a section on security responsibilities. It does not matter what domain, air or ground, in the vicinity of an airport or aircraft, security is a prime requirement for each and every employee in the aviation industry. It has become a necessity to have professionally trained and educated personnel in key security positions at all levels of the aviation community. ICAO has already put into effect some of the suggestions that have been made.[12]

Security cannot be relegated to online study or correspondence course study to obtain a qualification for a position as an aviation security specialist. These courses are acceptable for employees whose primary duty is nonsecurity; but positions that are directly security oriented must require professional training and extensive technical training in order to ensure that operatives are able to operate some of the existing, and soon to be existing, technological equipment.

## CRISIS MANAGEMENT TEAMS

One of the most neglected counterterrorist tools is the "think tank." Academic think tanks are said to be helpful in providing a broader view of the phenomena of international terrorism. It is considered a necessity that an organization such as a think tank, a threat assessment team or a crisis management team, hereafter called simply a "team," be organized within the organizational structure of ICAO.

Annex 17, chapter 2, paragraph 2.1.3.b, SARPs, speaks directly to the development of regulations, practices, and procedures that "are capable of responding rapidly to meet any security threat."[13] This paragraph may actually provide for the formation of a crisis management team in each contracting state, with the prototype organization being organized in the ICAO's Air Transport Bureau. This organization would be able to provide a fresh, broad perspective on any international terrorist "incident," as the team would not be directly or operationally involved with the actual incident. Its members would be able to view the incident from all angles and positions.

The team would be directly involved in the examination of all existing documents relating to aviation security management; additionally, in the course of their duties, the members of the team would be "gaming" scenarios of potential terrorist threats, to determine the exact nature of the threat and to assist in establishing a risk management model to ensure that an appropriate level of response is assigned to each determined threat level.

The team would deal with actual incidents and apply the knowledge gained from them to examine existing regulations and procedures with an eye to better preparing the international community. A great deal of experience is

available in the international community, and that experience should be utilized and considered in preparing for the selection of qualified personnel for participation in the team. What better way is there to utilize the skills of dedicated and experienced security specialists, who have actually been involved in combating terrorists and in countering their activities, than in a consulting or operational capacity on a crisis management team. These specialists can provide critical observations and feedback to the international community.

What is needed, and suggested, is a network of crisis management teams throughout the various regions of ICAO, to keep the international community and the various member states up to date on the latest threats and the current counterterrorist technology. It is urged that such a network among the several contracting states be considered by, and supported by, the international organizations and by state security management organizations from the international community.

There is a need for multiple international centers of competence, which will concentrate on specialized tasks as an interdisciplinary contribution to the global war on terror. It is recognized that nationalism and the possibility of compromising the security of a sovereign state is of primary importance. The suggestion of organizing a team as described above may not be realized due to political or bureaucratic problems. Official government operations and coordinated strategies are often held back by procedures, bureaucracy, and political interests.

If such a team is possible, however, the ability to be involved in all phases of an international incident would allow it to examine all aspects of any given situation, from start to finish, with an eye to applying whatever corrections, amendments, or supplements are needed to existing regulations or procedures. An additional advantage of such a team is that some basic weaknesses in procedure could be corrected quickly. The suggestion of such a team comes as a result of a study of the actions of several contracting states in their attempts to achieve a more efficient method of dealing with international terrorism and unlawful interference with civil aircraft.

In almost every state, procedures have been implemented to organize an effective method to forecast threats and develop a national threat level program that will alert the population and all security organizations within the country to the seriousness of the potential threat. Additionally, the setting of a threat level allows the identification of actions that need to be taken at each step of the threat level process. This system is very helpful when dealing with a large population and a large number of security organizations and other organizations that may be the subject of or affected by the threat.

It must be understood at the outset that ICAO has no apparent operational responsibility to perform threat assessment or to take action when an international incident is in progress. The function of ICAO, a coordinating body at best, leaves the operational handling of an incident to the contracting states for the most part. The affected states have the opportunity to employ an ongoing risk management program that is directed toward their state assets,

vulnerabilities, and capabilities. A state, after an incident, has the opportunity to critique its own actions and the actions of other states involved. International organizations, like ICAO or IATA, have little opportunity to participate directly in the incident and are only able to gain access to pertinent information after the fact.

It is suggested that the team lists its first responsibility as reviewing all the international security documents for currency and applicability. It is necessary to review the existing documents to determine how to better assist the contracting states to develop, maintain, and manage a current and effective aviation security program.

## POSSIBLE SOLUTIONS

First, the ICAO document, Annex 17 to the Convention on International Civil Aviation, needs to be reviewed and possibly to have portions rewritten to allow more effective coordination during an incident. Rather than concentrating on assisting the states involved after an incident, ICAO documents should be written to allow for forecasting and preventing incidents, as well as real-time coordination to effect immediate changes or alterations to existing standards and recommended practices (SARPs) to meet specific security requirements.

As an example of the need for real-time coordination, it is necessary to recall that ICAO SARPs discourage a state from requiring a security standard of another state that is in excess of the ICAO standard. If an affected state feels the necessity to demand that specific security measures be taken in another state's sovereign territory, rather than have an argument between the states over whether or not a state can require a higher standard of security, SARPs should be rewritten to reflect the ways in which real-time coordination can be used to temporarily allow for the raising of security standards. Following an incident, security measures may return to the standard called for in the SARPs.

Second, a minimum level of security must be maintained by all states. This requirement would allow each contracting state to know the level, at least the minimum level, of security to be maintained. Additionally, ICAO and other international bodies can identify more readily which states need assistance either to meet the minimum requirements or to implement current or increased requirements. There is a wide disparity among states concerning levels of security. It is not expected that a state such as Bhutan will need the same level of security that Indonesia will need; however, that being said, a minimum level of security at each and every airport in the international system is both desired and anticipated.

Third, the team should be established and organized with the ability to analyze intelligence information and assist in the development of a threat analysis program for contracting states. This program will be designed based on most of the world's threat-analysis programs, adhering to the same risk

management principles and allowing for analysis and forecasting using "gaming principles," while developing real-time responses to threat levels. The responses will allow coordination during an incident on a real-time basis, and, in the aftermath, examine the entire incident with an eye to improving the international community's response to a terrorist threat. A key item in the aftermath will be to reexamine the existing documents and determine whether changes or alterations are needed or desired. The team will, of necessity, be staffed by dedicated security specialists, fully trained in every aspect of aviation security management.

The team would utilize the well-known principles of risk management. Risk management is a cardinal security principle that almost every state employs in its efforts to prepare to meet aviation security threats. Protective security measures are extremely expensive to utilize, and to apply resources when the threat does not dictate it involves a waste or, at the very least, a misuse of those resources. It is for that reason that a risk management system is the only viable way to predict threat level, thus allowing an appropriate level of response to a perceived threat.

One major problem in using risk management principles in the international arena is that two affected states or two security organizations may not see the threat in the same light, thus making an appropriate response to the threat next to impossible. A method must be developed to harmonize differing risk management programs in the international arena, to allow for an adequate response and to ensure efficient utilization of available resources. It will be impossible to arrive at a single risk management program for all states, but a minimum acceptable level of response to threats by all states can and should be achieved.

If one examines the principles involving the development of appropriate risk management procedures, it is obvious that the response can be different with each perceived threat. The reason for developing the program is to provide a vehicle for assessing the threat and devising an appropriate response to that threat. Recognizing this fact allows the state's program to be flexible, allowing for various threats to be properly assessed. There is a need, then, for every state to develop and to formally endorse, in a written document, its risk management program.

Further, the program must be the primary vehicle for the promulgation of all of the state's aviation security management programs. All other security programs will then be derived from the core principles of the risk management program.

Associated with, and an essential part of, the team is the creation of a formal section dedicated to the development and operation of the risk management program. The appointed head of the team must be a direct subordinate of a senior management official. An organizational chart should be developed in which responsibilities are clearly defined and have a dedicated point of contact. The specific procedures for the establishment of the organization can be left up to the individual states.

Each state that has air carriers operating in international airspace should cooperate with and assist those carriers in the development of their individual risk management/threat assessment programs so that the state's team can be complementary to the airlines/organizations.

An effective risk management program depends upon information, a lot of information, derived from state intelligence sources, Internet traffic, verbal tips, and a host of other sources that are needed in order to be able to properly identify and assess a potential threat. A particularly good example is the attack on the World Trade Center in New York on September 11, 2001. There was a wealth of intelligence indicating that a terrorist event was planned prior to the horrific events of that day, but it was not in the hands of a "threat assessment team" or an intelligence group in which all the bits of information could be examined in relation to the other parts. That being said, there was no "silver bullet" giving specific information as to what would be targeted or when or where the attacks would take place. Steps might have been taken by U.S. security organizations to alert airports, increase security measures, inspect incoming foreigners, and check those foreign individuals taking pilot training, had that information been made available to and properly assessed by a single intelligence group. Taking the appropriate steps might have delayed or even prevented the attacks.

A major problem that has been identified as a result of this incident is that the several security organizations in the U.S. did not, for whatever reason, share intelligence information. The sharing of pertinent intelligence information must be a vital part of any risk management program in every state. Information must be processed by one organization in the state dedicated to preventing unlawful interference with international civil aviation.

As part of the team there must be a threat assessment section, to analyze and assess unlawful interference with international civil aviation. The organization is responsible for threat assessment, and then for setting the state's threat level. Threat levels are established to assist security organizations to predict the general responses that are required at specific levels. The system is designed to be as efficient as possible. The threat level will dictate the general response from the state. The threat level also gives the international aviation community and the public information on the status of security in each particular state. The state may utilize the threat level to issue threat warnings or warnings of related incidents affecting civil aviation to many state organizations, departments, and agencies. The information can include in-depth reports on international incident trends, actual terrorist activities worldwide, or the capabilities of terrorist organizations. All the information will have been used to develop the threat level.

Some issues regarding the organization of the team need to be addressed. One of the most important of these is the fact that since the team will be, more than likely, an adjunct of ICAO, the staffing of the team will be controlled by the regulations that presently govern staffing matters in ICAO. This will present a problem. Since ICAO is made up of many sovereign states that must all receive the same consideration, it is possible that a state that

actively sponsors international terrorism may wish to be part of the team and may have a qualified individual to present for a position. The requirement for equal treatment of states by ICAO and the existence of diplomatic immunity are ever present. The problems associated with this situation are clear. At present, there is no solution to this problem.

The team would be made up of professional security specialists selected by the Air Transport Bureau. It is recommended that the organization should be classified as staff members of the Air Transport Bureau (ATB) and report directly to the head of that organization. The ATB would give appropriate autonomy to the team and allow it to function independently of the Security and Facilitation Branch, while allowing it to have appropriate disciplines represented by adjunct members of the team. It is recommended that security qualified personnel from Air Transport, Rules of the Air and Search and Rescue, and Air Communications personnel be included as members. It is possible that a professional psychologist specializing in terrorist profiling techniques may be required or desirable. The specific organization of the team will be dictated by the contracting states and the Air Transport Bureau, in a conclave specifically convened for that purpose. Some responsibilities of the team are suggested here:

1. To review and recommend changes or alterations to all existing international civil aviation security-related documents;
2. To establish a threat assessment program for international civil aviation contracting states;
3. To review and recommend coordination requirements with all ICAO contracting states;
4. To establish a "gaming" program to examine existing procedures for weak and deficient areas;
5. To establish an after-the-fact investigative process with regard to every incident concerning international civil aviation, and provide appropriate recommendations to the Air Transport Bureau for changes, alterations, or supplements to existing regulations or procedures; and
6. To provide a formal, in-depth assessment of the incident, with recommendations, to the Air Transport Bureau.

The threat assessment section of the team will utilize risk management principles in its efforts to provide each contracting state with as much advance information on the possibility of an international incident as possible. Some of the principles of the risk management concept will include the following:

1. Identification of assets;
2. Identification of vulnerable areas of concern;
3. Identification of the threat;
4. Composition of threat scenarios;
5. Determination of whether the threat is credible;

6. Definition of countermeasures;
7. Calculation of the risk; and
8. Optimization of the countermeasures.

## STEPS IN A THREAT ASSESSMENT

The first step of the team will be to identify the system's major assets. In the case of ICAO, the list would include all international civil aviation aircraft and ground support facilities. If possible, the team will provide the financial worth of the international civil aviation system if it or elements of it were destroyed or damaged. This initial function of the team is probably the most difficult of all. Each state could assist by preparing its own list of assets and reporting them to the team. The list and the financial aspect of the list will then be the basis for the structuring of the efforts made to prevent or minimize loss and will be used to prioritize potential threats.

The second step is to identify vulnerabilities and flaws in the contracting states' security regulations and procedures. It is possible to identify major areas of concern and optimize efforts to protect those areas. This is an iterative process and will be combined with the team's actual understanding of the threat. It will be necessary to prioritize vulnerable areas so as to be able to focus attention on the most valuable items.

The third step of the team will be to identify the threat. In order to accomplish this step, an assessment of current intelligence from a variety of sources is necessary, so that the team can evaluate the threat and determine what individual or organization constitutes the threat; also, can the organization or persons identified actually accomplish the potential terrorist incident?

The fourth step is to compose threat scenarios. In how many ways can the threat be actualized? When will the threat be accomplished? Where will it occur? How will it occur? What weapons will be used? Will it be directed against persons or facilities? Questions must be answered, as this process is vital to the determination of a threat level and an appropriate response.

The fifth step is to "game" the scenarios. This means introducing each scenario by computer and examining the actions and reactions of both sides of a potential incident, thereby preparing oneself to make decisions concerning threat level and appropriate responses. It is at this point that previous experience is utilized to compose the various scenarios, evaluate their feasibility, and the assess the probability of a particular scenario. This will enable the team to make appropriate suggestions to the various contracting states concerning security precautions they should prepare for. This step makes a final determination as to whether or not the threat is credible. Information gained from "gaming" the scenarios should give the team a realistic view of a credible event and will allow an appropriate response to be developed.

The sixth step is to define countermeasures. Upon "gaming" the scenarios and establishing that there is a credible threat, the team will determine what actions can be taken to prevent the incident or minimize the damage of a

successful incident. This will include coordination with all affected states and their threat assessment teams.

The seventh step is to calculate the risk involved and determine the appropriate threat level. The threat level will have specific responses attached, and these will be implemented as soon as practicable.

The final step is to "fine tune" the countermeasures to ensure an appropriate response to a specified threat.

It is important to note that ICAO has no operational responsibility or authority to participate in any "action" pursuant to any given international incident. The team will be allowed only to seek and to question, to develop scenarios, to "game," and to discover and/or create innovative ways to meet a terrorist threat. A major advantage will be the opportunity to allow the team to critique all of the actions taken, in a live incident, by all concerned, and then to make recommendations to improve the management of aviation security. The team will be restricted to coordination functions during the actual occurrence of any incident involving a contracting state or its resources. With the use of such a team, ICAO can be an active participant in the development of better regulations, procedures, and programs to assist all contracting states in combating the current terrorist threat. The program will allow an ongoing evaluation and critique of the existing civil aviation security management system. The process would be in real time and on a continuing basis.

When there is no active threat, the team will be involved in developing various scenarios and "gaming" them in order to stay current on all potential threats. The system can be tested at any time for a specific scenario, and the team can accomplish what is known as a "command post exercise." Such an exercise essentially operates on the premise that a "fictional" incident is generated and all systems and organizations are tested to determine the strengths and weaknesses in the states' response. These exercises will be used to modify and modernize the system. As new technology is developed, it can be introduced into the system as a "gaming" item and be tested as if it were actually in place.

## PROFESSIONAL TRAINING NEEDED FOR SECURITY SPECIALISTS

The final step in the process of revisiting the security management of international organizations is to address the training aspect. Since the events of September 11, 2001, it has been recognized by virtually all members of the international community that new, innovative technologies and procedures are in the process of being developed to counter the increasing terrorist threat.

It is obvious from some of the technology being currently developed that special training and education will be required in order to effectively utilize this new technology. It behooves the international aviation community to establish a formal training program for aviation security managers. In the following paragraphs, some of the technology that is now under development will be introduced.

The United States Department of Defense, Defense Advanced Research Projects Agency (DARPA), reported in 2002 that it had developed and was continuing to improve a program called War-Gaming the Asymmetric Environment (WAE).[14] WAE is a revolutionary approach to identifying predictive indicators of terrorist-specific attacks and behaviors by examining their behavior in the broader context of their cultural, political, and ideological environment. WAE has developed indication and warning models for select terrorist individuals and organizations. These models have been tested historically and, in some cases, operationally, to predict an active terrorist group's next action (attack/no attack, target characteristics, location characteristics, tactical characteristics, time frames, and motivating factors). The results have been statistically significant, and several models have been transitioned to Department of Defense and intelligence community partners. DARPA is extending its predictive technology research to model a larger set of terrorist groups and individuals, and these will further exploit predictive technologies to increase the level of detail for each predictive model. This technology needs to be included in the pantheon of tools to be used in the international community to combat terrorist activity.

The Defense Advanced Research Projects Agency (DARPA) has technology in the works that will provide a valuable tool in the identification of terrorists. It is called the Human Identification at a Distance (HumanID) Program, and it will use automated biometric identification technologies to detect, recognize, and identify humans at great distances.[15] A biometric technology approach is a method for identifying an individual from his/her face, or fingerprints, or the way he/she walks. These technologies will provide critical early warning support for force protection and homeland defense against terrorist, criminal, and other human-based threats. They will prevent or decrease the success rate of such attacks against operational facilities and installations. The HumanID Program will develop methods for fusing biometric technologies into advanced human identification systems to enable faster, more accurate, and unconstrained identification at great distances.

DARPA is also developing a device called the Handheld Isothermal Silver Standard Sensor (HISSS). This device is a biological sensor capable of laboratory quality detection of the full spectrum of biological threats—bacteria, viruses, and toxins.[16]

The operation of such a sophisticated piece of technology will require extensive specialized training/education, and so it is highly recommended that the international civil aviation community should establish a formal program to educate future aviation security managers/specialists.

## SUMMARY

In order for the international civil aviation community to recognize the validity of the proposals in this chapter, it will be necessary to examine its members' current posture and determine whether the suggestions have merit.

If they are determined to have merit, and the community desires to implement these suggestions, a conference of all contracting states will be required. The conference would be convened to discuss the relative merits of the suggestions and decide on responsibilities, organization, and funding. It is strongly recommended, in any case, that the appropriate international aviation interests take positive steps to update and improve its system, and take aggressive action to provide a safer system for the international aviation community.

## NOTES

1. William Gutteridge, Institute for the Study of Conflict, *The New Terrorism* (London: Mansell Publishing, 1996), 3.

2. International Civil Aviation Organization, Annex 17 to the Convention of Civil Aviation Security, *Safeguarding International Civil Aviation against Acts of Unlawful Interference* (Montreal: International Civil Aviation Organization, 2006) chapter 2, sub chapter 2.1.3b.

3. Ibid., Chapter 2., subchapter 2.4.

4. United States, Secretary of Transportation, *Anti-terrorist Act of 1996*, Title XIV, Code of Federal Regulations, section 129.25.

5. HatchAmendment,http://900000_ASI_April_1996_hatch_amendment_USA_01, April 1999, 1–3.

6. Ibid., 6.

7. International Civil Aviation Organization, *Accomplishments under the ICAO Aviation Security Plan* (Air Transport Bureau), para. 3.9, sub para. 3.1.0.

8. International Civil Aviation Organization, *Aviation Security Plan of Action* (Security Training Programs), para. 3.8.

9. International Air Transport Association, *Security Management Systems for Air Transport Operators* (Executive Summary), September 2006.

10. Ibid.

11. Isaac Kfir, Institute for Counter Terrorism, *The United Nations Approach to International Terrorism Following 9/11* (Article, March 19, 2004), www.ict.org.il/apage/5522.php.

12. International Civil Aviation Organization, *Accomplishments under the ICAO Aviation Security Plan* (Air Transport Bureau), para. 3.9., sub para. 3.1.0.

13. International Civil Aviation Organization, Annex 17 to the Convention of Civil Aviation Security, *Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, chapter 2, sub chapter 2.1.3b.

14. United States Department of Defense, Defense Advanced Research Projects Agency (DARPA) *A Compendium of DARPA Programs*, April 2002, 7–9, www.darpa.mil/body/news/2002/darpa-fact.html.

15. Ibid., 7–9.

16. Tony Tether, Director of the Defense Advanced Research Projects Agency (DARPA), *Report*, submitted to Sub-committee on Terrorism, Unconventional Threats and Capabilities of the House of Representatives Armed Services Committee, March 29, 2006, 25.

# CHAPTER 3

# Dealing with Human Vulnerability in Aviation Security: Effectiveness of SCAN Detecting "Compromise"

*Anthony T. H. Chin*

The aviation sector spends millions of dollars on sophisticated hardware in securing airports and airplanes. However, the weakest link, often overlooked, is that between security and airport or airline personnel. Lapses in security can be a result of graft, where an individual compromises security in exchange for payment. This is a criminal offense that can cost lives. Compromises in security or criminal behavior are perceived by many as decisions largely based on personality characteristics, moral values, socioeconomic conditions, or family background; factors that are seemingly beyond the study of economics. However, economists suggest that individuals make rational decisions as to whether to commit crimes. Armed with a robust economic theoretical framework, the economist seeks to show that increasing the probability of detection and the magnitude of punishment or penalties ought to deter a would-be criminal or compromiser of security. Such deterrence can perhaps be carried out in inexpensive and efficient ways through the use of forensic assessment tools. Simply increasing the probability of detection through effectively employing instruments such as the polygraph, verbal/behavioral analysis, and statement analysis can deter prospective security compromisers.

An experimental framework was thus set up to test the reliability of forensic tools as an instrument to increase the probability of detection. Scientific content analysis (SCAN), a technique that analyzes linguistic structure and content, was chosen as the object of interest. In the resulting analysis, various dominant strategies emerge for guilty as well as for innocent participants, which will provide a framework of applying SCAN to aviation security.

The results indicate that SCAN is most efficient if used together with other forensic tools. This is because it is weaker in detecting innocence in participants

and hence would need to be employed jointly with other assessment tools in order to improve in this aspect. This study shows, however, that increasing probability of detection can be achieved through the use of forensic assessment tools such as SCAN, which is inexpensive to administer. Through the use of such tests, crime deterrence can now be efficiently achieved at a low cost by raising the probability of detection, which in turn results in an optimal equilibrium level of crime or deception.

## INTRODUCTION

Prior to Becker's seminal study on the economics of crime and punishment, few economists looked at crime within an economic framework.[1] This was possibly due to the fact that crime is associated with immoral values and attitudes, which defy methodical economic investigation. In addition, crime seemed to be primarily influenced by socioeconomic factors, family background, personality, or even genetics, and thus was best left to psychology or sociology.[2] Moreover, crime was perceived as an irrational behavior resulting in an inefficient decision. This is because criminals having full knowledge of the penalties if arrested still choose to commit the crime. Crime was thus viewed as being incompatible with an economic framework, where rationality results in efficient decisions.[3]

However, an economic framework is possible if the act is viewed as part of an individual's choice set. Criminal activity seeks to maximize gains from crime, given the severity of punishment and the probability of apprehension. Viewed in this light, the decision to commit a crime is in fact an individual's rational choice maximization. Additionally, rational behavior entails an individual weighing the pros and cons of alternatives before choosing one that maximizes his utility. This is consistent with the criminal decision-making process, since individuals do consider the foregone opportunity costs of legal activities in deciding to commit a crime.[4]

From society's viewpoint, crime is inefficient because it generates negative externalities. Hence, deterrence is needed to inhibit criminal activity. The deterrence hypo-study states that the level of criminal activity responds to the costs and benefits of crime.[5] Since valuation of the benefits of crime is determined by individuals, law enforcers can only regulate crime through increasing its costs. This can be achieved by increasing the probability of arrest and/or the severity of punishment. Logically, it would seem that complete deterrence would be optimal for society since crime is something which society tries to avoid. This is incorrect and in actual fact inefficient, because deterrence comes at a cost. This cost includes expenditure on hiring law enforcement officers or installing anticriminal devices such as hidden cameras. Thus, the optimal level of deterrence is reached when the marginal cost of deterrence is equal to the marginal benefit of crime. This is contrary to popular wisdom in the economic analysis of crime, and if the larger deterrent effect is significant, it entails costly law expenditure.

This study seeks to examine whether the probability of detection can be increased indirectly through the use of affordable forensic assessment tools in criminal investigations. In particular, we are interested in examining the validity and time reliability of the forensic tool, scientific content analysis (SCAN). In addition, we examine how SCAN's validity is affected by gender and prior antideception training. Thus, this study endeavors to quantify SCAN assessment and determine how it affects the probability of detection as well.

The next section discusses the market for crime and the concept of optimal quantity of crime, followed by an analysis of how an individual optimizes his amount of crime based on expected payoffs and costs under norm-guided rational behavior. The third section introduces SCAN and explains how it detects deception by analyzing linguistic structures. The experimental framework, the objectives, and the way the experiment was conducted are covered in the fourth section. Results from the experiment are presented and analyzed, and the study concludes with a summary of the main findings from the experiment and the policy implications.

## LITERATURE REVIEW

In the economic analysis of crime, individuals will only commit a crime when their expected marginal benefits exceed their expected marginal costs. This section looks at the macroeconomic market demand and supply of offenses, followed by the microeconomic behavior of individuals when deciding whether to commit a crime.

### Supply and Demand for Offenses

The crime market is based on five key assumptions.[6] First, all participants in the market, buyers and sellers of illegal activities/goods and law enforcement officials, behave according to the rules of optimizing behavior. All agents seek to maximize personal utility subject to constraints. Second, certain expectations about legal and illegal activities payoff are formed based on the information that is available. This payoff is determined by the probability of detection and the severity of punishment. Third, there is a stable distribution of preference for crime as well as safety from crime. This translates into the derived demand for law enforcement. Fourth, law enforcement aims to maximize social welfare. Finally, the summation of all individuals' preferences in the market leads to an equilibrium level of crime (q*), since this is where demand intersects with supply.

#### *Supply of offenses*

The supply of offenses is a function of why people choose to commit crime. With reference to the assumptions stated earlier, we can determine the profit function of crime. The profit function ($\pi_c$) varies positively with income from crime ($w_c$) and is negatively related to costs of crime ($c_c$),[7] wages forgone from

legal activities ($w_1$), and the multiplication of probability of detection and severity of penalty ($p_c \cdot f$). Mathematically, this can be written as follows:

$$\pi_c = w_c - c_c - w_l - (p_c \cdot f) \quad (1)$$

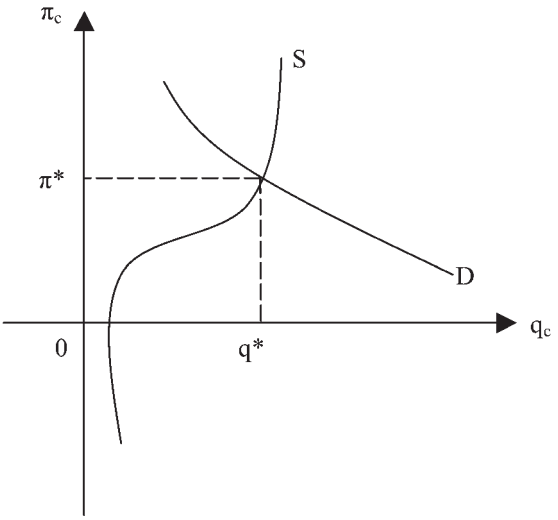
Individuals are risk neutral and aversion to crime is a constant. This aversion to crime will affect an individual's decision to commit crime. To induce an individual to commit crime, the net expected benefits must exceed a certain level to compensate for his aversion. Thus, the resulting supply of offenses will be a function of an individual's private net expected benefit from crime.

Based on these assumptions, the supply of offenses is then the minimal level of benefit from illegal activities needed to induce crime. Conversely, it can be viewed as the summation of individuals' maximum threshold to crime aversion, since exceeding this level will entice one to crime. Assuming that the population's threshold for crime is normally distributed, the supply of offences will be upward sloping,[8] as depicted in Figure 3.1 (S). This means that crime ($q_c$) increases as the net benefits from crime rise.

### *Demand for offenses*

The demand for crime is a derived demand because crime protection incurs costs. Since absolute protection from crime is costly, individuals need to live with an optimal amount of crime, which is the point where the marginal benefits of crime protection are equal to its marginal costs. Thus, demand for crime is derived from the optimal demand of crime protection.[9]

**Figure 3.1**
**Regression Results of Detention Strategy**



The demand for crime protection is derived from minimizing expected loss from crime. Optimal expenditure has a direct positive relationship with and is a function of the probability of being a crime victim and the expected loss from crime. Assuming rational expectations, every individual perceives his/her risk of being victimized as equal to the crime rate ($q_c$) in the population. Therefore, the demand for crime protection increases as the crime rate rises. With reference to Figure 3.1, the derived demand for crime is downward sloping (D). This is because with higher crime rates, individuals will spend more on crime protection (direct relationship between crime protection expenditure and crime rates), which in turn reduces the offender's benefit from crime. The benefits from crime are lowered as the offender has to spend more time and effort now to commit the crime (thereby raising his/her direct costs of crime, $c_c$), and his/her opportunity costs of losing wages from legal activities are higher ($w_l$). Thus, the expected net benefits from crime (see equation 1) are now reduced.

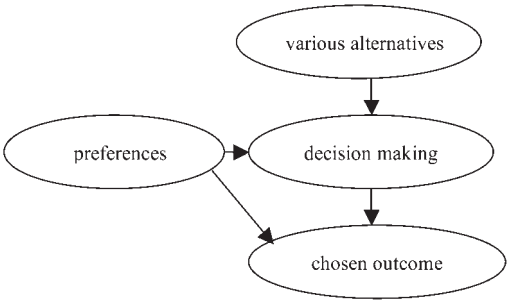
## Extension of Rational Behavior with Norms

After establishing the market equilibrium for crime, we now turn our attention to how individuals rationally optimize their choice of criminal activity based on utility maximization. The rational criminal commits a crime only when his/her benefit from illegal activity is higher than that from legal alternatives. In contrast, sociologists, criminologists, and psychologists model crime based on social factors. Individual choice is not important and crime originates from biological, environmental, psychological, and socioeconomic factors. Norms[10] are therefore important in their analysis, since crime deviates from socially accepted behavior.

Empirical research thus far suggests that both approaches should be included in the analysis of crime and neither is superior to the other. To reconcile the two approaches, Eide suggests an extension of the traditional rational behavior model by including norms in the decision-making process.[11] This inclusion is important in the economic analysis of crime because norms do affect the desirability of outcomes. An individual has to consider monetary gains as well as society's disapproval and possible rejection when weighing the benefits and costs of crime. Figure 3.2 graphically delineates the extended rational decision-making process.

From Figure 3.2, it is clear that individual preferences affect the decision-making process with regard to the most desirable outcome. Preferences in the extended model include monetary benefits and norms like social acceptance and warmth. If we include norms as part of decision making, individuals may choose not to commit a crime even if the monetary benefits are higher than the costs. This is because if they value social acceptance highly, the costs of crime will be greater than its benefits, since they face possible rejection by society. In this extended model, then, norms guide the rational choice decision but are not pivotal in the final selection of outcome. Therefore, the individual still weighs the costs and benefits of each outcome before making an optimal choice.

**Figure 3.2**
**Preferences and Decision-making Factors**




In a self-reported survey of 808 young males, more than 40 percent stated that personal restraints[12] would stop them from committing a crime, indicating that norms do play a significant role in the decision to commit crime.

### The Individual's Risk Preference

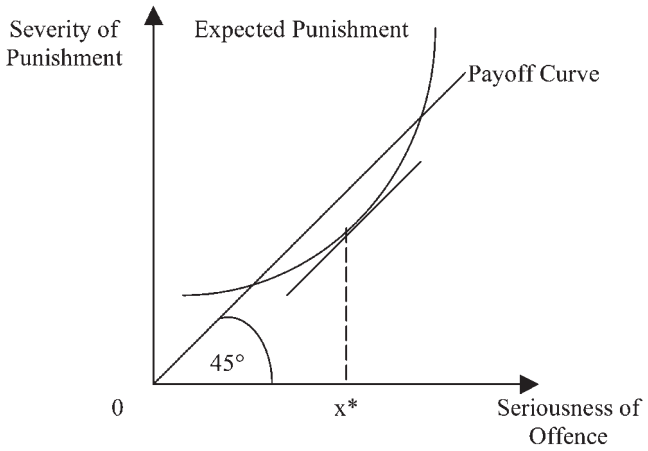
To develop our understanding of an individual's decision-making process, it is important to know his/her risk preference under norm-guided rational behavior. This is attributable to microeconomic theory, where an individual's risk preference determines his/her behavior in a situation of uncertainty. A similar analysis is employed here because individuals do not know their true probability of detection, and risk preferences determine optimal law enforcement, which in turn affects criminal behavior. Risk neutral individuals will make a decision to commit crime by comparing the benefits and costs of crime. In contrast, risk averse individuals will only commit a crime when the marginal benefit of crime is greater than the marginal costs.

Compared to the case of a risk neutral population, the fine imposed for a risk adverse population will not be as large and the probability of apprehension will be higher. This is so because the benefits from lower law enforcement expenditure must be considered against the increased level of risk. Accordingly, the level of risk borne by risk averse individuals should be minimized. Thus, the optimal probability of apprehension and fine will be a calibration of how the probability of apprehension falls as law enforcement expenditure decreases and the degree of risk aversion in the population.

### The Economic Theory of Crime

In the economic framework of crime, all offenders are assumed to have norm-guided rational behavior and they will choose criminal behavior only when the expected payoff is greater than the expected punishment. With reference to Figure 3.3, the x-axis is the seriousness of offence while the y-axis

**Figure 3.3**
**Punishment, Seriousness of Offence, and Payoff**




is the severity of punishment. In Figure 3.3, the severity of punishment is directly proportional to the seriousness of crime. This implies that that the expected gain is a function of crime. Thus, the expected payoff line has an angle of 45°, since x = y. The expected punishment curve is a function of the probability of apprehension ($p_c$) and the severity of punishment (f). Optimally, the rational criminal will choose to commit x* amount of crime since this is the point where marginal benefit from crime is equal to marginal cost. The expected punishment curve will shift when $p_c$ or f changes. In reality, the probability of apprehension rises with the severity of the offense, since more serious crimes (e.g., murder) will produce greater enforcement effort. The severity of punishment is also positively related to the seriousness of the crime. In addition, the expected punishment is influenced by possible societal disapproval when norms are violated and by the shame felt by the offender.

It is clear that the optimal amount of crime is influenced by the probability of detection, severity of punishment, and degree of risk aversion. Since most individuals are assumed to be risk averse, it would be beneficial to modulate crime through increased probability of detection rather than by harsh penalties to reduce the risk premium. However, cost considerations come into play because of the direct relationship between higher detection rates and enforcement expenditure. It is plausible that forensic assessment techniques can contribute to aid detection since they are less costly to enforce. In particular, we employ scientific content analysis (SCAN).

## SCIENTIFIC CONTENT ANALYSIS AND HYPO-STUDY

One way to increase the probability of detection of crime ($p_c$) is to increase the "amount" of law enforcement. This is so partly because the probability of

detection can be increased indirectly through the use of forensic assessment interview tools such as the polygraph test, psychological profiling, and observation of body or verbal language and analysis of written statements.

## Scientific Content Analysis (SCAN)

Scientific content analysis (SCAN) draws on many years of intensive research into verbal communication, specifically researching on linguistics in communication. The basic hypo-study postulates that most people do not want to lie and would rather give information freely, and that about 90 percent of all statements are truthful. However, if one tells lies, one prefers not to lie directly but to employ conversational tricks. Some of these tricks include the omitting facts, feigning forgetfulness, or pretending to be ignorant. A question is answered with a question, very brief in critical parts of stories. or narrative gaps are filled in with uninformative statements like "we talked" (about what topic?) or "afterward" (after what event?).

SCAN detects deception by analyzing the structure and content of the written statement through the use of speech patterns. The truth is simply hidden when people lie. Thus, through the analysis of written statements and the breaking of linguistic codes, linguistic inconsistencies are detected. SCAN testing also includes a section called View Guidebook, a series of structured questions based on the SCAN principles.[13] The linguistic structure of responses to these questions is also analyzed for deception. Statements are a form of alternate reality and are even more important than the person. "The person is dead, the statement is alive."[14]

### *Analysis of responses*

The use of pronouns can indicate whether a person is being truthful.[15] Pronouns are significant in the analysis because one can never be confused by their use. A change in pronoun use thus suggests a shift in relationship. Inappropriate use of pronouns may also signal possible deception. To illustrate this, it is highly suggestive if a victim in a kidnapping case uses the pronoun "we" to refer to the kidnapper and himself. This is because "we" signifies compliance, teamwork, and partnership.

## Hypo-study

Although SCAN has been proven useful in assisting law enforcement to determine a suspect's guilt, it is still far from an ideal system, because it is very subjective and does not have a formula for scoring. This is due to the fact that analysis is solely based on the evaluator's judgemnt upon reading the statements. This is a major point of contention and has led many people to doubt SCAN's validity. Further, there is a time lag between the crime and the interrogation. To be robust, SCAN should be able to accurately detect deception regardless of whether the suspect was tested one day after committing the crime or a few years later.

The Internet has created an awareness of forensic testing and of possible techniques to pass the examination. Rationally, both innocent and guilty suspects will seek this information and prepare themselves for an assessment. This is because the innocent are doubtful of the tool's accuracy and would want to avoid a false positive conclusion, so they learn these skills to prove their innocence. In contrast, the guilty would strive for a false negative outcome[16] and hope that learning such skills would enable them to beat the system.

Finally, in order for SCAN to be a valid testing tool for deception, its detection rates should be consistent across gender. If gender bias were present, this would render the test inefficient. This study seeks to examine whether SCAN is valid as a forensic assessment tool in an experimental setup. Its validity is ascertained by testing for accuracy, time consistency, and gender bias. In addition, we examine whether prior training to defeat forensic testing will affect SCAN's accuracy in detecting deception. By controlling for these factors that exist in reality, we gain more confidence in our resulting analysis, which has greater external validity.

As discussed earlier, deterrence has often been achieved by manipulating the severity of fine because it is the most cost efficient method. Unfortunately, this leads to a less than optimal amount of crime, because risk averse individuals are "over-deterred." If SCAN is determined to be valid as a tool in detecting deception, this means that it is able to significantly increase the probability of detection. Given that deterrence is a function of probability of detection and severity of fine, this translates into lower fines in law enforcement to achieve the same level of deterrence. Consequently, the risk premium of risk averse individuals can be lowered and an optimal level of crime will be achieved, because they will not be "over-deterred."

## EXPERIMENTAL SETUP

### Experimental Objectives

A crucial disadvantage of SCAN as a forensic assessment tool is its subjective scoring based on heuristics. Due to this, many have discredited its use because of the belief that this scoring method leads to biased judgments based on an evaluator's impression. In this experiment, we seek to test whether this censure is valid by having an evaluator assess SCAN using a scoring formula. Although this deviates from the usual heuristic assessment, the systematic evaluation technique is still founded on the principles of SCAN.

Due to investigative procedures, criminal suspects are often apprehended some time after committing the crime. The time lag varies from a day to a few years. Thus, this experiment attempts to find out if there is empirical support for SCAN's consistency as a forensic tool given a time difference between committing the crime and administering the test. This is achieved by assigning participants to be tested either one day (t+1) or three days (t+3) after the experiment (which is described below). A proportion of participants who have

been assigned as guilty or innocent receive antideception training, that is, they are taught either mental or physical antipolygraph techniques. Although these skills are not specifically designed to deceive SCAN, it would be useful to see whether antideception training skills are transferable across forensic assessment tools.

As discussed in the hypo-study, both innocent and guilty suspects have an incentive to learn these techniques in order to appear innocent. This intrinsic motivation is replicated in the experiment by giving a larger monetary reward if participants are deemed to be innocent after testing, regardless of their true state. Through this monetary motivation, this study gains greater external validity as well, because participants will do all they can to appear innocent during testing, which is exactly what happens in real life. In addition, having the same payoff structure for both guilty and innocent participants ensures that their severity of punishment is kept constant. This means that their only variable in determining cost of crime is the probability of detection, which in this case is SCAN. Finally, an equal number of males and females were selected for this experiment to test for gender bias in SCAN.

## Sample Population

From a pool of participants who responded to calls for participation in an experiment, a random sample of 72 males and 72 females were selected. All 144 participants were undergraduates from the National University of Singapore (NUS). In this $3 \times 2 \times 2$ experimental design, an equal number of male and female participants were randomly assigned to each of the 12 experimental conditions. A graphical outline of the experimental design is given in Figure 3.4, while the distribution of participants from each gender in each of the 12 experimental conditions is shown in Table 3.1.

**Figure 3.4**
**Sample Structure**

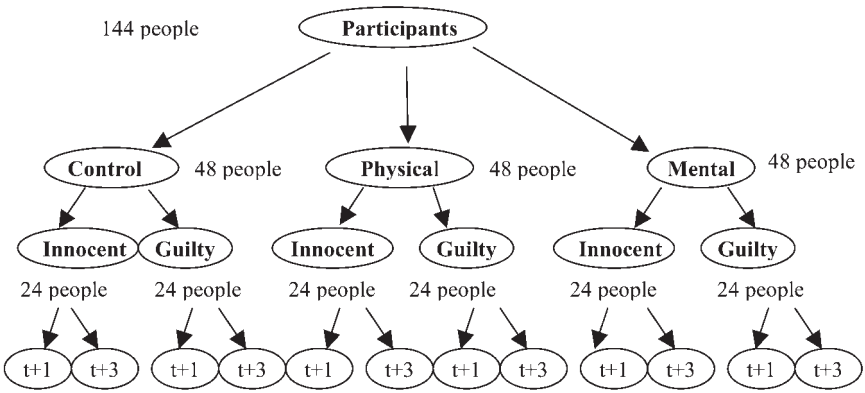


**Table 3.1**
**Distribution of Participants Across Experimental Groups**

| *Experimental group/ Gender* | *Number of Days* | *CG* | *CI* | *PG* | *PI* | *MG* | *MI* |
|---|---|---|---|---|---|---|---|
| Male | t + 1 | 6 | 6 | 6 | 6 | 6 | 6 |
| | t + 3 | 6 | 6 | 6 | 6 | 6 | 6 |
| Female | t + 1 | 6 | 6 | 6 | 6 | 6 | 6 |
| | t + 3 | 6 | 6 | 6 | 6 | 6 | 6 |
| Total | – | 24 | 24 | 24 | 24 | 24 | 24 |

CG = Control Guilty, CI = Control Innocent, PG = Physical Guilty, PI = Physical Innocent, MG = Mental Guilty, MI = Mental Innocent.

## Experimental Groups

In this $3 \times 2 \times 2$ experimental design, there are three main treatment groups (control, physical, mental), two conditional groups within each treatment (innocent, guilty), and a further two conditional conditions within each group (t+1, t+3). Thus, there are in total 12 experimental conditions as depicted in Table 3.1, with 6 males and 6 females in each condition. Participants in the control group are not given antidetection training before testing. Therefore, they can be viewed as the baseline measurement for comparison with the other two experimental groups to observe the effects of training.

On the other hand, participants in the physical or mental treatment groups are taught techniques to pass the polygraph test. For example, participants in the physical treatment group are taught how to regulate or hasten their breathing rates when the control questions are asked, in order to corrupt the physiological readings. In contrast, participants in the mental treatment group are taught cognitive skills to defeat the polygraph. For example, they are taught how to count backwards when asked sensitive questions, in order to regulate their physiological responses.

In addition, participants who have been assigned to a guilty condition will have to simulate criminal behavior by accepting a bribe in the form of money from an individual in exchange for the security plans of an airport. In contrast, participants in the innocent conditions will have no knowledge except that a crime has been committed. Depending on whether they have been assigned to be tested either one (t+1) or three days (t+3) after the conduct of the experiment, all participants will report back to NUS for a SCAN test followed by a polygraph examination.

## Conduct of the Experiment

The experiment was conducted in the grounds of the National University of Singapore (NUS). All participants were asked to report to a tutorial room where they were given instructions via a taped recording. Participants who were in any of the three guilty conditions[17] were given 15 minutes to complete

the transaction, that is, commit the crime. Instructions were given for them to find their way with the aid of a map to a particular room where they would look for a black briefcase in which they were to put the security plans of an airport in exchange for a brown envelope marked "X" on both sides.[18] Before entering, they would have to knock on the door and check that no one was in the room. If no one answered, they would then proceed to let themselves into the room. They would then have to search the contents of the briefcase carefully to find a sealed envelope marked with an "X" on both sides. After locating the envelope, they would have to replace the contents and the plans in the briefcase as if it had not been tampered with. Participants were warned that should someone walk in at any time while they were committing the crime, they would have to think of an excuse and continue whatever they were doing.

This instruction was given to model the fear that criminals have when they are committing a crime in reality that someone might walk in on them. After committing the crime, the participants had a 20-minute break in which they were free to walk around the campus before reporting back to the experimenter with the envelope. Upon returning the envelope to the experimenter, they were asked to tear the envelope open and remove five 10-dollar notes from inside it. They would then return this money to the experimenter and sign their names on the stolen envelope. Instructions were also given to them not to discuss the experiment with anyone, to deny all involvement with the crime if asked, and always to appear truthful.

All participants would then return for testing either one or three days later, depending on their condition assignment. The only difference between the three guilty conditions would be that participants who had been assigned to be taught either mental or physical techniques would complete their training immediately after returning the money to the experimenter. Participants in the innocent conditions would listen to a taped recording as well. However, they would not be instructed to find the room with the black briefcase but instead be given a 15-minute leisure period in which they were free to do whatever they wanted. They did know that a crime was being committed during this time, but they had no details. After 15 minutes, they would report back to the experimenter and return for testing either one or three days later. As with the guilty participants, the only difference between the innocent treatment groups[19] was that participants in the physical or mental condition would have to receive their training immediately upon returning from their break.

All participants would first undergo the SCAN test and then a polygraph examination, regardless of whether they returned one or three days later. All participants had an incentive to prove themselves innocent in both tests. This was because they would receive a SG$50 token if they were declared innocent at the end of testing, regardless of whether they were truly innocent.[20] If the verdict was inconclusive or guilty, they would only receive a token of SG$30. Thus, all participants, including those who had been assigned to the innocent conditions, had a strong motivation to pass the detection tests and earn a higher token.

## ANALYSIS AND DISCUSSION OF RESULTS

### Evaluation of SCAN

The SCAN questionnaire consisted of eight pages on which suspects wrote their answers in full sentences. They were instructed to think of their answer carefully before writing, because they were not allowed to make corrections. All completed SCAN questionnaires were independently assessed by a certified forensic evaluator. As discussed earlier, the analysis of SCAN statements is very subjective because there is no precise numerical scoring technique. Therefore, evaluators make their judgment calls based on their experience and their impression of the narrative. We report the judgment calls from three experts based on the VIEW questionnaire[21] (based specifically on the eight questions; see Appendix).

The evaluator used an objective scoring system in which each question is given a possible rating of –2 to 2 (inclusive of zero). A rating of –2 or –1 means the evaluator feels that the suspect is lying or possibly lying, respectively. On the other hand, a score of 2 or 1 implies that the evaluator feels the suspect is truthful or possibly truthful. A score of 0 suggests that the evaluator cannot come to a conclusion about the statement.

Next, the rating of each question is added up and the final view call is based on the sum of the scores on the eight questions. The range of the sum of scores attainable is from –16 to 16. Based on these scores, participants are determined to be either problematic (i.e., guilty), leaning toward being problematic, leaning toward being cleared, or cleared (i.e., innocent). It must be noted that although this scoring scheme is markedly different from SCAN's standard assessment, it is based on the principles of SCAN. Figure 3.5 illustrates the assessment scheme.

### Graphical Analysis of SCAN's Accuracy

One major obstacle to testing the accuracy of SCAN in detecting deception was that the true state of the suspect is not available in reality. This

**Figure 3.5**
**Detecting Deception**

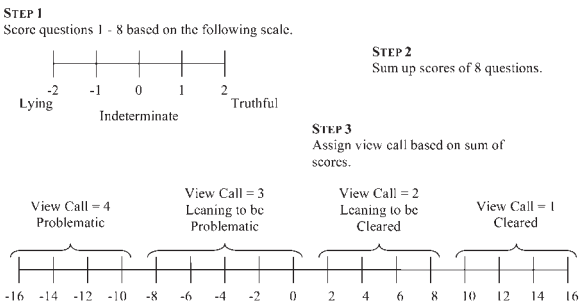
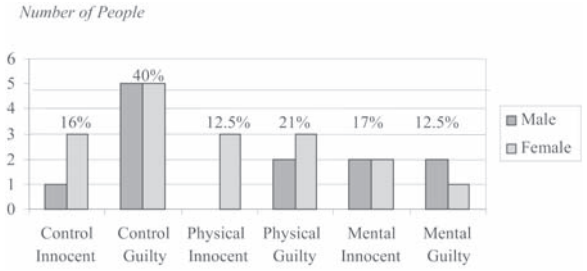


**Figure 3.6**
**Gender Differences**




was overcome in the experimental framework because the true condition of each participant is known. With reference to the earlier discussion on SCAN evaluation, there are four view calls under which suspects fall. In this study, the accuracy of SCAN (the hit rate) is determined to be the correct fit between the true condition (guilty or innocent) and the view call (problematic or cleared). Participants who were classified as leaning toward being cleared or leaning toward being problematic are disregarded. Figure 3.6 illustrates the distribution of correct hits SCAN achieved between groups and within each gender.

The hit rate percentage from Figure 3.6 indicates that SCAN is reasonably accurate in detecting deception in all treatment groups, except when mental techniques are taught. This is reflected in the higher hit rates in the guilty condition compared to the hit rates in the innocent condition in both the physical and control groups, except in the mental group. It is most accurate in guilt detection in the control group, where there is a high hit rate of 40 percent.

However, SCAN is not very efficient in detecting innocence, because the innocence accuracy rates are lower than the guilty hit rates. It is higher only in the mental treatment group, but only at a marginal rate of 4.5 percent. This is in comparison with a difference of 24 percent in the control group and 8.5 percent in the physical group.

## Gender Differences between Groups

### *Graphical analysis*

One of the experimental objectives was to see if there is any gender bias in SCAN evaluation. As can be seen in Figures 3.7 and 3.8, which chart the mean score of females and males, respectively, across the groups, there is a clear difference between the scores of the control guilty and control innocent groups. In particular, the control innocent groups have positive scores while the control guilty groups' scores are negative. This trend supports SCAN's efficiency in detecting deception, because a clear disparity exists between the two groups.

**Figure 3.7**
**Females**

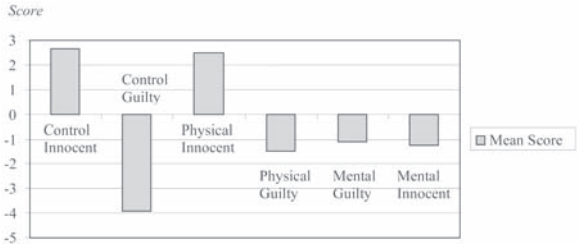
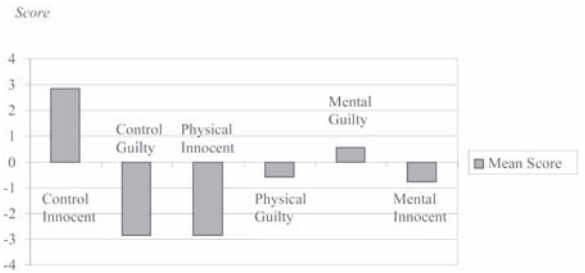



**Figure 3.8**
**Males**




However, the mean scores for the remaining four treatment groups are skewed. To illustrate this, females' mean scores for mental innocent and males' mean score for physical innocent, mental guilty, and mental innocent all work against the theory of SCAN. This shows that SCAN is inefficient in detecting deception once participants have received any form of training. This result echoes the graphical analysis of SCAN's accuracy given in the previous section. Specifically, Figure 3.8 suggests that guilty males should employ mental techniques because they will be able to pass the test. In contrast, the negative score in the mental guilty condition in Figure 3.7 hints that the mental techniques are ineffective for females because the scores are negative. This is incorrect, however, because upon closer observation, we see that the score for mental guilty is higher than the score for physical guilty, which means that mental techniques are still more effective for females.

Innocent females should learn physical techniques because they will be able to ensure that their scores will be positive, matching their true state. This contrasts with innocent males, who should avoid physical techniques because their scores are negative. Thus, gender bias is suggested by the graphical analysis, as seen in the different mean scores obtained between groups and the conclusion that males and females should employ different techniques to achieve their goals of displaying innocence or hiding guilt.

### *F-Test of mean scores between groups for gender differences*

F-tests were conducted to test if the gender difference in mean scores between groups is significant. The null hypo-study states that there is no significant difference in scores between males and females. If the null is not rejected, it shows that SCAN does not discriminate across gender when testing. The results are summarized in Table 3.2 below. At the 10 percent significance level, all p-values are greater than 0.1, which means that the test fails to reject the null, except for the physical innocent group. Therefore, there is a gender bias in the SCAN test in this treatment group. This statistical result concurs with the graphical analysis shown earlier, where there were differences across gender mean scores in the physical innocent group.

F-tests were also carried out to test the mean scores of the six groups within each gender. The results are summarized in Table 3.3. The F-statistic obtained for males was 1.632 ($p > .1$), which means that scores are not significant between groups for males. Simply, the different treatment groups had no effect on males' SCAN scores. However, the F-statistic obtained for females was 2.672 ($p < .1$), which rejects the null. Thus, we can conclude that after controlling the gender variable, the mean scores differ significantly between groups for female participants at 10 percent significance level.

## Time Consistency of SCAN

### *Graphical analysis*

Participants underwent SCAN testing either one or three days later after being taught antipolygraph techniques. This experimental variable sought to test if SCAN gives the same consistent result regardless of when the test is administered after the crime is committed (i.e., time effect). If SCAN is a consistent tool, there should be no divergence in scores whether participants are tested one day or three days after committing the crime. This is to say

**Table 3.2**
**Results of F-Test for Gender Differences Between Groups**

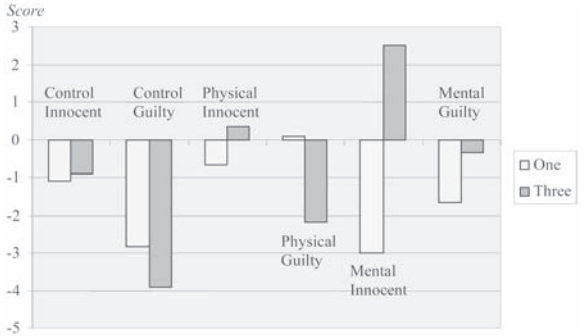
| *Experimental Group* | *CG* | *CI* | *PG* | *P I* | *MG* | *MI* |
|---|---|---|---|---|---|---|
| F-statistic | 1.2169 | 0.1709 | 5.5162 | 0.1321 | 0.3447 | 0.0492 |
| df | (1, 22) | (1, 22) | (1, 22) | (1, 22) | (1, 22) | (1, 22) |
| Probability | 0.2819 | 0.6833 | 0.0282 | 0.7198 | 0.5631 | 0.8265 |
| CATEGORY statistics | | | | | | |
| Female mean | 0.33333 | –3.9166 | 2.5000 | –1.5000 | –1.0833 | –1.2500 |
| Male mean | –2.3333 | –2.8333 | 5.6219 | –0.5833 | 0.5833 | –0.7500 |

CG = Control Guilty, CI = Control Innocent, PG = Physical Guilty.

**Table 3.3**
**Results of F-Test for Mean Score Differences Between Male and Female**

| *Gender* | *Male* | *Female* |
|---|---|---|
| F-statistic | 1.631533 | 2.672493 |
| df | (5, 66) | (5, 66) |
| Probability | 0.1639 | 0.0293 |
| CATEGORY statistics—Mean scores | | |
| Control Guilty | –2.833333 | –3.916667 |
| Control Innocent | 2.833333 | 2.666667 |
| Mental Guilty | –0.750000 | –1.250000 |
| Mental Innocent | 0.583333 | –1.083333 |
| Physical Guilty | –0.583333 | –1.500000 |
| Physical Innocent | –2.833333 | 2.500000 |

**Figure 3.9**
**Breakdown by Groups**




that all guilty participants and innocent participants should always have negative and positive scores, respectively. Figure 3.9 illustrates the distribution of mean scores between the six groups, with a breakdown of the mean score for participants who were tested one day or three days after training.

As seen in Figure 3.9, the mean scores are unambiguously negative for the control group, regardless of whether participants are guilty or innocent. The only observable difference is that the scores for the guilty are higher on the negative scale in comparison to the scores for the innocent. This is consistent with the analysis provided above, showing that SCAN detects guilty suspects more efficiently. A time effect is observed in the physical treatment group, because there is a divergence of scores in both the guilty and innocent conditions. The distribution of mean scores reveals that the innocent obtain negative scores when testing is performed one day later and positive scores when it is performed three days later. Guilty participants, on the other hand, obtain negative scores when tested three days later and positive scores when tested a day later.

Like the physical innocent, mental innocent participants have a disparity in mean scores between testing after one or three days. This leads us to the same conclusion that we came to earlier: that innocent participants should not learn any form of techniques to pass forensic tests because their scores will be biased in the wrong direction. There is also a wider difference in scores in the mental innocent condition compared to the scores in the physical innocent condition. This means that the mental innocent have a higher probability of being incorrectly deemed guilty after learning mental techniques. Figure 3.9 also shows that no time effects exist for guilty participants, because their scores are negative regardless of the time they are tested after committing the crime.

### *F-Test of mean scores between groups for time differences*

The preceding graphical analysis indicates that time inconsistency exists in the SCAN results, so an F-test was conducted to test for mean score differences between participants who took the test one day after training and those who took it three days after training. The null hypo-study states that the number of days (t+1 or t+3) after which SCAN is administered following the crime does not significantly affect the mean scores between the two groups. The F-statistic obtained was 0.582 ($p > .1$) with degrees of freedom (1, 142). Therefore, we fail to reject the null at 10 percent significance level and conclude that the SCAN results are consistent between participants who take the test either one day or three days after committing the crime.

Further F-tests were performed within each condition to check if mean score differences exist due to time differences. The results are summarized in Table 3.4, and we fail to reject the null hypo-study across all the groups, except in the mental innocent condition where p-value is less than 0.1. Thus, we can infer that time differences do not exist within each group except within the mental innocent treatment group. The significant result obtained in the mental innocent condition supports our previous argument that innocent participants should avoid learning mental techniques to prove their innocence, because of the great difference in scores in the wrong direction.

## Regression of Scores against Gender, Experiment Groups, and Test Effects

The analysis thus far suggests that the SCAN score is a function of experimental groups, gender, and the number of days after the crime that the test is given. This is represented by equation 2.

$$Score = Constant + Gender + Experimental\ Group + Time\ Effects \quad (2)$$

An ordinary least squares (OLS) regression analysis was performed to test the function with score as the regressand, and gender, experimental

**Table 3.4**
**Results of F-Test for Time Effects Within Groups**

| *Experimental Group* | *CG* | *CI* | *PG* | *P I* | *MG* | *MI* |
|---|---|---|---|---|---|---|
| F-statistic | 0.0045 | 0.1708 | 0.1562 | 0.8203 | 4.44416 | 0.3548 |
| df | (1, 22) | (1, 22) | (1, 22) | (1, 22) | (1, 22) | (1, 22) |
| Probability | 0.9471 | 0.6833 | 0.6965 | 0.3749 | 0.0467 | 0.5575 |
| CATEGORY statistics—Mean scores | | | | | | |
| One Day | –1.0833 | –2.8333 | –0.6666 | 0.0833 | –3.0000 | –1.6666 |
| Three Days | –0.9166 | –3.9166 | 0.3333 | –2.1666 | 2.5000 | –0.3333 |

CG = Control Guilty, CI = Control Innocent, PG = Physical Guilty, PI = Physical Innocent, MG = Mental Guilty, MI = Mental Innocent.

groups, and number of days testing took place after the crime as the regressors. Since all explanatory variables are binary, the regression model has seven dummies. For example, the independent variable CNTRL_INNOC is the dummy that takes the value of 1 for the control innocent participants and 0 for all other participants. The variables GENDER takes on a value of 1 for males and 0 for females. TIME measures the time consistency of SCAN and takes on a value of 1 when testing takes place one day after the crime and 0 if testing takes place three days after the crime. The base group for this regression is the group in the mental guilty condition, whose effects are captured by the intercept, C. Table 3.5 shows the results of the regression analysis where all coefficients are statistically insignificant at 10 percent significance level and R-squared is 0.0373. This means that the model has low explanatory power since the independent variables account for only 3.73 percent of the variation in scores. The F-statistic for the model is 0.7533 ($p > .1$), which implies that the regression is statistically insignificant.

Although the coefficients are statistically insignificant in this regression model, they do have a practical significance in explaining how scores are related to gender, experimental groups, and number of days testing took place after the crime. From Table 3.5, it can be seen that all guilty experimental groups have a negative partial effect on scores when all other variables are fixed, with the control guilty affecting scores greatest by reducing scores by 2.375.

The physical guilty condition negatively affects scores the least, by 0.0417.

Innocent experimental groups have a positive partial effect on scores with the exception of the control group. This is similar to earlier graphical analysis, in which SCAN does not detect innocent suspects efficiently in the control group. SCAN has a mild gender bias as well, because being male reduces scores by 0.639. This is congruent with earlier analysis in which guilty males are more likely to be detected by SCAN.

**Table 3.5**
**Regression Results of Score Against Gender, Experimental Groups and Time Effects**

| *Variable* | *Coefficient* | *Standard error* | *t-Statistic* | *Probability* |
|---|---|---|---|---|
| C | –0.291667 | 1.449017 | –0.201286 | 0.8408 |
| Gender | –0.638889 | 1.024610 | –0.623544 | 0.5340 |
| Control Innocent | –2.48E-16 | 1.774676 | –1.40E-16 | 1.0000 |
| Control Guilty | –2.375000 | 1.774676 | –1.338272 | 0.1830 |
| Physical Innocent | 0.833333 | 1.774676 | 0.469569 | 0.6394 |
| Physical Guilty | –0.041667 | 1.774676 | –0.023478 | 0.9813 |
| Mental Innocent | 0.750000 | 1.774676 | 0.422612 | 0.6732 |
| Time | –0.777778 | 1.024610 | –0.759097 | 0.4491 |
| R-squared | 0.037323 | Mean dependent variable | | –1.138889 |
| Adjusted R-squared | –0.012226 | S.D. dependent variable | | 6.110419 |
| S.E. of regression | 6.147659 | Akaike info criterion | | 6.523972 |
| Sum squared resid | 5139.944 | Schwarz criterion | | 6.688962 |
| Log likelihood | –461.7260 | F-statistic | | 0.753254 |
| Durbin-Watson stat | 1.843377 | Prob(F-statistic) | | 0.627366 |

Testing one day after the crime negatively affects scores by 0.778. *Ceteris paribus*, this shows that the scores for all suspects, regardless of their true state, will be lower. However, since the coefficient is statistically insignificant at 10 percent significance level, we conclude that SCAN does give a consistent result when tested across time.

## Discussion of Results

### *Accuracy of SCAN*

SCAN has a satisfactory accuracy rate of at least 12.5 percent across all treatment groups. It is most accurate in detecting deception in the control guilty group, with a 40 percent hit rate. Comparing between gender, SCAN is able to better detect male guilt in comparison with females in the control group. Gender-biased anti-detection strategies also emerge from our graphical analysis. Table 3.6 shows what techniques each gender should employ to maximize their payoff (i.e., being deemed innocent if they are innocent or being deemed innocent if they are guilty). Table 3.6 reveals a dichotomy in the strategies that each gender should employ. The dominant strategy for guilty females would be to employ mental techniques to avoid detection, while guilty males show no difference between physical or mental techniques. This is consistent with reality, as females have been found to be superior in cognitive processes; therefore they are more adept at deciphering patterns. Thus they will be better able to avoid detection by employing mental techniques.

The graphical analysis thus brings us to the following conclusions:

1. *Ceteris paribus*, mental techniques are superior to physical training in antidetection.
2. SCAN is effective in detecting guilt in the control groups.
3. Gender bias is present in SCAN because guilty males have a higher hit rate than females in the control groups.

### *Gender differences between groups*

The result of analyzing gender differences in mean scores strengthen the conclusion that SCAN is effective in detecting deception in the control groups. This is evident in the positive scores both genders obtain when in the control innocent group and the negative scores in the control guilty group. However, once participants receive training, SCAN becomes inefficient in detecting guilt because the scores are now skewed in the wrong direction.

Referring to Table 3.6, which depicts the various optimal strategies each gender should employ, the analysis of gender differences between groups lends support to the contention that guilty females should use mental techniques to evade detection while innocent females should use physical techniques. In Table 3.6, guilty males are indifferent between physical or mental techniques because the detection rates were the same. In this analysis, the dominant strategy for guilty males is distilled; they should choose mental techniques because the scores are positive compared to when physical techniques are used.

A significant result was obtained for females when an F-test was conducted to test for mean differences between groups within each gender. This shows that the different treatment conditions had an effect on females' mean score. This in turn, leads to the conclusion that learning antidetection training has an effect on females' SCAN scores but not on males' scores.

### *Time consistency of SCAN*

The argument that SCAN can accurately detect deception in the control group is further reinforced when time effects are analyzed between groups. This conclusion is evident in the higher negative scores that participants obtain in the control guilty group compared to the control innocent participants.

**Table 3.6**
**Antidetection Strategies that Maximize Each Gender's Payoffs**

| *Techniques* | *Physical* | *Mental* |
|---|---|---|
| Guilty Females | × | ✓ |
| Innocent Females | – | × |
| Guilty Males | – | – |
| Innocent Males | × | ✓ |

The fact that scores for the control innocent are negative corresponds to the analysis in section on the accuracy of SCAN, which concludes that SCAN is relatively inefficient in detecting innocence.

Graphically, time effects exist for both physical and mental treatment conditions. Most striking in the analysis is the fact that there is a great divergence in scores for the mental innocent condition in the wrong direction when testing is done one day after committing the crime. Thus, mental techniques affect the scores of innocent participants negatively. This analysis illuminates the earlier conclusion that any form of training improves an innocent participant's probability of being deemed innocent. The introduction of time effects changes the conclusions completely. Specifically, the innocent should avoid learning any form of training because their scores will be negatively affected and they will receive a wrong judgment call.

### *Regression analysis*

The coefficients obtained in the regression analysis strengthen the assertion that SCAN is most effective in detecting guilt in the control guilty group. It is relatively less efficient in determining innocence, a conclusion that was reached above and supported by the negative coefficient in the regression model. The gender bias toward males is also substantiated by the regression analysis, where males are more likely to have negative scores. SCAN gives time consistent results because the coefficient of TIME is insignificant.

## Contradictions between Graphical and Statistical Analysis

One recurring feature of the analysis is the contradiction between graphical and statistical analysis. The graphical analysis indicates differences between groups but these observed differences are mostly not supported by statistical testing. One possible reason for this discrepancy would be the small sample size of 12 in each condition. With a sample size of less than 30, the population does not follow a normal distribution and hence nonsignificant results are observed.

There is also a restriction in the range of scores observed, as most of the participants are classified as leaning toward being problematic. Therefore, insignificant results are obtained because the differences between scores are too small. However, these slight differences are magnified in a graphical analysis, which allows us to detect trends between groups.

## Implications of Results

Clearly, the results show that SCAN is accurate in detecting deception in the control group. This result holds even after accounting for gender and time effects. However, SCAN is relatively inefficient in detecting innocent

suspects as innocent. This does not jeopardize the use of SCAN as a forensic assessment tool because in reality, suspects are evaluated using various tools and innocent suspects will be cleared in subsequent testing. Therefore, SCAN is still very useful as a screening tool in the early stages of investigation to assess guilt. Most importantly, it is easier and more convenient to administer than polygraph testing. This is especially so when a criminal case involves a large number of suspects and an easy and effective screening tool is needed.

With the advent of Internet technology, information can be shared freely across national borders at any time. This means that criminals are now more informed on the forensic assessment tools that they might face if they are brought in for investigation. Thus, they can now prepare themselves to increase their probability of being detected as innocent during assessment. Since the most commonly known tool is the polygraph machine and antipolygraph techniques are easily available online, criminals can be rationally expected to acquire this knowledge and lower their probability of being apprehended.

Although the techniques learnt are not designed specifically to pass a SCAN test, the results show that these mental or physical forms of training do have an effect on SCAN results. Explicitly, we observe the dominant strategies that emerge for each gender to maximize their payoff to crime after controlling for the true state of the suspect, gender effects, and time effects. In particular, we note that innocent suspects should avoid learning any form of techniques to ensure that they will be correctly assessed, because the training backfires and will make them look guilty instead.

Gender bias is present in SCAN testing, as guilty males have a higher probability of detection compared to females. Although this seems to reduce the validity of SCAN as an assessment tool, we have to bear in mind that the gender differences observed may not stem from flaws in SCAN. Specifically, the gender bias in SCAN may be a result of fundamental differences in each gender's cognitive workings. As mentioned earlier, females are better at detecting patterns, and hence they are able to escape from detection because they can predict the questions and answer accordingly.

A significant result from the analysis was that the accuracy rate of SCAN declines once participants have learnt antipolygraph techniques. This implies that once suspects have received antideception training, SCAN will not be able to detect their true state accurately. Since criminals are rationally expected to train themselves, criminal investigations in the real world call for a "multiple hurdles" approach to assessing a suspect. This implies that SCAN should be used as one of many assessment tools to gauge a suspect's true condition.

## Future Research Possibilities

The results of SCAN are based on analyzing the difference in linguistic structure between a guilty and an innocent suspect. This suggests that an incorrect conclusion may be reached due to differences in the suspect's educational background or geographical difference in language. In this experiment,

the assessment criteria have been modified to suit the local language structure. In future research, it would be intriguing to employ SCAN in languages other than English and observe its validity in assessment.

The overall nonsignificant F-statistic obtained and the low R-squared from the regression model suggest that the choice of explanatory variables may be incorrect. In later research, other variables such as a person's number of years of education, family background, or intelligence quotient (IQ) scores may be tested to see if they affect the mean scores in SCAN testing.

Gender bias can also be examined across the different forms of forensic assessment techniques in future research. If gender bias is present in other forensic tools as well, then an alternative form of assessment has to be invented or an existing form modified for females so that they can be accurately detected.

Finally, if SCAN is to be part of a multitude of assessment tools used to assess deception, it is worth researching what would be the optimal basket of forensic tests that SCAN should be used with. This is because deception can be expressed in varied forms, and different forensic tools measure the concept on diverse scales. Determining the optimal number and type of tools that appraise guilt differently will lower enforcement costs without compromising the probability of detection. This will provide insights into the multifaceted façade of deception and the ways in which people express it.

## CONCLUSION

The economic framework in the analysis of deception or crime assesses an effective level of deterrence that can be achieved by adjusting the probability of detection or the severity of punishment. Economic analysis prescribes that efficiency should be achieved at the lowest possible cost. In the context of law enforcement, this would mean higher fines and lowered probability of detection. However, higher fines would mean additional risks undertaken by risk averse individuals. As a result, they will be "over-deterred" and the equilibrium level of crime will be below the optimal amount. Therefore, it would be best to seek a solution in which probability of detection can be increased in other ways besides hiring more law enforcers. This study identifies SCAN as a possible remedy and seeks to test if it is reliable and efficient in increasing the probability of detection.

Results from the experimental framework indicate that although SCAN is useful in detecting deception, it is still far from ideal. This is because it can correctly assess guilt in the control groups but this accuracy rate declines once participants have been trained in antideception. Thus, it is best to employ a broader bundle of assessment tools to increase the probability of detection.

Besides being able to accurately detect guilt, a reliable assessment tool should be able to determine innocence as well. The findings show that innocent suspects should refrain from learning antideception techniques, to ensure that they will be judged correctly. This is because such training will make them appear guilty. This is important because it means that the probability of detection

in innocent suspects who have undergone training is lowered. Assuming that the severity of punishment is kept constant, innocent suspects will now have a greater incentive to commit crime because their expected cost is lowered.

Since the results show that SCAN is not superior to other assessment techniques in detecting deception, it would be best employed together with other techniques such as polygraph testing and verbal/behavioral analysis to increase the probability of detection. This will ensure that the probability of detection will be higher across both guilty and innocent suspects. Consequently, an optimal level of deterrence will be achieved through higher probabilities of detection and lowered penalties.

Through the experiments, this study has illustrated that the probability of detection can be increased without great addition to cost in terms of hiring more law enforcers, especially for white collar crime. Given this insight, the equilibrium level of crime can now be achieved through lower costs with a higher probability of detection rather than through harsher punishments. This lowers the risk premium of risk averse individuals, resulting in an optimal level of crime.

## NOTES

1. Gary S. Becker, "Crime and Punishment: An Economic Approach," *Journal of Political Economy* 76, no. 2 (1968): 169–217.

2. Cesare Lombroso, *L'Uomo delinquente: The Criminal Man* (Milan: Hoepli, 1876).

3. Robert Cooter and Thomas Ulen, *Law and Economics* (Glenview, IL: Scott, Foresman and Company, 1988).

4. Erling Eide, *Economics of Crime: Deterrence and the Rational Offender* (Amsterdam: North Holland, 1994).

5. Cooter and Ulen, *Law and Economics*.

6. Eide, *Economics of Crime: Deterrence and the Rational Offender*.

7. These costs include self-protection costs incurred in order to avoid detection.

8. This is because crime ($q_c$) is a function of $\pi c$ and the second derivative is greater than or equal to zero. Mathematically, $q_c = S(\pi_c)$ and $S'(\pi_c) \geq 0$.

9. Protection from crime may range from buying insurance, locks, and burglar alarm systems to paying higher rents to live in a safer neighborhood and hiring bodyguards. See Issaac Ehrlich and Gary Becker, "Market Insurance, Self Insurance, and Self Protection," *Journal of Political Economy* 80, no. 4 (1972): 386–402.

10. Norms are defined as specific rules for behavior in particular situations. See Craig Calhoun, Donald Light, and Suzanne Keller, *Sociology* (New York: McGraw-Hill, 1997). These rules are imposed by society, and deviation from these socially accepted behaviors may result in society's rejection or disapproval.

11. Eide, *Economics of Crime: Deterrence and the Rational Offender*.

12. Personal restraints include reasons of conscience after violating norms and consideration for the injured party. They exclude physical inability to commit crime.

13. See the appendix to this chapter.

14. Avinoam Sapir, *The View Guidebook: Verbal Inquiry—The Effective Witness* (Phoenix, AZ: Laboratory of Scientific Interrogation, 1995).

15. For example, pronouns like "I," "you," "he," and "she" indicate partnership. Pronouns like "we," "you," "they," "my," "your," "his," "her," and "our" indicate possession.

16. A negative outcome is one in which the suspect is determined to be innocent. Thus, guilty suspects will strive to achieve a false negative judgment.

17. These three treatment conditions would be control guilty, physical guilty, and mental guilty.

18. Participants were given the security plan of an airport and briefed on it.

19. These treatment groups would be control innocent, physical innocent, and mental innocent.

20. At the time of the experiment US$1 = SGD1.70.

21. See Sapir, *The View Guidebook*, for a detailed description of the VIEW questionnaire. When this questionnaire is used to obtain information, it is employed for the purposes of identifying the truth, rather than identifying instances of deception.

# APPENDIX

# VIEW Questionnaire

1. How do you feel now that you have completed this form?
2. Should we believe your answers to the questions?
3. If your answer to the last question was yes, give us one reason why.
4. What would you say if it was later determined that you lied on this form?
5. While filling out this form what were your emotions?
6. Were you afraid while completing this form?
7. Did you ever discuss the possibility and reasons for this investigation with anyone? If yes, with whom?
8. If you are asked to compensate for the missing money, how much are you willing to pay?

# CHAPTER 4

# Emotive Profiling

*Terry A. Sheridan*

Airline passenger profiling in the past has been based on behavioral observation (for example, excessive sweating or rapid breathing), or purely on the race of known terrorists.[1] Well-known signs of short-term acute stress have been used app ropriately to pick up passengers showing distress. And, in today's context of terrorism, any Middle Eastern Muslims are regarded with suspicion. However, in many cases they prove to be false positives, and much time and effort is wasted in this regard.[2]

Most passengers are fairly accepting of the methods used, but there have been accusations that profiling, as it is implemented today, is racially oriented, which leads to confrontation on very shaky grounds.[3] This chapter contends that looking for acute stress symptoms may not reveal potential suicide bombers. Neither will racial profiling, as the terrorist strategists will respond with the use of different and unexpected racial types for their horrific task.

Not all suicide bombers who want to die for their cause would show stress, as the desire to be a martyr would override their fear of imminent death.[4] Hostages who saw suicidal terrorists at first hand in the Chechen rebels' seizure of a Moscow theater in 2002 were quoted as saying, "They were calm about it. Death was not something that they were afraid of."[5] Suicidal terrorists would have been practicing, imagining the moment of their death and immediate salvation, hundreds if not thousands of times. Also the physicians attending the hostages in the Moscow theater reportedly noted that most of the terrorists were euphoric and some were in a trance-like state. None were showing signs of depression, hopelessness, or despair—states of mind traditionally associated with impending suicide.[6] Nevertheless, the potential suicide bombers would have shown signs of deep long-term stress, noticeable

to the informed outsider. Death is what martyrs want above all else, however bizarre and contrary it is to our thinking. Most people want to live a normal lifespan. And some cohorts in society, like teenage males, feel invincible and think they will live forever. In our society, it is not normal to think constantly about your own death, or to take actions to induce your death, as most Western people fear dying and take few risks that might lead to an early death. Many give up smoking to avoid an early death.

## LIVING WITH THE NOTION OF DEATH

Let me share with you a personal event, so that you may understand the death wish more. I am an adoptee, and for years I suffered from long-term stress brought about by being separated from my mother as a baby. Recent research is demonstrating that such separation is traumatizing for the infant, and I lived under this cloud for nearly five decades.[7] The infant conceptualizes upon birth that it is still part of the mother, and when the mother disappears, usually forever for an orphan or adoptee, the infant feels the death of a part of him- or herself. This is a real death to the infant, but the problem is that the infant continues to live. Therefore he or she has to accommodate to a perpetual dying in "normal" life.[8]

The way I processed this notion of continually dying was to experience the event in dreams or in daytime fears. For most of my adult life I would think about dying before I went to sleep. I would experience the moment of death over and over in my mind. I would imagine what it would feel like—the possible pain and the release when my soul left my dead body. Repeatedly, I have gone through the final moments of my life. So, in some sense, I have felt what the suicide bomber goes through in coming to terms with his or her final action. However, in my case, it would be resolved through dealing with my feelings about my first "death," in the form of my mother leaving me.

For the suicide bomber, it is only resolved through the completion of their last act on this earth to overcome evil and enshrine themselves as martyrs to the cause. I feel sure that imagining death before the event is an experience also shared by prisoners on death row, as well as people who contemplate suicide for a long time. There has been some research on suicidal individuals who have survived, who have talked about seeking relief through death, as they see it as their only solution to the crisis at hand.[9] However, I went through this for a much longer time than most others. And for me, it wasn't a matter of release. Like the death row prisoners, I knew that it would happen sooner or later, that it would hurt and be painful, that I would have to put up with it, and that my soul would live on in an eternal abyss.

As I was brought up as a Catholic, a sense of "soul" was instilled in me. I have often wondered if people without a religious belief in a soul would have the same death experience, as all death would be for them merely an end to sensation. However, suicide bombers, as they present themselves today, also believe in the concept of a soul, and this feeling of release would be in their

minds too. To me, death was a pathway into darkness, but death to a martyr is a pathway to eternal bliss. So how can security pick out passengers who are actually happy as they are about to die for their cause, and therefore typically do not show signs of acute stress? No one ever picked me out from a passenger line, yet I travel frequently on aircraft. I am not a terrorist, but I knew what it would be like if the airplane crashed, or if it were bombed, or just fell out of the sky, as I lived those moments over and over again. I did not suffer from sweaty hands or go weak at the knees, but I knew in every intimate detail what death of this type would be like.

The Chechen women terrorists, who had bombs strapped on them, were very calm about it; they just sat there waiting for death. So how would an airport security officer pick me out if I were a terrorist? They would not. I look too ordinary, despite my alliance with death. Clearly, different approaches are needed and have been called for by others.[10] The answer that came to me in my research effort was another, entirely different approach, called emotive profiling.

Emotive profiling is based on an emerging theory of emotional energy, which has been developing in a variety of fields over the last 17 years.[11] Recently it has reached a wider audience and acceptance through the concept of emotional intelligence.[12] This concept is now taught in management schools in many countries, essentially using awareness of emotions as a management tool. I have developed this concept further to assist with screening in recruitment, as well as helping hundreds of candidates understand their behavior and create pathways for change.

Having a very different background than most airline security investigators, being a career-development specialist for managers and executives, I have faced the problem of screening, but in a totally different environment. My problem is how to sort out the good managers from the bad. Which ones pose the risk? They all look fine at interview, yet some will wreak havoc in their new positions. Similarly, airline passengers have to be screened, and the same question has to be asked: which ones pose a risk? For airline security personnel, it is about saving an aircraft and its passengers; for me it is about saving companies and their personnel (and their emotional fallout) from potential fraudsters and corporate psychopaths. I found that normal screening wasn't adequate to assess these risky candidates. No matter how confident they were at interview, my intuition told me to be wary, but it was unfair to deny them opportunities purely on a gut feeling. This led me to initiate an investigation of existing screening techniques.

Modern, advanced techniques of psychometric testing and behavioral-based interviewing have not made any impact on executive fraud. When I talked to experienced recruiters about this problem, they informed me that this is due to the age-old problem of "impression management." That is, people like to make a good impression on others, and sometimes they will exaggerate claims in order to do so. It is virtually certain that potential fraudsters will do this, covering up their deceitful and harmful purposes. Similarly, terrorists seeking

to board an aircraft will use impression management so that they behave and look like ordinary passengers to airline security. Furthermore, they will likely not show signs of acute stress at being about to blow themselves up, as ordinary people would.

## EMOTIONAL ENERGY MODEL

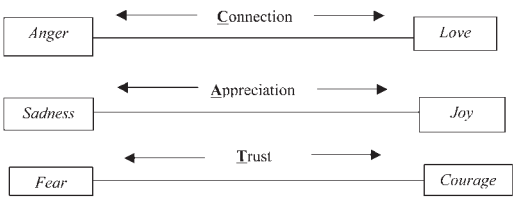
It struck me from the psychological literature that as emotions rule our thoughts and behaviors, this just might be the means by which potentially damaging behavior may be uncovered. After considerable investigation and research with various groups and individuals, I constructed a model representing emotional energy. There are three dimensions to this energy (see Figure 4.1).

The first dimension is all about connection. Connection refers to all the emotions that one feels connecting to another in a relationship, whether it is a casual, single meeting or a fullblown, lifelong relationship. The positive emotion that is experienced in this dimension is love or respect; the negative emotion at the other end of the spectrum is anger.

Initially, this may be a little puzzling, with two diverse emotions of love and anger. In what way could anger be in the same dimension of connection as love? Consider the example of two warring individuals engaged in contentious litigation following some bad behavior on one side or the other. If you walked up to them on the steps of the court and told them that they each have the same amount of connection as the day they released the great news of their initial partnership, the two parties would give vehement responses to the contrary. They would express in simple terms that they hated each other. However, if there is no connection, there is no emotion. The hostile parties are very much connected, but the connection is strongly negative, hence the legal battle. Connection is the fundamental emotion in any human relationship. It ranges from loving to liking, to thinking they are okay, to finding them irritating, and to finally hating them.

Hatred is the overt expression of extreme negative human connection. Terrorist-martyrs believe they are dying for love of their religion, political party, or nation, because they have hatred in their hearts for the dominating faction. These people are just as connected to you and me as we are to ourselves, but the connection is in a highly negative form. The fact of the matter

**Figure 4.1**
**CAT Model**



is that connection is a very strong emotion that will drive them to conceive and implement many actions that will connect them with the "other side—and the more it hurts the better. Westerners and nonextremists will likely retaliate, because the provocateurs have inflicted great pain. The strike back usually results in many lives lost (on both sides), to "teach them a lesson." This strike–counter strike *danse macabre* proves the power of connection. This negative form of emotional energy is so powerful that it drives wars and large-scale threats to society.

The second dimension is that of appreciation. On one side there is the positive emotion of joy; on the other side is sadness. Again, there is a whole range of feelings between being appreciated and not being valued by others. Joy is the expression of the positive side of being appreciated, and sadness is all about loss. Sadness brings about terrible emotions of feeling subjugated, not having what others have, envy, greed, and miserliness, and it also fuels depression in people over time.

The third dimension is that of trust. At the positive end of the continuum there is the emotion of courage or confidence; at the negative end lies fear. As we all know, fear is the basis of phobias and anxiety states. Insecure people commit troublesome acts as they have low self-esteem and in reality, low confidence in their abilities. What they have learned to do for years is to bury these inner feelings completely, even to themselves.

Once the emotional model (which is referred to as the CAT model, short for connection, appreciation, and trust model) is understood, it is clear that people can be fairly easily measured on the three dimensions. For instance, if people are feeling very upset and angry, they will be at the low, or negative end, of their emotional energy in that dimension, maybe at around 10 percent. If they are just feeling mildly irritated with life, perhaps the measure would be more like 40 percent. If they are feeling "on top of the world" and gain valid respect from those around them, then the measure may be 80 percent or even 90 percent. People can easily find words that describe their feelings and they can place themselves on the scale without too much trouble.

Now, so far so good, but what about the potential martyrs who are reading this, too? Regardless of their knowledge base, they will want to represent themselves as being in the 70–85 percent range, to impress security as they line up at the X-ray machines and passport control. In reality, they are feeling about 5 percent or lower, and are just waiting for the moment to achieve the disaster/holy release that they have been dreaming of. And this is the nub of their problem; they cannot hide their emotional energy from people. It's just that those around them don't understand the small emotional signs underpinning the terrorists' highly destructive negative behavior.

One of the rules of recruitment is that "like seeks like," and the negative energy–based terrorist will surround him- or herself with other negative energy individuals. A negative energy mastermind will choose fearful incompetents, who make you look good but are prone to make mistakes, so they are given basic tasks or will be blackmailed or brainwashed into actions they

would not ordinarily perform. Not many people will go against their desire to live; they have to be in an extremely negative state of emotion to allow the ending of their life. The masterminds choose their candidates very well: the sad and the fearful and those who hate society.[13]

Notice that the perpetrator does not get on the plane him- or herself; it is always others who commit these acts. Moreover, the martyr candidates are not necessarily illiterate peasants. Recently the West was shocked to learn that professional doctors blew themselves up in a terrorist attempt on Glasgow Airport.[14] The emotional energy or CAT model predicts that any people—no matter who they are, whatever their class, education, or bank balance—can perform such destructive acts if they are in a state of sufficient negative energy. Therefore, detecting abnormal emotional energy levels is vital and possibly more important than focusing on racial characteristics and acute stress symptoms. Not all terrorists will have dark skin and look devious. The masterminds will choose other candidates, with different skin color, race, and socioeconomic background, to throw the behavioralist-trained security staff off the scent.

Negative energy passengers will include nonterrorrists. It requires a skillful interrogation to weed out the final group of terrorist suspects from among the negative energy passengers (see Figure 4.2).

## INTERRELATION OF THE EMOTIONAL ENERGY DIMENSIONS

One of the characteristics of the emotional energy dimensions is that they work in conjunction with each other. If Person A is feeling high self-esteem (this excludes narcissism and egocentric behavior), he or she will generally have a good outlook on life (which will be measured as courage, say, 80 percent), value the job and family (joy, 80 percent), and have self-respect (love, 80 percent). In other words, the score on connection will be roughly the same as for the dimensions of appreciation and trust on the CAT model. Figure 4.3 shows what the 80 person for Person A would look like on the model.

Similarly, when Person B is in negative energy, he will record a low score on the connection dimension if he is admitting to much frustration in his life

**Figure 4.2**
**The Energy Look**

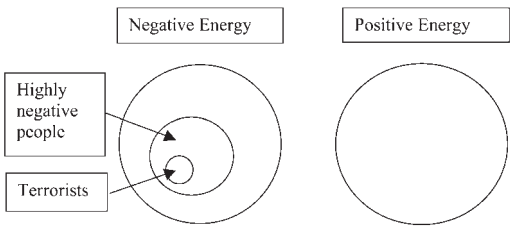
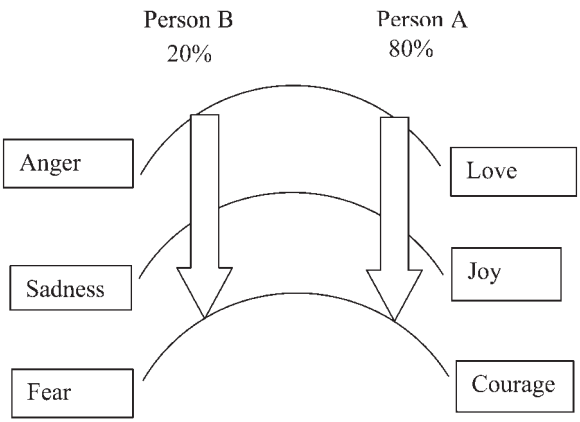


**Figure 4.3**
**The 80/20 Rule**




(anger measured at perhaps 20 percent). It would also be expected that he is feeling fairly low (sadness, 20 percent) and anxious (fear, 20 percent) as well.

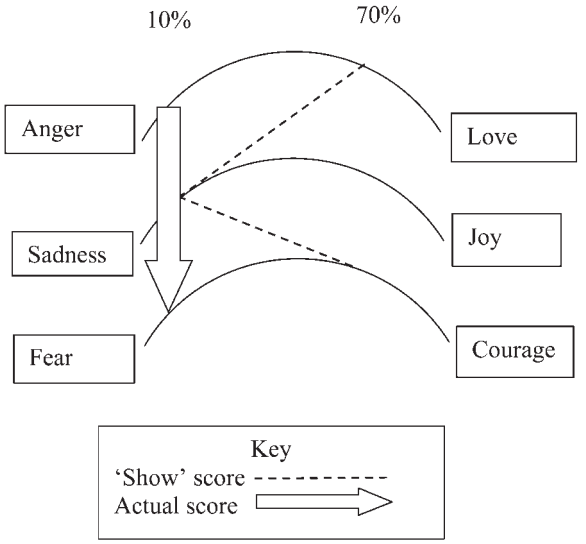
What about people who have contradictory scores? Here a rather facetious example will be used: a passenger with expensive luggage demonstrates that she has self-respect (say, 70 percent), and she is showing nonchalance, perhaps even a smile as she lines up to board a plane (courage, 70 percent), but she smells badly from several days' accumulation of body odor (indicating a severe lack of self-worth, say, 10 percent). This should be investigated as it is incongruous on the emotional energy model. There are no incongruities in the CAT model. The truth is that the woman is operating at the lowest denominator of 10 percent; the rest is show or impression management, as the bad odor would not be tolerated by any self-respecting person in the 70 percent range. With this clue, security personnel would interview the woman and ask her questions about where she has been to get such a body odor (ruling out cultural nuances regarding differences in body odor, or the possibility that the odor came about, for example, due to delays caused by canceled flights.

Innocuous tests could easily be carried out to check the traveler's ability to smell, for instance, acknowledging and getting the traveler to talk about the duty-free fragrance in her bag (ruling out a physical cause). If no satisfactory explanation (e.g., delays are confirmed, olfactory malfunction is present, or there is verification by passport that she is from a culture that tolerates body odor) is found, further, serious questioning should take place. Figure 4.4 demonstrates the appearance of the inconsistent scores if represented on the CAT model.

## EMOTIONS DETERMINE BEHAVIOR

The CAT model demonstrates the dimensions of the range of emotions. We do know that emotions determine our behavior, even such a simple

**Figure 4.4**
**The 70/10 Rule**



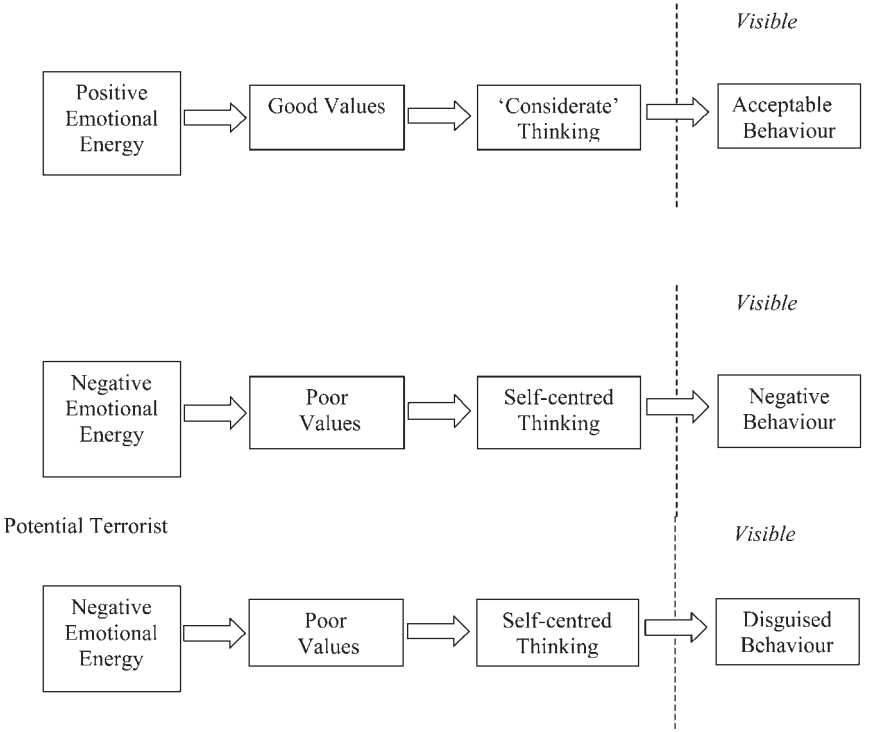

emotion as embarrassment.[15] Taking the CAT model as the foundation, it can be seen that that emotional energy determines emotions and the depth of what is felt, which determine thoughts, which in turn determine behavior. If assumptions are made about behavior, that is, about the underlying emotional base, then misleading conclusions are drawn. There is a masking or a deliberate attempt to disguise the feelings underneath, where there is negative emotional energy. Positive energy is never disguised or withheld; only negative emotional energy is camouflaged to deceive (see Figure 4.5).

The terrorist will mask her own negative behavior as much as she can, in order to act within culturally allowable limits of acceptable behavior, but she cannot do it on all dimensions all the time.

## EMOTIONAL ENERGY AND STRESS

The theory of emotional energy is linked with stress. The more stress in a person's life, the more likely that the emotional energy will be negative. It is assumed that babies are born on the positive side of the equation, confident of their mother's love and nurturing, which develops their self-esteem and self-worth. But babies grow up and eventually go to school, college, and work; then they get married and have their own kids. Each step along the life cycle creates stress to some degree in an individual, and it is this stress that pushes the person into negative emotional energy. The bigger the stress, the more quickly and deeply the individual's emotional energy becomes negative.

**Figure 4.5**
**Value Chains**




Some individuals get pushed more quickly than others, due to life's lottery, for example, being born to a depressed mother who is unable to care emotionally for her child, a bullying episode at school, marrying the wrong person, the death of a beloved partner, and other reasons. However, for many, there is a process of adjustment and acceptance of what has happened, thus relieving the impact of the stress (without the person concerned or others being harmed) and permitting a return to the positive side of the model.

For the ones who experience setbacks in life at a very early age, it is very likely that they will be more stressed and will exhibit negative behavior for a longer time than a resilient adult. It has long been observed that orphans growing up in orphanages and refugee children exhibit different, sometimes bizarre behavior.[16]

Traumatic events occur inside and outside the family unit, and may be caused by societal or environmental events, but most commonly they are caused by car accidents, fires, abductions, poor sanitation and disease control, and war.

Finally there are natural disasters—earthquakes, cyclones, and hurricanes, tsunamis, electrical storms, tornadoes, and others. Being in the wrong place at the wrong time has an enormous impact on many people's lives. Events that can cause negative energy are listed in Table 4.1.

**Table 4.1**
**Categories of Traumatic Attachment Levels and Examples of Events**

| *Category of attachment level* | *Examples of events* |
|---|---|
| Maternal Attachment: loss of, or disorder. | Orphans, those not living with their families, adoptees, children with mothers who were "emotionally absent" through disease, disability, or mental illness, particularly in the first 2 years of life. |
| Familial attachment—fathers, siblings, close relatives, close friends of family that take on parenting roles. | Fatherless children, absence of major family figures, parents and siblings who have died or become severely affected through disease, etc. Sibling rivalry. Abuse by family figures, or friends of the family, or step-parents, etc. |
| Secondary attachment—school, work, university, college, hobby groups, church. | Bullying, violence, tyrannical behavior by supervisors, bosses, alienation, apathy. |
| Community attachment—income maintenance systems, education, penal systems, religion, public sanitation and disease control. | Low-level or nonexistent social involvement, which causes a class of people to live in disease and permanent poverty. |
| Social attachment—disasters caused by humans. | War, drug trade, terrorism, car accidents, industrial accidents, etc. |
| Random events—no attachment, disasters caused by nature. | Earthquakes, tornadoes, tsunamis, cyclones and hurricanes, landslides, floods, and fires. |

It is suspected that those who endure random natural disasters wars and come through relatively unscathed have had a good attachment or bonding with their mother, but there has been little research in this area, most of it from studies of animal behavior.[17] The security of initial attachment enables the individual to face each event with a degree of strength. It is as if there is an understanding, a basic optimism, in the individual, who is confident that somehow she or he will survive.[18] Optimism is an inner belief built into the child that he or she has a right to live fairly and decently and to be respected. Those who have not had that luxury grow up to believe that bad things will continually happen to them (pessimism), events that are equal to or worse than the event that originally caused their pessimism. Adults that have been caught up in terrible situations for the first time in their lives have a resilience, but those affected earlier, children and babies, have far less resilience and are likely to develop problematic behaviors.[19]

War zones result in stressed-out dysfunctional families and societies that are, in turn, breeding grounds for negative energy.[20] Furthermore, children grow up ignorant of the positive ends of the dimensions and without experiencing real love, real joy, and real confidence. The paradox is that they probably

think that they do experience happiness, but when a further in-depth look is taken, the reality will be seen in unhappy, dysfunctional relationships, fear, depression, and feelings of inadequacy and insecurity. Early childhood stress sets a person on a negative pathway for years. And there lies another problem: the person may be blind to his own behavior, as the negativity has been an ongoing theme throughout life and is perceived as normal, cloaked by an outer layer of impression management. The length of time for which a person experiences problems is always a clue to that person's emotional energy level. The more ingrained the negativity is, the more self-destructive it will be.

## "BLINDNESS"

It has been found that apart from conscious behavior, the individual is blind to underlying negative behavior, sometimes referred to as our shadow self.[21] Blind behavior is similar to habits that we all have and don't realize that we have, such as scratching ourselves or picking our teeth. It takes an outsider to tell us at times when we are doing these things, as we are unaware of them. Similarly, there may be emotional indicators below the conscious radar.

Table 4.2 provides a list of some of the behaviors indicating negativity, many of which will be exhibited unconsciously by negative energy individuals. The Chechen rebels in the Moscow theater, as described by Speckhard and associates, recounted their emotions, and one to which the terrorists themselves would have been blind was a degree of laziness, particularly in the latter part of the siege.[22] No earnest martyrs would want it to be known that they were lazy! Yet laziness is a strong negative emotion that is found on the connection dimension—see Table 4.2—and people trained in emotive profiling could expect this to appear, despite the terrorists' unawareness.

Because one negative condition indicates that a person will show the same degree of negativity on the other emotional dimensions, similar negativity will be exhibited in the negative sets of anger, fear, or sadness. Questioning in the other dimensions will bring the other negative areas to light in an intensive interview. The answers have to be immediately tested, to avoid unwarranted detention.

It is my contention that "blindness" creates terrorism and other extreme social behavior. Damage early in childhood creates the parameters for later life. The more negative the emotional energy is, the more self-harm occurs. This self-destruction can be long-term, as in alcoholism or drug dependency, or it can be short-term, as in suicide. In addition, self-destructive people always exhibit a notable lack of concern about the effects of their self-harm on others. When corporate psychopaths and fraudsters are looked at in some depth, they share a similar lack of empathy.[23] They also share the same inflated sense of self (narcissism)—which derives from the negative side of the CAT model.

The brains behind airplane sabotage are usually extremely narcissistic and strategically cunning, pushed on by their success with their own groups.[24] These leaders are perceived as demonstrating their power and strategic ability

**Table 4.2**
**Negative Emotions Generate Negative Behaviors**

| *Dimension* | *Negative emotion* | *Negative behaviors* |
|---|---|---|
| Connection | *Anger* | Lying, cheating, overt aggression, passive aggression, showing no respect for others, killing, harassing, domineering. Self abuse and harm. Suicide talk or actual attempts. Short fuse. Hatred, despising others and/or self. Racism. Criticism. Putting down others. Being hateful, spiteful, or malicious. Getting back at others. Revenge. Holding secrets. Laziness. Physical, sexual, and emotional abuse. Sabotaging behavior. Gossip. |
| Appreciation | *Sadness* | Depression. Tiredness. narcissism, kleptomania, envy, greed, stealing, "keeping up with the Joneses," consumption beyond income, status symbols, traveling as a "been there, done that" exercise. Excessive collection of artifacts, excessive hoarding. Home is cluttered, untidy. Maximizing profits to excess, at other people's expense. Miserliness. Lack of generosity. Jealousy. Taking credit where one does not deserve it. Nit-picking, taunting, teasing. Withholding love and kindness. Isolating others. Being excessively untidy, dirty, smelly, having an unkempt appearance. Arrogance. |
| Trust | *Fear* | Difficulties in relating directly to people. Isolating oneself from normal social activities. No close adult partner for a few years. No one to confide to. Excessive worry or anxiety. Phobias—anxiety fixated on certain things or conditions, e.g., agoraphobia. Free-floating anxiety—worrying about anything or anyone. Predicting doom and gloom—the world is coming to an end. Pessimism. Insecurity. Uncertain future, can't decide. Procrastination. Being in a rut, never moving out of it. Excessively codependent relationships. Double checking oneself. Constant reminders of previous failures. Overcontrolling. Overprotective. Micromanaging, excessive supervision. Bullying others. |

to push their agenda, and many have inflated egos as well. Ordinary members of the groups are attracted to or put up with negative emotional energy, as they rally around the cause that the mastermind has skilfully articulated as the objective. Followers become spellbound or are coerced to bear extreme negativity in order for the oppressed group to benefit from the organizer's strategies.[25] Similarly, if the terrorists are operating in a group, there will be a leader who will exhibit negative emotional energy in dealing with his subordinates, and if dealing with a group of suspects at an airport, it would be wise to watch for negative behavior by the group leader.

Quite frequently, the investigator may be the only one who is suspicious of a passenger, a lonely voice crying in the wilderness. Tapping into the suspect's emotional energy will increase the confidence of the examiner, as it will give an understanding of the suspect's capability for terrorism and reinforce the examiner's intuition regarding the intended wrongdoing. Sometimes investigators give up the trail as it becomes politically unwise to continue (for example, taking a Muslim clergyman into questioning), and therefore emotional energy assessments of travelers will provide a far better assessment of potential harm than a gut feeling. Every terrorist sabotage attempt can be discovered before the event; it is purely a matter of resources.

Emotional energy assessments should be used as an additional layer added to existing protocols for passenger traffic, not on their own. The other proviso is that the facts need to be tested before a final judgment is made to allow a person onto a plane. Perhaps only one lie needs to be revealed, and it must not be ignored. Even if it is a tiny detail, it could well be the crack in the mask that warrants further investigation.

The other use for emotive profiling is for screening airport personnel themselves. Terrorists are increasingly infiltrating airlines and baggage handling and catering companies, in order to get past the passenger security line. It is imperative that emotional energy assessments should be made at all personnel levels, just as executives are screened to guard against fraud and other negative and destructive behavior in companies.

While only an outline of emotive profiling has been provided in this chapter, more detailed and intensive work has been undertaken that would prove useful for the security front line at airports as well as for other uses. Emotional energy is a new tool, which, with correct training, can be very useful in screening passengers with harmful objectives. It takes us far beyond watching for certain racial characteristics or acute stress symptoms in passenger lineups, instead concentrating on observations of emotional functioning, which in many ways is far more revealing of a passenger's true intentions.

## NOTES

1. Peter Robinson, *Israeli Style Air Security, Costly, and Intrusive, May Head West*, 2006, http://www.bloomberg.com/apps/news?pid=20601109&sid=aFyfihM1e3G4&refer=news; John Horgan, *Why We'll Never Construct a Single Profile for Terrorists*, November 2007, news.scotsman.com.

2. Pat O'Malley, "Risks, Ethics and Airport Security," *Canadian Journal of Criminology and Criminal Justice* 48, no. 3 (2006).

3. Ihekwoaba D Onwudiwe, "Defining Terrorism, Racial Profiling and the Demonisation of Arabs and Muslims in the USA," *Community Safety Journal* 4, no. 2 (2005).

4. Anne Speckhard et al., "Research Note: Observations of Suicidal Terrorists in Action," *Terrorism and Political Violence* 16, no. 2 (2004).

5. Ibid., 319.

6. Anthony Spirito and Christianne Esposito-Smythers, "Attempted and Completed Suicide in Adolescence," *Annual Review of Clinical Psychology* 2 (2006).

7. Cynthia M. Kuhn and Saul M. Schanberg, "Responses to Maternal Separation: Mechanisms and Mediators," *International Journal of Developmental Neuroscience* 16, nos. 3–4 (1998).

8. Norma Tracey, "From Oblivion to Being: Faith and Catastrophe," *Psychoanalytic Review* 94, no. 2 (2007).

9. Spirito and Esposito-Smythers, "Attempted and Completed Suicide in Adolescence."

10. Michael P. Arena and Bruce A. Arrigo, "Social Psychology, Terrorism, and Identity: A Preliminary Re-Examination of Theory, Culture, Self, and Society," *Behavioural Sciences and the Law* 23, no. 4 (2005).

11. William A. Kahn, "Psychological Conditions of Personal Engagement and Disengagement at Work," *Academy of Management Journal* 33, no. 4 (1990); Michael Schwalbe, "Emile Durkheim and Erving Goffman Meet Dr. Magneto," *Contemporary Sociology* 36, no. 3 (2007); Peter A C Smith and Meenakshi Sharma, "Rationalizing the Promotion of Non-Rational Behaviors in Organizations," *The Learning Organisation* 9, no. 5 (2002); Philip Vassallo, "Turning Emotional Energy into Purposeful Writing," *et Cetera* 61, no. 1 (2004).

12. Reuven Bar-On and James D A Parker, eds., *The Handbook of Emotional Intelligence: Theory, Development, Assessment, and Application at Home, School and in the Workplace* (San Francisco: Jossey-Bass, 2000); Daniel Goleman, *Emotional Intelligence: Why It Can Matter More Than IQ* (New York: Bantam Books, 1995).

13. Laurence Miller, "The Terrorist Mind," *International Journal of Offender Therapy and Comparative Criminology* 50, no. 2 (2006).

14. Horgan, *Why We'll Never Construct a Single Profile for Terrorists.*

15. Christine R Harris, "Embarrassment: A Form of Social Pain," *American Scientist* 94, no. 6 (2006).

16. Julie B. Kaplow et al., "The Long-Term Consequences of Early Childhood Trauma: A Case Study and Discussion," *Psychiatry* 69, no. 4 (2006).

17. Kuhn and Schanberg, "Responses to Maternal Separation: Mechanisms and Mediators."

18. Beverly H Brummett et al., "Prediction of All-Cause Mortality by the Minnesota Multiphasic Personality Inventory Optimism-Pessimism Scale Scores: Study of a College Sample During a 40-Year Follow-up Period," *Mayo Clinic Proceedings* 81, no. 12 (2006).

19. Elizabeth M. Hill et al., "Family History of Alcoholism and Childhood Adversity: Joint Effects on Alcohol Consumption and Dependence," *Alcoholism: Clinical and Experimental Research* 18, no. 5 (1994).

20. Patricia B. Sutker et al., "Exposure to War Trauma, War-Related PTSD, and Psychological Impact of Subsequent Hurricane," *Journal of Psychopathology and Behavioral Assessment* 24, no. 1 (2002).

21. Kenneth Reeves, "Racism and Projection of the Shadow," *Psychotherapy: Theory, Research, Practice, Training* 37, no. 1 (2000).

22. Speckhard et al., "Research Note: Observations of Suicidal Terrorists in Action."

23. James Blair, Derek Mitchell, and Karina Blair, *The Psychopath: Emotion and the Brain* (Malden, MA: Blackwell Publishing, 2005).

24. Ian Palmer, "Terrorism, Suicide Bombing, Fear and Mental Health," *International Review of Psychiatry* 19, no. 3 (2007).

25. Miller, "The Terrorist Mind."

# CHAPTER 5

# Principles and Requirements for Assessing X-Ray Image Interpretation Competency of Aviation Security Screeners

*Adrian Schwaninger, Saskia M. Koller, and Anton Bolfing*

## COMPETENCY ASSESSMENT IN AIRPORT SECURITY SCREENING

In response to the increased risk of terrorist attacks, large investments in aviation security technology have been made in recent years. However, the best equipment is of limited value if the people who operate it are not selected and trained appropriately to perform their tasks effectively and accurately. In recent years, the relevance of human factors has increasingly been recognized. One important aspect of the human factors is the competency of the aviation security screeners and its assessment.

Competency assessment maintains the workforce certification process. The main aim of certification procedures is to ensure that adequate standards in aviation security are consistently and reliably achieved. Certification of aviation security screeners can be considered as providing quality control over the screening process. Using certification tests, important information on strengths and weaknesses in aviation security procedures in general as well as on each individual screener can be obtained. As a consequence, certification can also be a valuable basis for qualifying personnel, measuring training effectiveness, improving training procedures, and increasing motivation. In short, certification and competency assessment can be very important instruments to improve aviation security.

The implementation of competency assessment procedures presents several challenges. First, what should be assessed has to be identified. Then, there should be consideration of how procedures for the certification of different competencies can be implemented. Another important challenge is international standardization, since several countries, organizations, and

even companies are developing their own certification or quality control systems.

The following international documents refer to the certification and competency assessment of aviation security staff:

- EU Regulation 2320/2002
- ICAO Annex 17, 3.4.3[1]
- ICAO-Manual on Human Factors in Civil Aviation Security Operations (Doc. 9808)[2]
- ICAO Human Factors Training Manual (Doc. 9683), Part 1, Chapter 4, and Appendix 6, Appendix 32[3]
- ICAO Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference, Doc. 8973, Chapter 4, I-4–45[4]
- ECAC Doc. 30, Chapter 12, and Annex IV-12A[5]
- ECAC Doc. 30 of the European Civil Aviation Conference specifies three elements for *initial* certification of airport security screeners:
  - an X-ray image interpretation exam
  - a theoretical exam
  - a practical exam

The *periodical* certification should contain a theoretical exam and an X-ray image interpretation exam. Practical exams can be conducted if considered necessary.

This section covers the first element, that is, how to examine X-ray image interpretation competency. Guidance material on the two other elements (theoretical exam and practical exam) already exists in the above-mentioned documents.

First, human factors best practice guidance for assessing the X-ray image interpretation competency of aviation security screeners is provided. Three different possibilities are mentioned, which can serve to measure X-ray image interpretation competency: covert testing, threat image projection (TIP), and computer-based image tests. Second, on-the-job assessment of the screener competency using TIP is discussed. Third, an example of a reliable, valid, and standardized computer-based test is presented: this test is used at more than 100 airports worldwide to measure X-ray image interpretation competency and also for certification purposes. Fourth, the application of this test in an EU-funded project (the VIA Project) including several European airports is presented.

## Requirements for Assessing Competency

One of the most important tasks of an aviation security screener is the interpretation of X-ray images of passenger bags and the identification of prohibited items within these bags. Hit rates, false alarm rates, and the time used to visually inspect an X-ray image of a passenger bag are important measures

that can be used to assess the effectiveness of screeners at this task. A hit is a correctly detected prohibited item within a passenger bag. The hit rate refers to the percentage of all bags containing a prohibited item that are correctly judged as being NOT OK. If a prohibited item is reported in a bag that does not contain one, this counts as a false alarm. The false alarm rate consequently is the percentage of all harmless bags (i.e., bags not containing any prohibited items) that is judged by a screener as containing a prohibited item. The time taken to process each bag is also important, as it helps in determining throughput rates and can indicate response confidence.

The results of an X-ray image interpretation test provide very important information for civil aviation authorities, aviation security institutions, and companies. Moreover, failing a test can have serious consequences, depending on the regulations of the appropriate authority. Therefore, it is essential that a test should be fair, reliable, valid, and standardized. In the last 50 years, scientific criteria have been developed that are widely used in psychological testing and psychometrics. These criteria are essential for the development of tests for measuring human performance. A summary of the three most important concepts, namely reliability, validity, and standardization, is now presented.[6]

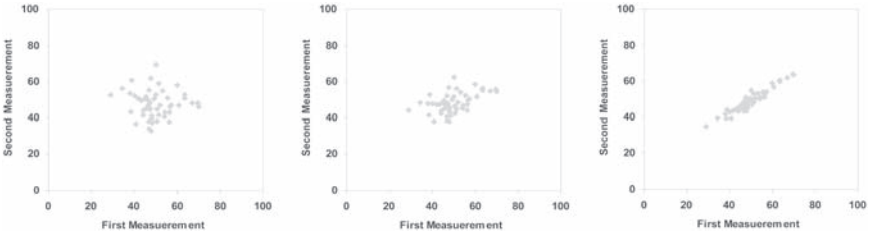
### *Reliability*

Reliability in the sense of the quality of measurement refers to the "consistency" or "repeatability" of measurements. It is the extent to which the measurements of a test remain consistent over repeated tests of the same participant under identical conditions. If a test yields consistent results for the same measure, it is reliable. If the repeated measurements produce different results, the test is not reliable. If, for example, an IQ test yields a score of 90 for an individual today and 125 a week later, it is not reliable. The concept of reliability is illustrated in Figure 5.1. Each point represents an individual. The x-axis represents the test results in the first measurement and the y-axis represents the scores of the second measurement with the same test. Figure 5.1 represents tests of different reliability. The test on the left in Figure 5.1 is not reliable. The score a participant achieved in the first measurement does not correspond at all with the test score in the second measurement.

The reliability coefficient can be calculated by the correlation between the two measurements. In Figure 5.1 left, the correlation is near zero, that is, $r = 0.05$ (the theoretical maximum is 1). The test in the center of Figure 5.1 is somewhat more reliable. The correlation between the two measurements is 0.50. Figure 5.1 right shows a highly reliable test with a correlation of 0.95.

The reliability of a test may be estimated by a variety of methods. When the same test is repeated (usually after a time interval during which job performance is assumed not to have changed), the correlation between the scores achieved on the two measurement dates can be calculated. This measure is called *test-retest reliability.* A more common method is to calculate the *split-half reliability.* In this method, the test is divided into two halves. The whole test

**Figure 5.1**
**Reliability Correlations**




is administered to a sample of participants and the total score for each half of the test is calculated. The split-half reliability is the correlation between the test scores obtained in each half. In the alternate forms method, two tests are created that are equivalent in terms of content, response processes, and statistical characteristics. Using this method, participants take both tests and the correlation between the two scores is calculated (*alternate forms reliability*). Reliability can also be a measure of a test's internal consistency. Using this method, the reliability of the test is judged by estimating how well the items that reflect the same construct or ability yield similar results. The most common index for estimating the internal reliability is Cronbach's alpha. Cronbach's alpha is often interpreted as the mean of all possible split-half estimates. Another internal consistency measure is KR 20 (for details see the documents mentioned above).

Acceptable tests usually have reliability coefficients between 0.7 and 1.0. Correlations exceeding 0.9 are not often achieved. For individual performance to be measured reliably, correlation coefficients of at least 0.75 and Cronbach's alpha of at least 0.85 are recommended. These numbers represent the minimum values. In the scientific literature, the suggested values are often higher.

### *Validity*

Validity indicates whether a test is able to measure what it is intended to measure. For example, hit rate alone is not a valid measure of detection performance in terms of discriminability (or sensitivity), because a high hit rate can also be achieved by judging most bags as containing prohibited items. In order to measure detection performance in terms of discriminability (or sensitivity), the false alarm rate must be considered, too.[7]

As for reliability, there are also different types of validity. The term *face validity* refers to whether a test appears to measure what it claims to measure. A test should reflect the relevant operational conditions. For example if a test for measuring X-ray image interpretation competency contains X-ray images and screeners have to decide whether the depicted bags contain a prohibited item, it is *face valid. Concurrent validity* refers to whether a test can distinguish between groups that it should be able to distinguish between (e.g., between

trained and untrained screeners). In order to establish *convergent validity*, it has to be shown that measures that should be related are indeed related. If, for example, threat image projection (TIP, i.e., the insertion of fictional threat items into X-ray images of passenger bags) measures the same competencies as a computer-based offline test, one would expect a high correlation between TIP performance data and the computer-based test scores. Another validity measure is called predictive validity. In *predictive validity*, the test's ability to predict something it should be able to predict is assessed. For example, a good test for preemployment assessment would be able to predict on-the-job X-ray screening detection performance. *Content validity* refers to whether the content of a test is representative of the content of the relevant task. For example, a test for assessing whether screeners have acquired the competency to detect different threat items in X-ray images of passenger bags should contain X-ray images of bags with different categories of prohibited items according to an internationally accepted prohibited items list.

### *Standardization/developing population norms*

The third important aspect of judging the quality of a test is standardization. This involves administering the test to a representative group of people in order to establish norms (a normative group). When an individual takes the test, it can then be determined how far above or below the average her or his score is, relative to the normative group. It is important to know how the normative group was selected, though. For instance, for the standardization of a test used to evaluate the detection performance of screeners, a meaningful normative group of a large and representative sample of screeners (at least 200 males and 200 females) should be tested.

In summary, competency assessment of X-ray image interpretation needs to be based on tests that are reliable, valid, and standardized. However, it is also important to consider test difficulty, particularly if results from different tests are compared to each other. Although two tests can have similar properties in terms of reliability, an easy test may not adequately assess the *level* of competency needed for the X-ray screening job.

## Competency Assessment of X-ray Image Interpretation

Currently, there are several methods used to assess X-ray image interpretation competency: Covert testing (infiltration testing), threat image projection (TIP), and computer-based image tests.

### *Covert testing*

Covert testing as the exclusive basis for individual competency assessment of X-ray image interpretation is only acceptable if the requirements

of reliability, validity, and standardization are fulfilled. For covert testing to achieve these requirements, a significant number of tests of the same screener is necessary in order to assess competency reliably. Note that this section does not apply to principles and requirements for covert testing used to verify compliance with regulatory requirements.

### *Threat image projection (TIP)*

Screener competency can also be assessed using TIP data. TIP is the projection of fictional threat items into X-ray images of passenger bags during the routine baggage screening operation. In this way the detection performance of a screener can be measured under operational conditions. However, using *raw* TIP data alone does not provide a reliable measure of individual screener detection performance For example, data need to be *aggregated* over time in order to have a large enough sample upon which to perform meaningful analysis. In order to achieve reliable, valid, and standardized measurements, several other aspects need to be taken into account as well when analyzing TIP data. One requirement is to use an appropriate TIP library. It should contain a large number of threat items, which represent the prohibited items that need to be detected and which feature a reasonable difficulty level. See the section on reliable measurement of performance using TIP for more information on how to use TIP data for measuring X-ray detection performance of screeners.

### *Computer-based X-ray image interpretation tests*

Computer-based X-ray image interpretation tests constitute a valuable tool for standardized measurements of X-ray image interpretation competency. These tests should consist of X-ray images of passenger bags containing different prohibited objects. The categories of threat items should reflect the prohibited items list and requirements of the appropriate authority, and it should be ensured that the test content remains up to date. The test should also contain clean bag images, that is, images of bags that do not contain a prohibited object. For each image, the screeners should indicate whether or not a prohibited object is present. Additionally, the screeners can be requested to identify the prohibited item(s). Image display duration should be comparable to operational conditions.

Test conditions should be standardized and comparable for all participants. For example, the brightness and contrast on the monitor should be calibrated and similar for all participants. This applies equally to other monitor settings that could influence detection performance (e.g., the refresh rate). In order to achieve a valid measure of detection performance, not only hit rates but also false alarm rates should be taken into account. An additional or alternative measure would be to count the number of correctly identified prohibited items (in this case, candidates have to indicate where exactly in the bag the threat is located).

The test should be reliable, valid, and standardized. Reliability should be documented by scientifically accepted reliability estimates (see above). If possible, validity measures should also be provided (see above). Individual scores should be compared to a norm that is based on a large and representative sample of screeners (see above).

The probability of detecting a threat item depends on the knowledge of a screener as well as on the general difficulty of the threat item. Image-based factors such as the rotation in which a threat item is depicted in the bag (view difficulty), the degree by which other objects are superimposed on a threat object (superimposition), and the number and type of other objects within the bag (bag complexity) influence detection performance substantially.[8] Tests should take these effects into account.

One of the skills that experienced screeners acquire is the ability to distinguish threat from non-threat objects and to have stored representations of what non-threat items look like within an X-ray image. Although the main task of an aviation security screener is the detection of threat items, an additional option could be the inclusion of non-threat objects in the test, which the test candidates are required to identify.

The section below on the X-Ray CAT describes a computer-based X-ray image interpretation test that is used at more than 100 airports worldwide for measuring screener competency and for certification purposes.

## Certification of X-Ray Image Interpretation Competency

As indicated above and as specified in ICAO Annex 17, 3.4.3, individuals carrying out screening operations should be certified initially and periodically. Certification can not only be considered as providing quality control over the screening process; it is also a valuable basis for qualifying personnel, measuring training effectiveness, improving training procedures, and increasing motivation. Certification data provide important information on strengths and weaknesses in aviation security procedures in general as well as on individual screeners. Furthermore, standardized certification can help in achieving an international standardization in aviation security. However, this is very challenging, since many countries, organizations, and companies develop their own certification and quality control systems. The present section gives a brief overview of how a certification system can be implemented.

As mentioned above, certification of screeners should contain a theoretical exam and an X-ray image interpretation exam. For periodical certification, practical exams can be conducted if considered necessary, unlike the initial certification, where practical exams are required. The exams should meet the requirements of high reliability and validity and standardization (see above).

The theoretical exam should inquire into the content of the regulations on aviation security screening. Apart from national rules and specifications, individual airports may enunciate questions covering special conditions. The

questionnaire should feature an acceptable reliability. It stands to reason that the questionnaire should be developed as a multiple choice exam. Good questions with qualitatively high answer possibilities (including distractor answers) are the basis for a good questionnaire, which differentiates between knowledgeable screeners and those who do not know the regulations very well.

The X-ray image interpretation exam can be adapted to the domain in which a screener is employed, that is, cabin baggage screening, hold baggage screening, or both. Since not every threat object always constitutes a threat during the flight, depending on where aboard the aircraft it is transported, screeners should be certified according to their domain. The certification of cabin baggage screeners should be based on cabin baggage images that contain all kinds of threat objects that are prohibited from being carried on in cabin baggage (e.g., guns, knives, improvised explosive devices, etc.). Objects that are prohibited from being transported in the cabin of an aircraft do not necessarily pose a threat when transported in the hold. Furthermore, different types of bags are transported in the cabin and the hold, respectively. Usually, small suitcases or bags serve as hand baggage, whereas big suitcases and traveling bags are transported in the hold of the aircraft. The certification of hold baggage screeners should be done using images of hold baggage. Hold baggage screeners only have to detect threat objects that are prohibited from being carried in the hold of an aircraft, like explosive materials. Persons working in both domains should be certified with both versions.

Screeners should be kept up to date regarding new and emerging threats. In order to verify whether this is consistently achieved, it is recommended that a recurrent certification should be conducted every year. The minimum threshold that should be achieved in the tests in order to pass certification should be defined by the national air transportation authority and should be based on a large and representative sample (see also the subsection below on standardization for more information on this topic).

## RELIABLE MEASUREMENT OF PERFORMANCE ON THE JOB USING THREAT IMAGE PROJECTION (TIP)

Threat image projection (TIP) is a function of state-of-the-art X-ray machines that allows the exposure of aviation security screeners to artificial but realistic X-ray images during the process of the routine X-ray screening operation at the security checkpoint. For cabin baggage screening (CBS), fictional threat items (FTIs) are digitally projected in random positions into X-ray images of real passenger bags. In hold baggage screening (HBS), combined threat images (CTIs) are displayed on the monitor. In this case, not only the threat item is projected but also an image of a whole bag that may or may not contain a threat item. This is possible if the screeners visually inspecting the hold baggage are physically separated from the passengers and their baggage. If a screener responds correctly by pressing a designated key on the keyboard (the "TIP key") it counts as a hit, which is indicated by a feedback

message. If a screener fails to respond to a projected threat within a specified amount of time, a feedback message appears indicating that a projected image was missed. This would count as a miss. Feedback messages also appear if a screener reports a threat although there was no projection of a threat or a CTI. In this case, it could be a real threat. Projecting whole bags in HBS provides not only the opportunity to project threat images (i.e., bags containing a threat item) but also non-threat images (i.e., bags not containing any threat item). This also allows the recording of false true alarms (namely, if a non-threat image was judged as containing a threat) and correct rejections (namely, if a non-threat image was judged as being harmless).

TIP data are an interesting source for various purposes like quality control, risk analysis, and assessment of individual screener performance. Unlike the situation in a test setting, the individual screener performance can be assessed on the job when using TIP data. However, if used for the measurement of individual screener X-ray detection performance, international standards of testing have to be met, that is, the method needs to be reliable, valid, and standardized (see above). In a study of CBS and HBS TIP, it was found that there were very low reliability values for CBS TIP data when a small TIP image library of a few hundred FTIs was used.[9] Good reliabilities were found for HBS TIP data when a large TIP image library was available. It is suggested that a large image library containing a representative sample of items of varying difficulty should be used when TIP is used for individual performance assessment. Also viewpoint difficulty, superimposition, and bag complexity may need to be considered. Finally, the data need to be aggregated over time in order to have a large enough sample upon which to perform meaningful analyses.

In addition to providing measures of operational performance, TIP is also a useful tool for increasing the motivation and attention of screeners. Screeners have to be continuously alert to avoid missing a TIP image. Finally, TIP allows the exposure of screeners to threat items they would usually not encounter (e.g., improvised explosive devices).

## X-RAY COMPETENCY ASSESSMENT TEST (X-RAY CAT)

This section introduces the X-Ray Competency Assessment Test (CAT) as an example of a computer-based test that can be used for assessing X-ray image interpretation competency. The CAT has been developed based on scientific findings regarding threat detection in X-ray images of passenger bags.[10] How well screeners can detect prohibited objects in passenger bags is influenced in two ways. First, it depends on the screener's knowledge of what objects are prohibited and what they look like in X-ray images. This knowledge is an attribute of the individual screener and can be enhanced by specific training. Second, the probability of detecting a prohibited item in an X-ray image of a passenger bag also depends on image-based factors. These are the rotation of

the prohibited item within the bag (view difficulty), the degree by which other objects are superimposed over an object in the bag (superposition), and the number and type of other objects within the bag (bag complexity). Systematic variation or control of the image-based factors is a fundamental property of the test and has to be incorporated in the test development. In this test, the effects of viewpoint are controlled by using two standardized rotation angles in easy and difficult view for each forbidden object. Superposition is controlled in the sense that it is held constant over the two views and as far as possible over all objects. With regard to bag complexity, the bags are chosen in such a way that they are visually comparable in terms of the form and number of objects with which they are packed.

The test contains two sets of objects in which object pairs are similar in shape. This construction not only allows the measurement of any effect of training, that is, if detection performance can be increased by training, but also possible transfer effects. The threat objects of one set are included in the training. By measuring detection performance after training using both sets of the test, it can be ascertained whether training also helped in improving the detection of the objects that did not appear during training. Should this be the case, it indicates a transfer of the knowledge gained about the visual appearance of objects used in training to similar-looking objects.

## Materials

Stimuli were created from Smiths-Heimann Hi-Scan 6040i color X-ray images of prohibited items and passenger bags (Figure 5.2 displays an example of the stimuli).

Based on the categorization of current threat image projection systems (Doc. 30 of the European Civil Aviation Conference, ECAC), four categories of prohibited items were chosen to be included in the test: guns, improvised explosive devices (IEDs), knives, and other prohibited items (e.g., gas, chemicals, grenades, etc.). The prohibited items were selected and prepared in collaboration with experts from the Zurich State Police, Airport Division, to be representative and realistic. Sixteen exemplars are used of each category (eight pairs). Each pair consists of two prohibited items of the same kind that are similar in shape.

**Figure 5.2**
**Prohibitive Item Identification**

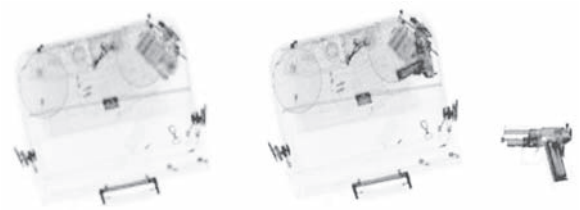


**Figure 5.3**
**Prohibitive Item Screen Projection**

The pairs were divided into two sets, set A and set B. Furthermore, each object within both sets is used in two standardized viewpoints (see Figure 5.3).

The easy viewpoint shows the object in canonical (easily recognizable) perspective,[11] the difficult viewpoint shows it with an 85 degree horizontal rotation or an 85 degree vertical rotation. In each threat category, half of the prohibited items of the difficult viewpoint are rotated vertically and the other half horizontally. The corresponding object of the other set is rotated around the same axis.

In order to compare the detection performance of an object to the detection performance of its counterpart in the other set, the two items (i.e., the bag images containing the threat objects) should not be different except for the object they contain. This means that the two objects should be comparable in regard to the rotation of the objects and their superimposition. Furthermore, the superposition should also be the same for both viewpoints of an object. This was achieved using an image-processing tool to combine the threat objects with passenger bags, controlling for superposition. This tool calculates the difference in brightness between the pixels of the two superimposed images (threat object and bag) using the following formula for superimposition:

$$SP = \frac{\sqrt{\sum [I_{SN}(x,y) - I_N(x,y)]^2}}{ObjectSize}$$

SP = Superimposition; $I_{SN}$ = Grayscale intensity of the $S_N$ (Signal plus Noise) image (contains a prohibited item); $I_N$ = Grayscale intensity of the N (Noise) image (contains no prohibited item); Object Size: Number of pixels of the prohibited item where R, G, and B are < 253

This equation calculates the superposition value of an object independent of its size. This value can be held constant for the two views of an object and the two objects of a pair, independent of the bag complexity, when combining the bag image and the prohibited item. To ensure that the bag images do not contain any other prohibited item, they were checked by at least two highly experienced aviation security instructors.

Clean bag images were assigned to the four categories and the two viewpoints of the prohibited items such that their image difficulty was balanced across all groups. This was achieved using the false alarm rate as the difficulty indicator for each bag image based on a pilot study with 192 screeners. In the test each bag appears twice, once containing a prohibited item (threat image) and once not containing a prohibited item (non-threat image). Combined with all prohibited items this adds up to a total of 256 test trials: 4 threat categories (guns, IEDs, knives, other) * 8 (exemplars) * 2 (sets) * 2 (views) * 2 (threat images v. non-threat images).

The task is to visually inspect the test images and to judge whether they are OK (contain no prohibited item) or NOT OK (contain a prohibited item). Usually the images disappear after 10 seconds. In addition to the OK/NOT OK response, screeners have to indicate the perceived difficulty of each image in a 100-point scale (difficulty rating: 1 = easy, 100 = difficult). All responses can be made by clicking buttons on the screen. The X-Ray CAT takes about 30–40 minutes to complete.

## Assessing Detection Performance

The detection performance of screeners can be assessed by their judgments of X-ray images. It should be stressed that not only is the hit rate (i.e., the proportion of correctly detected prohibited items in the threat images) an important value but so is the false alarm rate (i.e., the proportion of non-threat images that were judged as being NOT OK, that is, as containing a prohibited item). This incorporates the definition of detection performance as the ability not only to detect prohibited items but also to discriminate between prohibited items and harmless objects (that is, to recognize harmless objects as harmless). Therefore, in order to evaluate the detection performance of a screener, his or her hit rate in the test has to be considered as well as his or her false alarm rate.[12] There are different measures of detection performance that set the hit rate against the false alarm rate, for example d' or A'. These measures are explained in more detail below.

## Reliability of the X-Ray CAT

As elaborated earlier in this chapter, the reliability of a test stands for its consistency. As a measure of the X-Ray CAT's quality, the internal reliability index Cronbach's alpha and the Guttman split-half reliability were computed. The calculations are based on the results of a study at several airports throughout Europe (see below for the details and further results of the study) including the data on 2265 screeners who completed the X-Ray CAT. The reliability measures were calculated based on correct answers, that is, hits for threat images and correct rejections (CR) for non-threat images (# correct rejections = # non-threat items—# false alarms). The analyses were made separately for threat images and for non-threat images. Table 5.1 shows the reliability coefficients.

**Table 5.1**
**Reliability**

| *Reliability analysis* | | | |
|---|---|---|---|
| *Reliability coefficients* | | *Hit* | *CR* |
| X-Ray CAT | Alpha | .98 | .99 |
| | Split-half | .97 | .99 |

As stated above, an acceptable test should reach reliability values of at least .85 (Cronbach's alpha). Bearing this in mind, the reliability coefficients listed in Table 5.1 show that the X-Ray CAT is very reliable and therefore a useful tool for measuring the detection performance of aviation security screeners.

## Validity of the X-Ray Cat

Regarding the different types of validity as described above, the face validity and the content validity can be confirmed instantly. In terms of face validity, the X-Ray CAT is valid as it appears to measure what it claims to measure and it reflects the relevant operational conditions. In terms of content validity, the X-Ray CAT is valid as its content is representative of the content of the relevant task. The test includes prohibited items from different categories based on the definition in Doc. 30 of the European Civil Aviation Conference (ECAC) that have to be detected by the aviation security screeners. Regarding the convergent validity of the CAT, it can be compared to another test that measures the same abilities. An example of such a test that is also widely used at different airports is the Prohibited Items Test.[13] To assess convergent validity, the correlation between the scores on the X-Ray CAT and the scores on the PIT of a sample that conducted both tests is calculated. This precise procedure was applied to a sample of 473 airport security screeners. The result can be seen in Figure 5.4 (r = .791).

Since correlation coefficients range from 0 (no correlation) to 1 (perfect correlation) (see also above), the convergent validity can be classified as quite high. This means that the X-Ray CAT and the PIT measure the same X-ray image interpretation competency. Other studies have also confirmed the concurrent validity, that is, the ability of a test to discriminate, for example, between trained and untrained screeners.[14] Figure 5.5 shows the results of the study. It can be seen that the detection performance increases for the trained screeners but not for the untrained screeners. This means that the test is able to discriminate between screeners who received training with the computer-based training system X-Ray Tutor and those who did not receive training with X-Ray Tutor.[15] Therefore, the concurrent validity of the X-Ray CAT can be confirmed.

**Figure 5.4**
**CAT and PIT Detection Performance**

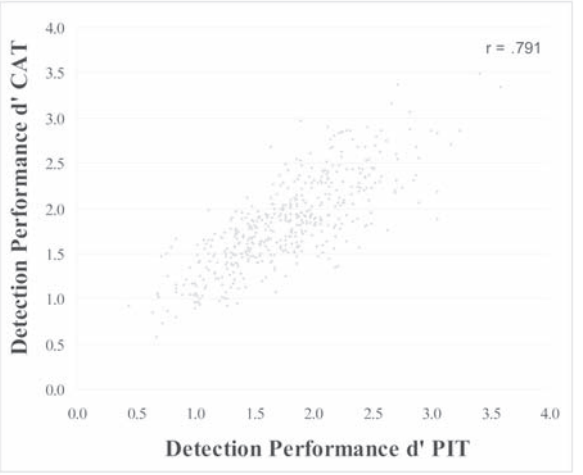
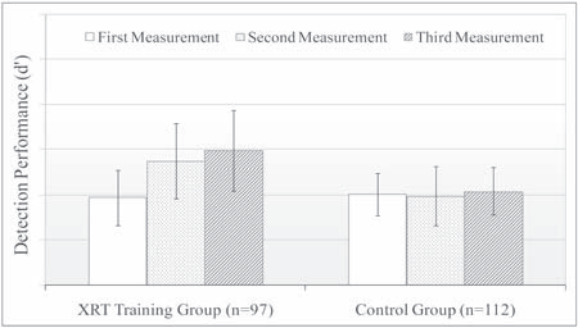



**Figure 5.5**
**Detection Performance of Groups**




## Standardization

The X-Ray CAT was standardized in regard to its development. The revisions of the test were based on data from representative samples (N > 94) of airport security screeners (more details on the revisions can be found in the following subsection). In the study described in the section on real world application, involving a large and representative sample of airport security screeners (*N* = 2265), a mean detection performance A' of 0.8 (SD = 0.08) was achieved. There are different approaches to the definition of pass marks. The normative approach defines a pass mark as the threshold at which a certain proportion of screeners fails the test (e.g., not more than 10 percent), based on a test measurement. That is, a screener is rated in relation to all other screeners. The criterion-referenced approach sets the pass mark according to a defined crite-

rion. For instance, the results could be compared to the test results obtained in other countries when the test was conducted the first time or by having a group of experts (e.g., using the Angoff method)[16] rate the difficulty of the test items (in this case the difficulty of the images) and the minimum standard of performance. These approaches can of course be combined. Furthermore, the standard might be adjusted by taking into account the reliability of the test, the confidence intervals, and the standard error of measurement.

According to the Measurement Research Associates, the level of performance required for passing a credentialing test should depend on the knowledge and skills necessary for acceptable performance in the occupation and should not be adjusted to regulate the number or proportion of persons passing the test.[17] The pass point should be determined by careful analysis and judgment of acceptable performance. The Angoff method is probably the most basic form of criterion-based standard setting, due to the relatively simple process of determining the pass points.[18] In this method, judges are expected to review each test item and a passing score is computed from an estimate of the probability of a minimally acceptable candidate answering each item correctly. As a first step, the judges discuss and define the characteristics of a minimally acceptable candidate. Then, each judge makes an independent assessment of the probability for each item that this previously defined minimally acceptable candidate will answer the item correctly. To determine the probability of a correct response for each item, that is, the passing score, the judges' assessments of the items are averaged. Then, these probabilities for all items of the test are averaged to obtain the pass point for the test.[19] The Angoff method features several advantages: it is easy to implement, understand, and compute.[20] However, the Angoff method also has disadvantages. First, it assumes that the judges have a good understanding of the statistical concepts. Second, the panelists may lose sight of the candidates' overall performance on the assessment due to the focus on individual items, as this method uses an item-based procedure.[21] Moreover, the continuum of item probabilities tends to result in considerable variability among the judges. Many judges have difficulties defining candidates who are minimally competent.[22] In the case of aviation security screeners, judges would have to focus on a person who would be just sufficiently capable of doing the job.

## Revision

The development of a scientifically approved test is a complex procedure. Here, the development of the X-Ray CAT is explained in order to provide an example. The first step in a test's development is the definition of what should be measured and how. It was planned that a test should be developed for the purpose of measuring the X-ray image interpretation competency of airport security screeners when they search X-ray images of passenger bags for prohibited objects. In order for the test to be face valid (see above), the nature of the items to be chosen was obvious. They should be X-ray images of passenger bags where some of these images contain a prohibited item and some do

not. Careful thought should be invested in the design of the test. In this case, since it is known that several factors can influence the detection performance of an aviation security screener, the items should be constructed considering these factors. That is, the items should be constructed by controlling for the image-based factors view difficulty, superposition, and bag complexity. Furthermore, the effects that should or could be measured with the test should be considered. Depending on the initial point and the aims, the items can be developed quite differently. The X-Ray CAT is composed of two similar sets and contains prohibited items of different categories, each one in two different viewpoints. The set construction serves the purpose of measuring the transfer effects. Transfer effect means the transfer of knowledge about threat objects that is gained during training to threat objects that were not included in training but are similar to objects that were included. The X-Ray CAT can measure several effects: the effect of viewpoint, threat category, training, and transfer (see above for a more detailed description).

After the first version of the test had been constructed, it was administered to a large and representative sample in a pilot study ($N = 354$ airport security screeners). Based on the results of this pilot study, the first revision took place. First of all, a reliability analysis gave information on the quality of the test and each item (item difficulty and item-to-total correlation). Those items with a difficulty below the range of acceptable difficulty had to be revised. The range of acceptable item difficulty depends on the answer type. In this case, an item can be correct or incorrect, that is having a 50 percent chance probability. The range of acceptable difficulty was defined between 0.6 and 0.9. Furthermore, the items should possess as high an item-to-total correlation as possible. In this case, all items with a negative or very small item-to-total correlation were corrected. In order to measure any effect of threat category on the detection performance, the detection performance of a threat object should depend only on the threat object itself and not on the difficulty of the bag it is placed in. To this end, the difficulty of the bags should be balanced across all categories, across both viewpoints of the test, and also across the two sets. As a measure of difficulty for the bag images, the false alarm rate was consulted (i.e., how many times a bag was judged as containing a threat item although there was none). Then, the bags were assigned to the four categories in such a way that their mean difficulty was not statistically different. The threat objects were built into the new bags if necessary, again considering superposition. At last, the items were shifted between the two sets (always incorporating the twin structure) in order to equalize the difficulty of the sets. The revised test was administered to another sample ($N = 95$ airport security screeners), repeating the revision steps as necessary. After a third ($N = 359$ airport security screeners) and a fourth ($N = 222$ airport security screeners) revision, the X-Ray CAT was acceptable in terms of stable reliability, item difficulty, and item-to-total correlation.

In summary, the test was revised according to the image difficulty, the item-to-total correlation, and the balancing of the difficulty of the clean bag

images. The aim is a high reliability with items featuring high item-to-total correlations and acceptable item difficulty. The difficulty of a threat image (a bag containing a prohibited object) should depend only on the object itself and not on the difficulty of the bag. Otherwise, a comparison between the detection performance for the different threat categories could be biased.

## REAL WORLD APPLICATION OF THE X-RAY COMPETENCY ASSESSMENT TEST (X-RAY CAT)

X-Ray CAT was used in several studies and in a series of international airports in order to measure the X-ray image interpretation competencies of screening officers. In this section, the application of X-Ray CAT is presented along with discussions and results obtained by means of the EU-funded VIA Project.

### The VIA Project

The VIA Project evolved from the tender call in 2005 of the European Commission's Leonardo da Vinci program on vocational education and training. The project's full title is "Development of a Reference Levels Framework for A'VIA'tion Security Screeners." The aim of the project is to develop appropriate competence and qualification assessment tools and to propose a reference levels framework (RLF) for aviation security screeners at national and cross-sectoral levels.

To date, 11 airports in six European countries are involved in the project. Most of these airports are going through the same procedure of recurrent tests and training phases. This makes it possible to scientifically investigate the effect of recurrent weekly computer-based training and knowledge transfer and subsequently to develop a reference levels framework based on these outcomes. The tools used for testing in the VIA project are the computer-based training (CBT) program, X-Ray Tutor,[23] and the X-Ray CAT. Subsequently, the results of the computer-based test measurements included as part of the VIA project procedure are reported in detail.

### VIA Computer-Based Test Measurement Results

As explained earlier, the X-Ray Competency Assessment Test (CAT) contains 256 X-ray images of passenger bags, half of which contain a prohibited item. This leads to four possible outcomes for a trial: a "hit" (a correctly identified threat object), a "miss" (a missed threat object), a "correct rejection" (a harmless bag correctly judged as being OK), and a "false alarm" (an incorrectly reported threat object).

In terms of sensitivity, the hit rate alone is not a valid measure to assess X-ray image interpretation competency. It is easy to imagine that a hit rate of 100 percent can be achieved by simply judging every X-ray image as containing a prohibited item. In this case, the entire set of non-threat items is

completely neglected by this measure (the false alarm rate would also be 100 percent). In contrast, Green and Swets in 1966 developed a signal detection performance measure d' (say, d prime), taking into account hit rates as well as false alarm rates.[24] Often, d' is referred to as sensitivity, emphasizing the fact that it measures the ability to distinguish between noise (in our case an X-ray image of a bag without a threat) and signal plus noise (in our case an X-ray image containing a prohibited item).

D' is calculated using the formula d' = z(H)—z(F), where H is the hit rate, F the false alarm rate, and z the z-transformation. For the application of d', the data have to fulfill certain criteria (noise and signal plus noise must be normally distributed and have the same variance). If these requirements are not fulfilled, another established, "non-parametric" measure is often used: A' (say, A prime). The measure also meets the requirement of setting the hit rate against the false alarm rate in order to achieve a reliable and valid measure of image interpretation competency. A' was the measure of choice for the current analyses because its non-parametric character allows its use independently from the underlying measurements distributions. A' can be calculated as follows, where H represents the hit rate of a test candidate or group and F represents its false alarm rate: A' = 0.5 + [(H—F)(1 + H—F)] / [4H(1—F). If the false alarm rate is greater than the hit rate, the equation must be modified:[25] A' = 0.5—[(F—H)(1 + F—H)] / [4F(1—H)].[26]

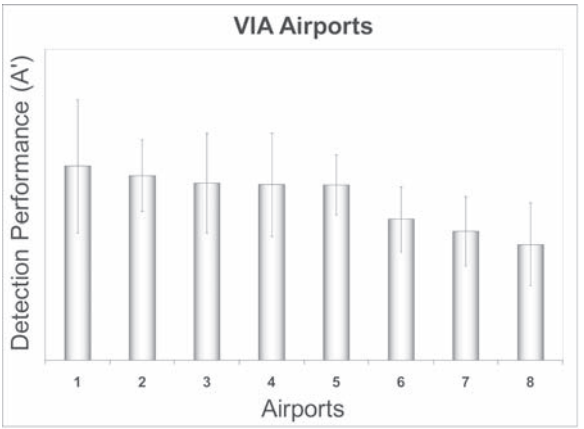
The reported results provide graphical displays of the relative detection performance measures A' at the nine European airports that participated in the present study by the VIA Project, as well as another graph showing the effect of the two viewpoints on the different threat categories as explained earlier. In order to provide statistical corroboration of these results, an analysis of variance (ANOVA) on the two within-participants factors, view difficulty and threat category (guns, IEDs, knives and other items), and the between-participants airport factor is reported as well. As part of the ANOVA, only the significant interaction effects are reported and considered to be noteworthy in the context.

### *Detection performance comparison between airports*

Figure 5.6 shows the comparison of the detection performance achieved at eight European airports that participated in the VIA project. First, the detection performance was calculated for each screener individually. Then, the data were averaged across screeners for each airport; this is shown in Figure 5.6. Thin bars represent the standard deviation (a measure of variability) across screeners.. Due to its security sensitivity and for data protection reasons, the individual airports' names are not indicated and no numerical data are given here.

Although no numerical data is displayed in the graph, we can discern substantial differences between the airports in terms of mean detection performance and standard deviation. As described above, all VIA airports go through a similar procedure of alternation of test phases and training phases. Nevertheless, there are considerable differences between them. There were large differences

**Figure 5.6**
**Detection Performance of Airports**




in the initial positions when the project was started, and the baseline assessment test, which is reported here, was conducted at different times at different airports. The differences can be put down to differences in the amount of training that was accomplished prior to this baseline testing as well as to differences in the personnel selection assessment. Some of the reported airports were already coached prior to the VIA project, though with diverse intensity and duration. Taking these differences into account, the reported results correspond fairly well with our expectations based on earlier studies of training effects.

### *Detection performance comparison between threat categories regarding view difficulty*

Figure 5.7 shows again the detection performance measure A', but with a different focus. The data are averaged across the airports shown in figure 5.6, but analyzed by view difficulty within threat categories. There is a striking effect on detection performance deriving from view difficulty. Performance is significantly higher for threat objects depicted in easy views than for threat objects depicted in difficult views (canonical views rotated by 85 degrees).

Although this effect can be found in every one of the four threat categories, there are significant differences between them regarding general differences between the mean detection performances and also between the effect sizes of view difficulty that are unequal between threat categories. Knives and IEDs, for example, differ very much in view difficulty effect size but not so much in average detection performance. As can be seen in Figure 5.8, the reason is quite simple: IEDs consist of several parts and not all parts are depicted in easy or in difficult view at the same time. Some parts are always depicted in easy view when others are difficult, and vice versa. Knives have very characteristic shapes. They look consistently longish when seen perpendicular to their

**Figure 5.7**
**Airport Detection of Prohibitive Items**

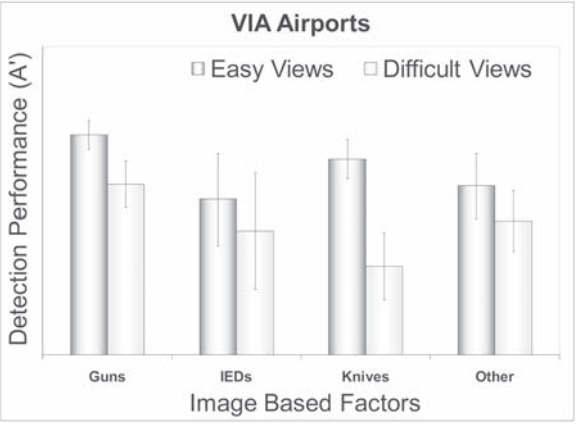
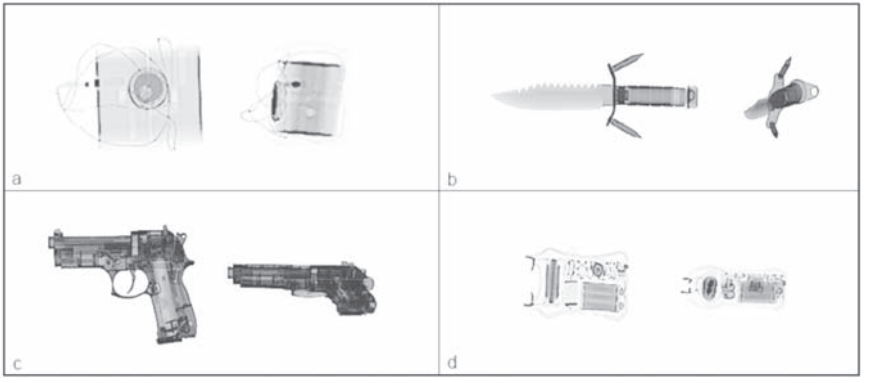



**Figure 5.8**
**Views of Prohibitive Items**




cutting edge but very small and thin when seen in parallel to their cutting edge. This interaction effect between threat item category and view difficulty can easily be observed in Figure 5.7, where the difference between easy and difficult views is much larger in knives than in IEDs. Furthermore, based on earlier studies of training effects, it is important to mention here that this pattern shown in Figure 5.7 is also highly dependent on training (interaction effects [category * airport and view difficulty * airport]).[27] Figure 5.8 illustrates two separate views of four prohibitive items.

### *Analysis of Variance (ANOVA)*

The following statistics provide quantitative values for what has been reported graphically. This allows us to compare the effects of the different

factors. We applied a three-way ANOVA to the two within-subjects factors, category and view difficulty, and one between-subjects airport factor on the detection performance measure A'.

The analysis revealed highly significant main effects on threat category (guns, IEDs, knives, and other items) with an effect size of $\eta^2 = .131$, $F(3, 5602.584) = 339.834$, $MSE = 2.057$, $p < .001$, on view difficulty (easy view v. difficult/rotated view) with an effect size of $\eta^2 = .47$, $F(1, 2257) = 2009.772$, $MSE = 9.031$, $p < .001$, and also on the between-subjects airport factor with an $\eta^2 = .080$, $F(1, 2257) = 28.128$, $MSE = 1.415$, $p < .001$. The following two-way interactions were also highly significant: threat category * view difficulty: $\eta^2 = .094$, $F(3, 6542.213) = 233.969$, $MSE = .931$, $p < .001$, threat category * airport $\eta^2 = .068$, $F(3, 5602.584) = 23.411$, $MSE = .142$, $p < .001$, and view difficulty * airport $\eta^2 = .159$, $F(1, 2257) = 60.953$, $MSE = .274$, $p < .001$. These results indicate different detection performance for different threat categories and higher detection performance for prohibited items in easy view than for rotated threat items (the effect of viewpoint).[28] This is consistent with results reported in the view-based object recognition literature (for reviews see, for example, two works by Tarr and Bülthoff.[29] The effect sizes were very large according to Cohen's conventions.[30]

### Discussion

Although the reported real world application consists of baseline measurement data only, some important features of the X-Ray CAT could be illustrated well. X-Ray CAT allows us to measure and to evaluate the effects of view difficulty and threat objects practically independently of each other. Furthermore, the X-Ray CAT can be used as very reliable tool to compare the X-ray image interpretation competency of security staff at different airports and other types of infrastructure using X-ray technology for security control procedures.

## SUMMARY AND CONCLUSIONS

The competency of a screener to detect prohibited items in X-ray images quickly and reliably is important for any airport security system. Computer-based tests, TIP, and to a limited extent covert tests can be used to assess individual competency in X-ray image interpretation. However, to achieve reliable, valid, and standardized measurements, it is essential that the requirements and principles detailed in this chapter are followed by those who produce, procure, or evaluate the competency assessment of the X-ray image interpretation tests of individual screeners.

This chapter introduced the competency assessment in airport security screening. In order to achieve a meaningful result the assessment has to meet the criteria of reliability and validity. Furthermore, the assessment has to be standardized to allow the evaluation of screeners' performance in relation to the population norm. There are three means for assessing X-ray image

interpretation competency: covert testing, threat image projection (TIP), and computer-based image testing. Another important feature of maintaining the high level of X-ray baggage screening within aviation security is the initial and recurrent certification of screening personnel.

Threat image projection (TIP) as a means to assess X-ray image interpretation competency was illustrated in detail, as well as the conditions that have to be fulfilled in order for TIP to be a reliable and valid instrument.

This chapter also focused on the computer-based X-Ray Competency Assessment Test (X-Ray CAT). It features very high reliability scores and its design allows us to measure the X-ray image interpretation competency of aviation security screeners with regard to different aspects of their ability and knowledge. The X-Ray CAT is widely used at many different airports throughout the world, for competency assessment and certification purposes as well as in studies assessing the fundamentals of the demands required for the job of the aviation security screener.

This chapter continued by showing how a reliable, valid, and standardized test can be used to compare X-ray image interpretation competency across different airports and countries. The results of an EU-funded project (the VIA Project) showed remarkable differences in mean detection performance across nine European airports. All these countries conduct now weekly recurrent computer-based training. Since the X-Ray CAT will be conducted again in the first quarter of 2008, the VIA Project will also provide important insights on the benefits of computer-based training for increasing security and efficiency in X-ray screening.

## NOTES

1. ICAO Annex 17, 3.4.3 ("Each Contracting State shall ensure that the persons carrying out screening operations are certified according to the requirements of the national civil aviation security programme").

2. ICAO Manual on Human Factors in Civil Aviation Security Operations, Doc. 9808.

3. ICAO Human Factors Training Manual, Doc. 9683, part 1, chapter 4, and in Appendix 6—"Guidance on Recruitment, Selection, Training, and Certification of Aviation Security Staff"—and Appendix 32—"Guidance on the Use of Threat Image Projection."

4. ICAO Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference, Doc. 8973, chapter 4, I-4–45 ("Recruitment, Selection, Training, and Certification of Security Staff").

5. ECAC Doc. 30, Annex IV-12A, "Certification Criteria for Screeners," and ECAC Doc. 30, chapter 12, 12.2.3, "Certification of Security Staff," 1.1.10.3.

6. Joshua A. Fishman and Tomas Galguera, *Introduction to Test Construction in the Social and Behavioural Sciences. A Practical Guide* (Oxford: Rowman & Littlefield, 2003); Paul Kline, *Handbook of Psychological Testing* (London: Routledge, 2000); Kevin R. Murphy and Charles O. Davidshofer, *Psychological Testing* (Upper Saddle River, NJ: Prentice Hall, 2001).

7. Neil A. MacMillan and C. Douglas Creelman, *Detection Theory: A User's Guide* (New York: Cambridge University Press, 1991); Franziska Hofer and Adrian Schwaninger, "Reliable and Valid Measures of Threat Detection Performance in X-ray Screening," *IEEE ICCST Proceedings* 38 (2004): 303–8.

8. Adrian Schwaninger, Diana Hardmeier, and Franziska Hofer, "Measuring Visual Abilities and Visual Knowledge of Aviation Security Screeners," *IEEE ICCST Proceedings* 38 (2004): 258–64; Adrian Schwaninger, "Evaluation and Selection of Airport Security Screeners," *AIRPORT* 2 (2003): 14–15.

9. Franziska Hofer and Adrian Schwaninger, "Using Threat Image Projection Data for Assessing Individual Screener Performance," *WIT Transactions on the Built Environment* 82 (2005): 417–26.

10. Schwaninger, Hardmeier, and Hofer, "Measuring Visual Abilities and Visual Knowledge of Aviation Security Screeners"; Schwaninger, "Evaluation and Selection of Airport Security Screeners."

11. Stephen E. Palmer, Eleanor Rosch, and Paul Chase, "Canonical Perspective and the Perception of Objects," in *Attention and Performance IX*, ed. John Long and Alan Baddeley, 135–52 (Hillsdale, NJ: Erlbaum, 1981).

12. David M. Green and John A. Swets, *Signal Detection Theory and Psychophysics* (New York: Wiley, 1966); Neil A. MacMillan and C. Douglas Creelman, *Detection Theory: A User's Guide* (New York: Cambridge University Press, 1991); Hofer and Schwaninger, "Reliable and Valid Measures of Threat Detection Performance in X-Ray Screening"; Hofer and Schwaninger, "Using Threat Image Projection Data for Assessing Individual Screener Performance."

13. Diana Hardmeier, Franziska Hofer, and Adrian Schwaninger, "Increased Detection Performance in Airport Security Screening Using the X-Ray ORT as Pre-employment Assessment Tool," *Proceedings of the 2nd International Conference on Research in Air Transportation*, ICRAT 2006, Belgrade, Serbia and Montenegro, June 24–28, (Belgrade, Serbia: ICRAT, 2006), 393–97.

14. Saskia M. Koller et al., "Investigating Training, Transfer and Viewpoint Effects Resulting from Recurrent CBT of X-Ray Image Interpretation," *Journal of Transportation Security* 1, no. 2 (2008).

15. Adrian Schwaninger, "Computer-Based Training: A Powerful Tool for the Enhancement of Human Factors," *Aviation Security International* 10 (2004): 31–36; Adrian Schwaninger, "Increasing Efficiency in Airport Security Screening," *WIT Transactions on the Built Environment* 82 (2005): 405–16.

16. William Herbert Angoff, "Norms, Scales, and Equivalent Scores," in *Educational Measurement* (2nd ed.), ed. Robert L. Thorndike, 508–600 (Washington, DC: American Council on Education, 1971).

17. Measurement Research Associates, *Criterion Referenced Performance Standard Setting*, 2004, http://www.measurementresearch.com/wwa/default.shtml.

18. Muhammad Naveed Khalid and Muhammad Saeed, "Criterion Referenced Setting Performance Standards with an Emphasis on Angoff Method," *Journal of Research and Reflections in Education* 1 (2007): 66–87.

19. Angoff, "Norms, Scales, and Equivalent Scores."

20. Ronald A. Berk, "A Consumer's Guide to Setting Performance Standards on Criterion-Referenced Tests," *Review of Educational Research* 56 (1986): 137–72.

21. Measurement Research Associates, *Criterion Referenced Performance Standard Setting.*

22. Angoff, "Norms, Scales, and Equivalent Scores."

23. Ibid.

24. David Green and John Swets, "Signal Detection Theory and Psychopsychies," in *Detection Theory: A User's Guide*, ed. Neil MacMillan (London: Earlbaum, 1966).

25. Doris Aaronson and Brian Watts, "Extensions of Grier's Computational Formulas for A' and B" to Below-Chance Performance," *Psychological Bulletin* 102 (1987): 439–42.

26. Harold Stanislaw and Natasha Todorov, "Calculation of Signal Detection Theory Measures," *Behavior Research Methods, Instruments, and Computers* 31, no. 1 (1999): 137–49; Green and Swets, *Signal Detection Theory and Psychophysics;* Irwin Pollack and Donald A. Norman, "A non-parametric Analysis of Recognition Experiments," *Psychonomic Science* 1 (1964): 125–26; J. Brown Grier, "Nonparametric Indexes for Sensitivity and Bias: Computing Formulas," *Psychological Bulletin* 75 (1971): 424–29; ICAO Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference, Doc. 8973, chapter 4, I-4–45 ("Recruitment, Selection, Training and Certification of Security Staff").

27. Ibid.

28. Paul Kline, *Handbook of Psychological Testing* (London: Routledge, 2000).

29. Michael J. Tarr and Heinrich H. Bülthoff, "Is Human Object Recognition Better Described by Geon Structural Descriptions or by Multiple Views? Comment on Biederman and Gerhardstein (1993)," *Journal of Experimental Psychology: Human Perception and Performance* 21 (1995): 1494–1505; Michael J. Tarr and Heinrich H. Bülthoff, "Image-Based Object Recognition in Man, Monkey and Machine," in *Object Recognition in Man, Monkey and Machine*, ed. Michael J. Tarr and Heinrich H. Bülthoff, 1–20 (Cambridge, MA: MIT Press, 1998).

30. Jacob Cohen, *Statistical Power Analysis for the Behavioral Sciences* (New York: Erlbaum, Hillsdale, 1988).

# CHAPTER 6

# Constructing a Comprehensive Aviation Security Management Model (ASMM)

*Chien-tsung Lu*

In 1999, the Federal Aviation Administration (FAA) began to promote a new scientific and systemic troubleshooting procedure for aviation security and safety, derived from the FAA's Office of System Safety. Yet by the year 2007, most U.S. air carriers, manufacturers, and airports had not implemented the processes recommended in the *System Safety Handbook* and elsewhere. In addition to the absence of regulations, the lack of implementation results primarily from the fact that the value of system safety is unclear. While the concept of system safety is viewed with skepticism by the aviation industry, academia possesses an opportunity to help explain that it is essential and useful.

This chapter uses a case study with philosophy and documentary analysis to accomplish research objectives, which include the following: (1) reviewing the FAA's voluntary safety programs and revealing operational difficulty; and (2) proposing and demonstrating the process of a comprehensive aviation security management model.

Safety is the mission priority and universal norm for the worldwide aviation industry including airlines, airports, traffic control, fixed-base operators, and related sectors. The September 11 terrorist attacks in 2001 provided the impetus for further air transportation security measures. Airport security is of the utmost importance and, to a great extent, has triggered numerous studies and research projects involving operational performance. In the official report of the 9/11 Commission, a multilayer redundant system is recommended to effectively secure the needed safety quality and security levels.[1] According to the report,

> The FAA set and enforced aviation security rules, which airlines and airports were required to implement. The rules were supposed to produce a "layered" system of

defense. This means that the failure of any one layer of security would not be fatal, because additional layers would provide backup security.[2]

## SAFETY MANAGEMENT PROGRAM

In fact, system safety's philosophy of "redundancy" or the "safety net" inspired the U.S. government to generate a better aviation safety program beginning in 1996. Originally, the Office of System Safety was empowered to lead aviation system safety research, promote findings, and apply the findings. As described in the FAA's Order 8040–4,

> This order establishes the safety risk management policy and prescribes procedures for implementing safety risk management as a decision-making tool within the Federal Aviation Administration (FAA).[3]

FAA Administrative Order 8040–4 requires the Office of System Safety (1) to incorporate a risk management process for all high-consequence decisions including those involving airlines and airports, and (2) to provide a handbook/manual of system risk management and recommend system safety tools to all U.S.-based airlines.[4] To accomplish the appointed tasks and promote risk management within the industry, the Office of System Safety began sponsoring an annual system safety conference and workshop for airline and airport managers in 1999. Research efforts of the FAA, project contractors, and conference participants were exchanged and ideas were discussed during each workshop. Despite the fact that the *System Safety Handbook* contains safety theories, the current system safety studies coming from the industry are limited to engineering/hardware design such as that of navigation systems, weather and turbulence forecasts, global positioning systems, runway incursions, and airport operational procedures. Although an error management model has been disseminated by the FAA, a comprehensive procedure of application for nonengineering disciplines is nonexistent.

In 2006, Lu, Wetmore, and Przetak further conducted a content analysis study of the annual system safety conference.[5] They discovered that the FAA's advocate was mostly concerned with the conceptual nature of risk management, rather than with an in-depth demonstration of safety analysis techniques (see Table 6.1). As a result, most airlines (flag or nonflag), airports, and flight based operations (FBOs) did not incorporate nonmandatory system safety management procedures into their operation unless a voluntary engagement had been initiated.[6] In addition, the use of system safety concepts has primarily been tied to risk management using a basic descriptive trend study, however, most of the results are not accessible to the public. Examples of such voluntary programs include the FAA's Runway Incursion Information (RII), the Air Transportation Oversight System (ATOS) or Advanced Quality Program (AQP), the Safety Reporting System and Database (SRSD), Flight Operational Quality Assurance (FOQA), the Air Carrier Operations System

**Table 6.1**
**System Safety Workshops And Conferences—Content Analysis**

| | *2001* | *2002* | *2003* | *2004* |
|---|---|---|---|---|
| System Safety Management | X | X | X | X |
| Aviation System Safety Program (AvSP) | X | X | X | X |
| FAA-Airlines Collaboration | X | X | X | X |
| Data Collection & Risk Analysis | X | X | X | X |
| System Risk Management (SRM) & Safety Culture | | X | X | X |
| Flight crews-centered | X | X | | X |
| Non-flight crews-centered | X | X | X | X |
| All aviation workers | X | | | |
| Air Carrier Operations System Model (ACOSM) | X | | | |
| Aviation Safety Action Program (ASAP) | X | X | | X |
| Flight Operational Quality Assurance (FOQA) | X | X | | X |
| Advanced Quality Program (AQP) | X | | | |
| Aviation Safety Reporting System (ASRS) | X | | | X |
| Continuous Analysis and Surveillance Systems (CASS) | X | | | |
| Maintenance Resource Management (MRM) training | X | X | | |
| Human Factor CRM training | X | X | X | X |
| Case-based training/Naturalistic Decision-making | X | X | X | X |
| Regulations | X | X | X | |
| Cost-benefit and Safety Investment | X | X | X | X |
| Failure Mode and Effective Analysis (FMEA) Concept | | X | | |
| Failure Mode and Effective Analysis (FMEA) Application | | | | |
| Fault Tree Analysis (FTA) Concept | | X | | |
| Fault Tree Analysis (FTA) Application | | | | |
| Risk Control Management (RCA) | | | | X |
| Hybrid Causal Modeling | | | X | X |

*Note:* The origin of this Content Analysis Table was statistically extracted from the research projects and papers presented at the FAA System Safety workshops and conferences between 2000 and 2004. As shown in the above table, most researches either focused on the advocate of using System Safety concepts or risk analysis covering trend study. Researchers did not apply tools (i.e, FTA or FMEA) to their studies for a demonstration. Especially, there were only two papers explained FMEA and FTA techniques over the past four years. Yet no further application was found.

Model (ACOSM), the Aviation Safety Action Program (ASAP), and NASA's Aviation Safety Reporting System (ASRS).

All the aforementioned programs are checklisted trend studies centered around hazard identification, but they are segregated instead of integrated

into one system. More critically, despite the Air Cargo Program, the Alien Flight Student Program, HAZMAT programs, passenger screening, and other modern security-related programs coming from the Transportation Security Administration (TSA) that focus on the philosophy of "layers of security," there is no internal error reporting system or real-time alert program in place at U.S. airports. This situation has increased the government's workload simply because information about possible hazards and threats is not compiled into prioritized data banks up front by airports. Likewise, airport workers and passengers can not benefit from a risk-free environment without the implementation of an early warning mechanism, which system safety management is encouraging. In some cases, although airports might have had a security system, the functionality and benefits of the threat reporting system were not explained well enough to employees, and this resulted in incomplete information collection and system inaccuracy. These details reveal an opportunity for improvement and suggest a more comprehensive, user-friendly, and dynamic airport security management model.

## FAA AC 120–92 and AC 107–1

In 1972, the FAA published its *Advisory Circular (AC) 107–1 Aviation Security—Airport*. This circular recommends that airports comply with FAA Federal Aviation Regulation (FAR) 107 security requirements with regard to personnel, identifications, authority, signs, trainings, audit, security areas, and so on. The purpose of AC 107–1 is to provide guidelines for an airport security program and to "describe minimum acceptable standards for: (a) preparation of a master security plan, (b) establishing and maintaining a suitable authorized persons identification program, and (c) establishing and maintaining an adequate identification system for certain ground vehicles."[7] However, there is no detailed procedure for filing a threat report; and therefore no proactive airport threat analysis program could be set up.

In 2006, in view of the increasingly recognized merits of using system safety management in aviation safety, the FAA published its *Advisory Circular (AC 120–92) Introduction to Safety Management Systems for Air Operators* to meet two goals: (1) introducing the concept of a safety management system (SMS) to air transportation service providers, and (2) providing air carriers and airports with a guideline for an SMS. The purposes of this advisory circular focus on (1) safety management (risk management and safety assurance using quality management techniques, and a systemic approach to safety management), and (2) safety culture (the human-centered psychological, behavioral, and organizational elements).[8] Using safety risk management and safety assurance to manage safety in this publication is sound and plausible. However, the model embracing the risk matrix given by the FAA lacks specific details: first, the report's format is not user-friendly, which creates confusion about the proposed error management model; second, system safety tools like fault tree analysis (FTA) and operations and support hazard analysis (O&SHA)

should have been included in this guideline so that aviation industry could have a better picture of a true, proactive SMS.

### MIL-STD 882

To detect potential hazards, the FAA and TSA currently recommend risk management programs, which shed light on the applicability of a system safety concept. The original *Standard Practice for System Safety* (MIL-STD-882A, published in 1969) helps aircraft and aerospace engineers to better design products without utilizing the expensive fly-fix-fly doctrine embraced by the U.S. military, especially in the early project teams of X-planes before the end of World War II. After 1969, the U.S. Air Force and NASA both realized that MIL-STD-882 was extremely helpful in reducing a hardware system's causal failures, both active and latent.[9]

### Safety Theories

The security net for the air transportation system is rarely breached by a singular hazardous factor or an isolated risk.[10] When an aircraft hijacking occurs, it reveals the total failure of the layered security system. This can be examined by traditional safety models such as 5-M factors, the Swiss Cheese model, the Domino effect, the SHELL model, chain of events, and related safety analysis devices. Therefore, the concept of multifactor *causes event* ($X_s$ Y), where multiple causes contribute to the accident, is not a contentious issue. The cause, X, could be identified as a violation, distraction, complacency, carelessness, recklessness, fatigue, poor situational awareness, and other mechanical or human deficiencies. Although each is considered to be one security element/layer, there are some precursors to the so-called single element failure. For instance, the cause of the accident involving Comair Flight 5191 (initiating takeoff on the wrong runway) could be categorized as human error but may include miscommunication, situational awareness, crew resource management, flight training, ATC's complacency, or other latent preconditions. Nevertheless, the most reasonable question is: Why did human error (error involving pilots or the air traffic controller) occur in the first place? Was it due to a lack of training, personal problems, health, shortage of staff, sociopsychological status, or carelessness, or was it simply an intentional act?

### Organizational Factor

Problems with airport management can also endanger security. In 1997, James Reason published *Managing the Risk of Organizational Accidents*, showing that people make mistakes no matter what their intentions are. Reason categorized human behavior into three subgroups: (1) skill-based behavior (SB), (2) rule-based behavior (RB), and (3) knowledge-based behavior (KB). To identify potential errors hidden in the dark corners of a given management

**Figure 6.1**
**The Correlation Among 3Ps**


system, Reason suggested the examination of salient problems using three dimensions: (1) personnel: a worker is an agent of a system; (2) engineering: statistical prediction; and (3) organizational: various management segments of an organization are responsible for safety.[11] These three dimensions intertwine; for example, the organizational model controls the personnel and engineering models. Thus, understanding an organizational accident is critical in ensuring security performance. For instance, a security problem could occur when there is a breakdown within a hierarchical management system, in particular, when a safety management structure is ill-formed and allows threats to penetrate.[12]

### Policy, Procedure, and Performance

In his book, *Safety and Health: Management Planning*, and his paper, "Three Ps in Safety: Policies, Procedures, and Performance," Ted Ferry emphasized how essential it is to set up a policy so that procedure is created and performance is measured.[13] Moreover, the 3Ps concept is not a linear process but a recursive and cyclic activity linking policies, procedures, and performance into one frame (see Figure 6.1). If any segment of a management system is lacking, the entire safety/security loop will collapse and the program will fail. Clearly, setting policy is urgent and should first be done by the government. This concept has been echoed by Wells, who states that "Policy is usually referenced in the early part of all plans."[14] However, in today's aviation industry, establishing a new policy is not only unwelcome but it could also be extremely time consuming without knowledge of immediate or known threats.[15] With this in mind, an alternative policy should be introduced. An effective and efficient threat-prevention model is most cost effective when aviation workers can easily go through its guidelines, provide comments, gain recognition, be protected, and ultimately make aviation security flawless.

## DEFINITIONS OF SYSTEM SAFETY TECHNIQUES

To proactively identify potential threats leading to security breakdown, MIL-STD-882D suggests several techniques that security experts can apply.

Although this study demonstrates the basic application of only two tools, FTA and O&SHA, experts could expand their skills by applying other techniques that are recommended below. The system safety techniques described here are those most commonly used by system safety engineers.

*Job safety analysis (JSA).* "A generalized examination of the tasks associated with the performance of a given job and an evaluation of the hazards associated with those tasks and the controls used to prevent or reduce exposure to those hazards. Usually performed by the responsible supervisor for that job and used primarily to train and orient new employees."[16]

*Operating and support hazard analysis (O&SHA).* "Performed to identify and evaluate operational-type hazards. It is based upon detailed design information and is an evaluation of operational tasks and procedures. It considers human system integration factors such as human error, human task overload, cognitive misconception, [and] the effect on humans of hardware failure."[17]

*Fault tree analysis (FTA).* "Systems analysis technique used to determine the root causes and probability of occurrence of a specified undesired event. A fault tree analysis is a model that logically and graphically represents the various combinations of possible events, faulty and normal, occurring in a system that lead to a previously identified hazard or undesired event."[18]

*Failure mode and effective criticality analysis (FMECA).* "Tool for evaluating the effect(s) of potential failure modes of subsystems, assemblies, components or functions. It is primarily a reliability tool to identify failure modes that would adversely affect overall system reliability. FMECA has the capability to include failure rates for each failure mode in order to achieve a quantitative probabilistic analysis."[19]

*Management oversight and risk tree (MORT).* "MORT is an analytical technique for identifying safety-related oversights, errors, and/or omissions that lead to the occurrence of a mishap."[20] Regardless of the informed system risks, the focus of this model is on management's omissions or less than adequate (LTA) performance.

## RECENT STUDIES APPLYING SYSTEM SAFETY MANAGEMENT

In addition to aerospace engineering, applications of system safety techniques and concepts have been useful in the field of medicine. For instance, in the medical engineering industry, Robert L. Helmreich, an aviation safety legend now dedicated to the medical field, advocated the use of system safety's error management concept in medical practice.[21] In 1999, another medical device assessment was carried out by Manon Croheecke and his research associates, advocating FMEA.[22] William Hyman utilized the leading tool of system safety, the FTA, in evaluating potential hazards associated with newly developed medical equipment before moving toward the production-manufacturing phase in the device's life cycle.[23]

In aviation safety, the U.S. Air Force launched risk management and causal study to improve pilot training procedures. Diehl's cross-referenced analysis of 208 military accidents discovered the breakdown of the cockpit

communication and team performance known as crew coordination.[24] This communication breakdown led to military aircraft mishaps. Diehl's study applied an ergonomic human-face interface (an O&SHA concept) and suggested a modification of the cockpit layout of the Cessna Citation used by U.S. Air Force officers. This study linked accident investigation, hazard identification, and basic descriptive analysis to human factor and crew resource management (CRM) training and later provided an exemplary study to academia. Lu, Przetak, and Wetmore conducted a similar causal study using statistical analysis to discover the causes of nonflight accidents for FAR Part 121, on U.S.-based carriers yielding another view to measure aviation safety.[25]

A study by Thom and Clariett, published in *Collegiate Aviation Review* (*CAR*), focused on an essential section of system safety, the applicability of job safety analysis (JSA) and task analysis.[26] In their study, JSA was closely interpreted and the layout of the human-machine interface was emphasized. Using the risk homeostasis theory (RHT) of human dynamic behavior to study risk taking, Thom and Clariett helped identify potential hazards involving hangar, factory, or student workers, both within and outside the aviation industry. This study was of great interest to a safer aviation community.

Luis Bastos presented a risk management model based on feedback from 14 Code of Federal Regulations (14CFR) Part 135 pilots as well as the National Transportation Safety Board's (NTSB) accident data.[27] Bastos discovered that accidents are usually caused by multiple safety factors, which agrees with Reason's theory of organizational accidents. Since potential risk exists, reducing risk probability (Rp) and risk severity (Rs) upstream is essentially targeted. Bastos also proposed a risk management model similar to MIL-STD-882D Risk Matrix model (see Table 6.2).

Lu, Wetmore, and Przetak demonstrated the application of FTA in promoting safety performance.[28] Their analysis indicated that FTA, based on a risk tree analysis and a statistical forecast, can help proactively prevent undesired events or stop events from occurring. According to their study, FTA helps organizations such as the government or airlines to effectively and promptly identify accident postulates and to trigger the implementation of strategic safety prevention programs from the bottom up (upstream) (see Figure 6.2). Based on the FTA hierarchical block-diagram associated with the use of Boolean gates, any of the root factors on the bottom level can form a cut-set or a failure-chain contributing to an accident or system failure (a top event). Hence, compressing or eliminating the failure probability of root factors from the lowest level of the risk tree also identifies a training priority. A statistical simulation based on the required risk calculation concerning hazard probability and severity is shown in Figure 6.3. With the computerized-system design, a real-time, dynamic system safety model is possible.

Although the FAA realized the value of collecting data and monitoring trends, the FTA model provides a dynamic system with which to identify

**Table 6.2**
**Risk Matrix, Severity & Probability**

| Risk Matrix* *Frequency* | *Catastrophic (I)* | *Critical (II)* | *Marginal (III)* | *Negligible (IV)* |
|---|---|---|---|---|
| Frequent (A) | 1A | 2A | 3A | 4A |
| Probable (B) | 1B | 2B | *3B* | *4B* |
| Occasional (C) | 1C | *2C* | *3C* | 4C |
| Remote (D) | *1D* | 2D | 3D | 4D |
| Impossible (E) | 1E | 2E | 3E | 4E |

* A "Risk" falling into this category [1A, 2A, 3A, 4A, 1B, 2B, 1C] is "Unacceptable"
A "Risk" falling into this category [1D, 2C, 3B, 3C, 4B] is "Undesirable"
A "Risk" falling into this category [1E, 2D, 2E, 3D, 4C] is "Acceptable With Review"
A "Risk" falling into this category [3E, 4D, 4E] is "Acceptable Without Review"
The determination of "Unacceptable," "Undesirable," "Acceptable With Review," or "Acceptable without Review" is based on a System Safety analyst's subjective decision-making based on the onsite situation from case to case.

Risk Severity (S) and Probability (P) are defined as:

| Risk Severity (S) *Description* | *Category* | *Mishap Definition* |
|---|---|---|
| Catastrophic | I | Death or system loss/failure |
| Critical | II | Severity injury, occupational illness, or system damage |
| Marginal | III | Minor injury, occupational illness, or system damage |
| Negligible | IV | Other |

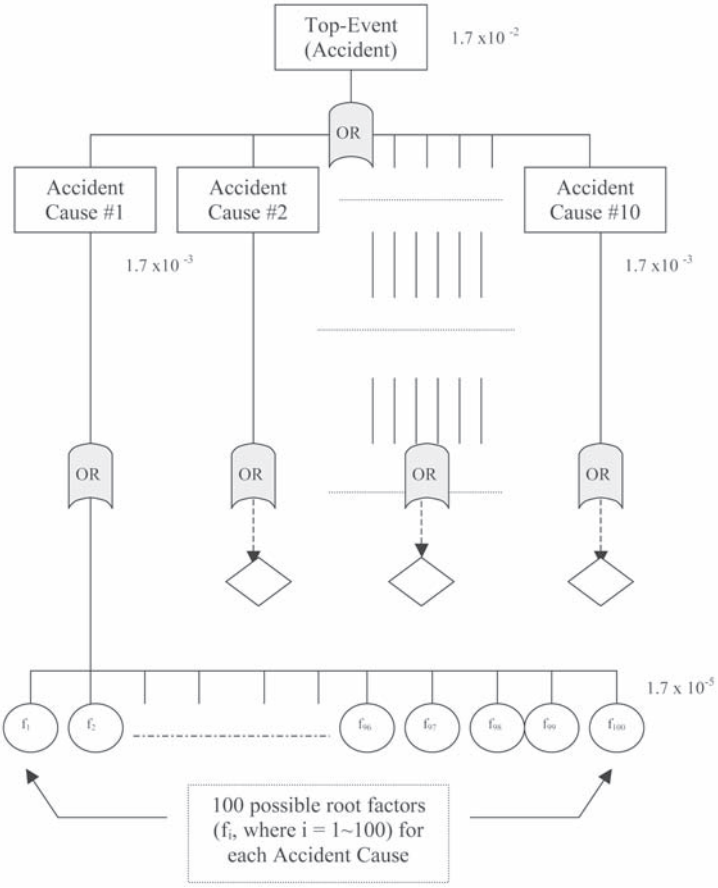
| Risk Probability (P) *Description* | *Level* | *Mishap Definition* |
|---|---|---|
| Frequent | A | Likely to occur frequently |
| Probable | B | Will occur several times during the life of an item |
| Occasional | C | Likely to occur sometimes in the life of an item |
| Remote | D | Unlikely, but may possibly occur in life of an item |
| Impossible | E | So unlikely, assumed that hazard will not occur at all |

*Source:* DOD MIL-STD-882B System Safety Program Requirements (1984)

hazards and to assign risk values using Bayesian analysis. Bayesian inference provides a quantitative framework for the iterative process of integrating information into useful models. It is the essence of predicting and therefore preventing accidents. The model is the keystone of safety management but has apparently been overlooked by the FAA.

Captain Luis Lupolis of the Brazilian Air Force achieved the application of organizational accident theory in July 2006.[29] His research hypothesized that

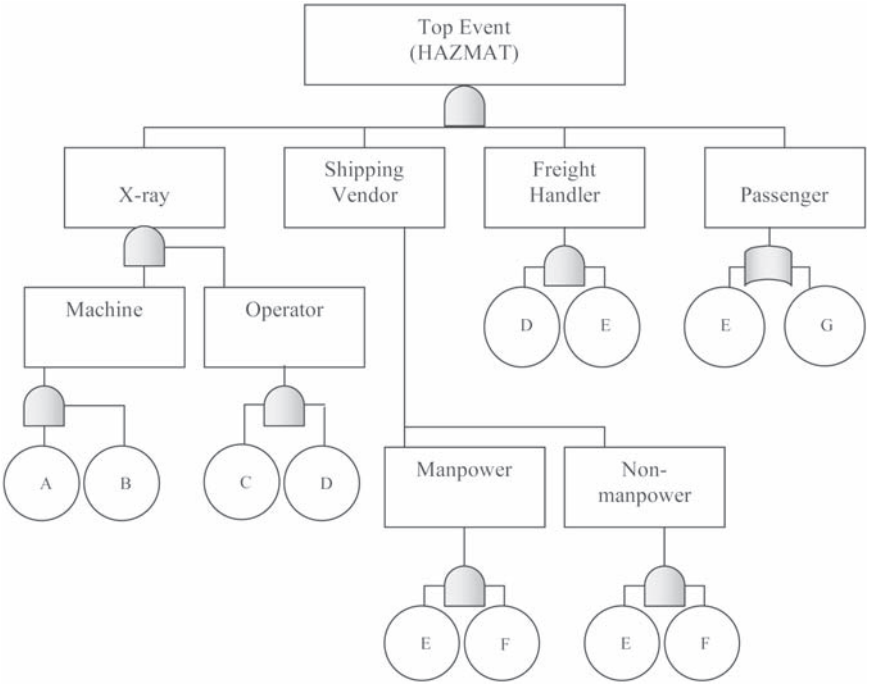
**Figure 6.2**
**Simulating the Probability of the Top-Level Event**




*Source:* Chien-sung Lu, Michael Wetmore & Robert Przetak. Another approach to enhance airline safety: Using System Safety techniques. *Journal of Air Transportation* 11, no. 2 (2006): 113–139.

deficient decision-making processes and poor organizational management by top-ranking officers could result in aircraft mishaps. Lupolis revealed, via self-administered surveys, that Brazilian Air Force squadron commanders have a limited knowledge of advanced safety theories like organizational accident theory, but they are all committed to operational safety. Thus, a more advanced safety education for top management is needed. Furthermore, although the top-ranking officers are aware of their lack of knowledge of a reliable decision-making process, they still use empirical means to make safety decisions. Capt. Lupolis recommends further research on the rationale these officers use to make safety decisions.

**Figure 6.3**
**Managing a Security Event**



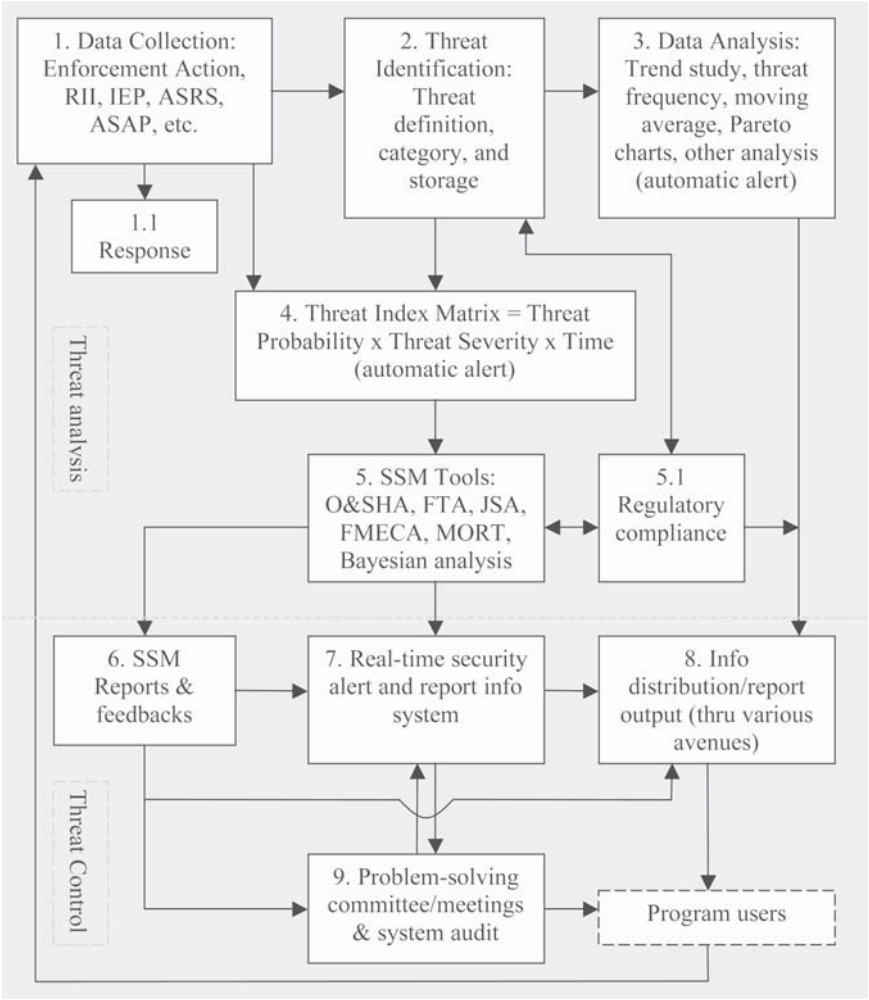

## RESEARCH FOCUS

Apparently, utilizing system safety in relation to flight safety has been recognized as useful. Yet in aviation security, it is new, innovative, and challenging. Therefore a well-designed aviation security management model prepared for airport security would be beneficial. The proposed security model meets the following criteria: (1) it is administratively practical; (2) its basis of measurement is quantifiable for qualitative analysis; (3) a valid measurement presents what it is supposed to represent; (4) the system safety tools utilized are understandable, user-friendly, and sensitive to situational change; (5) the security data is presented in a real-time reflection/alert fashion; and (6) the results are distributable and disseminated.[30]

## PROPOSED AVIATION SECURITY MANAGEMENT MODEL (ASMM)

The proposed aviation security management model (ASMM) contains nine major steps: (1) data collection, (2) threat identification, (3) data analysis, (4) threat matrix calculation and response, (5) system safety tools implementation and regulatory compliance, (6) reports and feedback, (7) result

**Figure 6.4**
**The Risk Analysis Process**




monitoring, (8) information distribution, and (9) problem-solving meetings (see Figure 6.4).

*Data collection.* Hazardous data can be retrieved from the current ongoing threat/hazard reporting programs such as the airport Enforcement Action database, TSA incident reports, runway incursion incidents (RII), the Aviation Safety Action Program (ASAP), the airport Internal Evaluation Program (IEP), the Aviation Safety Reporting System (ASRS), and others. The data on potential threats can be (1) reported by employees, (2) downloaded from self-maintained databases, or (3) obtained from government's documentary reviews. A suggestion with regard to this data collection phase is that the data

reporting mechanism should be ready for and open to all workers, allowing security project managers to receive genuine information from field specialists or anyone who would like to contribute. This collection must meet several requirements in order to encourage contributions: it must be (1) penalty-free, (2) anonymous, (3) confidential, (4) easy to report, (5) open-door in nature, and (6) useful for feedback and solutions.

*Threat identification.* The purpose of threat identification is twofold: threat definition and categorization. The criticality of threat identification focuses on the review of reports from frontline experts to see if it is a reportable threat (not blackmail or the like) and if it requires prompt internal analysis. In addition, collected data should be categorized and prepared for an immediate analysis and threat study.

*Data analysis.* This is the first analytical output of a review focused on identifying and reporting threat prioritization associated with a quick solution or immediate automatic security alert. Data analysis should contain, but not be limited to, some basic hazardous information, such as a trend study, hazard ranking, and preliminary reports provided during a specific time. Regulatory compliance must be reviewed, and this part of the information can be distributed to employees for self-alert and as weekly safety/security brief/educational materials.

*Threat matrix calculation and response.* During this phase of ASMM, the formation of a threat index matrix (TIX) can be generated. An example provided (see Table 6.3) suggests that the TIX uses addition instead of multiplication in order to provide an easier means of threat calculation and interpretation using figures ranging between 2 and 10, the higher number being better.

Meanwhile, a color-coded numerical index matrix indicates the risk level of a situation reported by employees. In this proposed model, the risk index 1 to approximately 4 is qualitatively defined as an "Emergency" threat that needs response or solution quickly. The risk index 6~12 indicates a "Cautious" situation needing a fast review and resolution, for which more information and analysis may be needed to determine the level of risk over the entire security system. Finally, the risk index 15~24 represents a "Supervisory" case and the

**Table 6.3**
**Threat Index Matrix (TIX)**

| | *Threat Probability* | | | | | |
|---|---|---|---|---|---|---|
| | *Impossible* | *Improbable* | *Remote* | *Occasional* | *Probable* | *Frequent* |
| *Threat severity* | *6* | *5* | *4* | *3* | *2* | *1* |
| Negligible 4 | *24* | *20* | *16* | *12* | *8* | *4* |
| Marginal 3 | *18* | *15* | *12* | *9* | *6* | *3* |
| Critical 2 | *12* | *10* | *8* | *6* | *4* | *2* |
| Catastrophic 1 | *6* | *5* | *4* | *3* | *2* | *1* |

** Index note: 1 ~ 4 Emergency 6 ~ 12 Cautious 15 ~ 24 Supervisory*

reported threat needs continuous measurement in the future. In the matrix for the airport industry, although the threat probability is extremely low ("Impossible" = 6), any possible fatality ("Catastrophe" = 1) is unacceptable, thus it is also categorized as "Cautious" instead of "Supervisory." Meanwhile, a "Frequent" rating (1) of threat probability with a "Negligible" (4) threat severity is also unacceptable because the threat could immediately be mitigated at a very low cost (i.e., a passenger's nonintentional violation of or carelessness with regard to a security procedure). Otherwise, threat accumulation (i.e., overlook) may lead to a larger scale of damage (i.e., from an intentional act, a lack of required HAZMAT training, or security breach to worker injury or facility damage). Equally important, the threat probability levels should be manipulated based on an individual airport's operational nature.

*System safety tools implementation and regulatory compliance.* This phase processes the information/reports and receives the hazard probability from the previous processing stage. The exemplary reporting forms using FTA and O&SHA (see Table 6.4) provide a conceptual demonstration. The real value of this phase is the application of system safety tools to conduct a detailed threat-incident-accident analysis and suggest countermeasures for new employee orientations, routine safety education, recurrent training, and an accident-prevention course based on regulatory requirements and identified safety gaps within the operational system.

*Reports and feedback.* The purpose of the investigation is to identify the problems, provide safety measures, and prevent similar problems from happening again. With this in mind, the analytical reports will be sent to a safety committee for review if the calculation of the threat index indicates a need. Also, the result and resolution need to be distributed to the submitters, if known. Otherwise, it should be posted on a security bulletin board or to a monitoring system for public review. A threat tracking system is equally important for two reasons: (1) it will help the safety manager identify the status of a threat report, and (2) it will show threat submitters the importance of their input and further motivate their participation.

*Real-time security alert.* The qualitative threat alert index of this proposed ASMM provides a visible image to safety managers or system users who need up-to-date information for prompt understanding. The author suggests a color-coded (at least three colors: red, yellow, and green, or more) system design for threat alert and identification. To accomplish this goal, sufficient digital databases and computerized systems are both critical.

*Information distribution.* This process should inform all employees about the status of the security level, as well as about cases identified by employees, peer airports, trade associations, or governments, since a threat to security at one airport would quickly raise concerns for other airports. Information distribution is accomplished by utilizing several formats such as e-mail, auto-voicemail, internal circulation, flight crew briefings, ground crew discussions, maintenance safety notices, recurrent/routine training, or airport notice to airmen (NOTAMs).

**Table 6.4**
**Conceptual O&SHA Analysis**

| *Item* | *Procedural tasks* | *Hazard condition* | *Cause* | *Effect* | *Risk level, criticality index* | *Assessment* | *Recommendation* |
|---|---|---|---|---|---|---|---|
| 1 | Luggage Ninspection | HAZMAT | Lack of training | Fire alert on board | 4(Emergency) | Inspector error | Reassurance and training |
| 2 | Luggage inspection | HAZMAT | Carelessness | Onboard fire | 3 (Emergency) | Inspector error | Reassurance and training |
| 3 | Luggage inspection | HAZMAT | Complacency | Freight damage | 7 (Supervisory) | Handler error | Reassurance and training |
| 4 | Luggage handling | HAZMAT | Carelessness | Toxic fumes | 2 (Emergency) | Handler error | Special tag, reassurance and special HAZMAT training |
| 5 | Luggage handling | HAZMAT | Ignorance | Dangerous weapon | 2 (Emergency) | Passenger error | Prohibited items reminder, X-ray, and reassurance |
| 6 | Luggage handling | Animal (such as iguana, dart frog, etc.) | Lack of knowledge | Worker injury | 5 (Cautious) | Handler error | Reassurance and training |

*Note:* Items are based on specific situations and can be expanded. O&SHA focuses on the problems of operator and operational interface. The threat index 2~4 means it is an "Emergency" case and needs an immediate response or solution. The threat index 5 ~7 indicates a "Cautious" situation that needs a fast review and resolution; more information and analysis may be needed to determine the level of threat eroding the entire operational system. The threat index 8 ~10 represents a "Supervisory" case and the reported hazard needs continuous measurement in the future.

*Problem-solving meeting and system audit.* Members of the safety committee should receive routinely, at least daily, a risk analysis and have the opportunity to provide comments and recommendations to upper management for further decision-making reviews (action or nonaction), if necessary. The safety committee generates solutions and mitigates potential hazards based on the magnitude of a risk. Frontline managers, employees, or union representatives should be invited to safety meetings, focus group discussions, and system audits periodically and be allowed to suggest training or resolutions because of their involvement in daily activities, their observations, and their career specialty.

## CONCLUSION: THE UPCOMING CHALLENGE

Although we "cannot protect every person against every risk at every moment in every place . . . in order to protect our country and defend our freedoms, we must continue to focus resources on the areas that pose the greatest risk."[31] We have recognized the value of the system safety concept to airport security (in terms of threat report, identification, risk analysis, risk matrix calculation, system safety analysis, safety countermeasures, performance assessments, and documentation). An airport security program could be more proactive and effective if risk analysis techniques such as O&SHA, FTA, FMECA, JSA, and MORT are used.

Over the last seven years, the Government Accountability Office (GAO)[32] has reported that using system safety would be beneficial to the aviation industry including airlines, airports, and FBOs. Most importantly, the airline industry and the FAA have both remarked that a sufficient database is critical to a mature threat prediction, mishap mitigation, passenger protection, and national security. With this in mind, the reluctance to use new analytical techniques by the aviation industry is dangerous to its loyal customers. The ASMM specifically follows a systemic and scientific way to troubleshoot a given system by identifying potential risks that endanger the whole air transportation system within the error-latent environment.

This study provides a comprehensive safety management model, namely ASMM, which combines error management, system safety techniques and MIL-STD-882D to form a streamlined risk analysis and risk control program for easier use and safety reporting. An exemplary format of FTA and O&SHA was applied to demonstrate the fundamental application of this proposed model. Because this is a conceptual safety management model, enthusiasts can freely and flexibly revise this model using different system safety techniques that are based on the characteristics of a unique hazardous environment such as those involving maintenance safety, flight safety, cabin safety, ground operations safety, air traffic control, and others. Launching an internal hazard reporting system is the key to a successful safety program and a vital safety culture.

## FUTURE STUDIES

Using computers to quickly solve problems is the future. Advocating a follow-up study implementing FTA, FMECA, or MORT by designing computerized statistical analysis and risk prioritization will improve the discipline of threat prediction and generate an automatic auditing or alert model for a system's real-time operational safety. Another follow-up study should focus on the performance and usefulness of the proposed ASMM as tested by airports, airlines and FBOs.

## NOTES

1. National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, authorized ed. (New York: W.W. Norton, July 2004).
2. National Commission on Terrorist Attacks Upon the United States (New York: W.W. Norton, 2006).
3. FAA, *FAA Order 8040–4 Safety Risk Management* (Washington, DC: FAA, 1996).
4. Ibid.
5. Chien-tsung Lu, Michael Wetmore, and Robert Przetak, "Another approach to enhance airline safety: Using System Safety Techniques," *Journal of Air Transportation* 11, no. 2 (2006): 113–39.
6. Chien-tsung Lu, Robert Przetak, and Michael Wetmore, "Discovering the Non-flight Hazards and Suggesting a Safety Training Model," *International Journal of Applied Aviation Science* 5, no .1 (June 2005): 135–52.
7. FAA, *Advisory Circular (AC) 107–1 Aviation Security—Airport* (Washington, DC: FAA, 1972).
8. FAA, *AC 120–92 Introduction to Safety Management Systems for Air Operators* (Washington, DC: FAA, 2006).
9. Department of Defense (DoD), *MIL-STD-882D: Standard Practice for System Safety* (Washington, DC: FAA, 2000).
10. Dan Petersen, *Safety Management: A Human Approach*, 2nd ed. (Goshen, NY: Aloray, 1988); Alexander Wells and Clarence Rodrigues, *Commercial Aviation Safety*, 4th ed. (New York: McGraw Hill, 2004); Richard H. Wood, *Aviation Safety Programs: A Management Handbook*, 3rd ed. (Englewood, CO: Jeppesen, 2003).
11. James Reason, *Managing the Risks of Organizational Accidents* (Burlington, VT: Ashgate, 1997).
12. Ibid.
13. Terry S. Ferry, *Safety and Health: Management Planning* (New York: Van Nostrand Reinhold, 1990); Terry S. Ferry, "Three Ps in Safety: Policy, Procedures, and Performance," *Professional Safety* 51, no. 6 (2006): 48–52.
14. Alexander. T. Wells, *Commercial Aviation Safety*, 3rd ed. (New York: McGraw Hill, 2002), 234.
15. Chien-tsung Lu, "Discovering the Regulatory Considerations of the Federal Aviation Administration: Interviewing the Aviation Rulemaking Advisory Committee," *Journal of Air Transportation*, 10, no. 3 (2005): 32–48.

16. Jeffrey W. Vincoli, *Basic Guide to System Safety*, 2nd ed. (Hoboken, NJ: Wiley & Sons, 2006), 206.

17. Cliffton A. Ericson, III, *Hazard Analysis Techniques for System Safety* (Hoboken, NJ: Wiley & Sons, 2005), 476.

18. Ibid., 472.

19. Ibid., 471.

20. Ibid., 423.

21. Robert L. Helmreich, "On Error Management: Lessons from Aviation," *British Medical Journal* 320, no. 7237 (2000): 781–85.

22. Manon Croheecke, Rachel Mak, and Mas B.A.J. de Mol, "Failure Mode and Effect Analysis and Fault Tree Analysis in the Use of the CoaguChek® Prothrombin Time System," *International Journal of Risk in Medicine* 12, (1999): 173–79.

23. William A. Hyman, "Generic Fault Tree for Medical Device Error," *Journal of Clinic Engineering* 27, no. 1 (2002): 134–40.

24. Alan E. Diehl, "Human Performance and Systems Safety Considerations in Aviation Mishaps," *International Journal of Aviation Psychology* 1, no. 2 (1991): 97–106.

25. James Thom and D. R. Clariett, "A Structured Methodology for Adjusting Perceived Risk," *Collegiate Aviation Review* 22, no. 1 (2004): 97–121.

26. Luis Lupolis and M. Bastos, "Risk Management Model for On-Demand Part 135 (Air Taxi) Operator" (master's thesis, University of Central Missouri, 2005).

27. Luis C. Lupolis, "Discovering the Brazilian Air Force Squadron Commanders' Perceptions Regarding Organizational Accidents" (master's thesis, University of Central Missouri, 2006).

28. U.S. Army, *Safety Program* (Washington, DC: Department of the Army, 1972).

29. Ibid.

30. Michael Chertoff, "There Is No Perfect Security," *Wall Street Security—Eastern Edition* 247 (2006): 22A.

31. USGAO, *System Safety Approach Needs Further Integration into the FAA's Oversight of Airlines* (Washington, DC: USGAO, 2005).

32. USGAO, *FAA's Safety Oversight System Is Effective but Could Benefit from Better Evaluation of Its Programs' Performance* (Washington, DC: USGAO, 2005).

# CHAPTER 7

# Growing Pains at the Transportation Security Administration

*Jeffrey Ian Ross*

Since September 11, 2001, the United States has significantly revamped the ways and means used to provide and ensure national security against terrorist attacks. Key legislation included the PATRIOT Act (signed October 2001) and its revision, the USA PATRIOT Improvement and Reauthorization Act of 2005 (passed March 2006), which created new rules on domestic surveillance and detention; the Homeland Security Act (signed November 2002), which established the Department of Homeland Security (DHS); and the Aviation and Transportation Security Act (passed November 2001), which created the Transportation Security Administration (TSA).[1]

Given the nature of the September 11 attacks, coupled with the failure of the then current safety measures to detect and/or deter the 19 al Qaeda terrorists, it seems logical that there would be increased demands for changes in the way the United States' transportation industry conducts its business. Congress has given the TSA responsibility for supervising all modes of travel in the United States. The TSA is, further, charged with implementing relevant security changes. In general, "The primary goals of the new TSA were to increase the effectiveness and efficiency of (1) identifying passengers who were potential threats and (2) screening passengers and luggage for potential weapons and explosives."[2]

Unless they work for the federal government agencies and/or as a first responder for either state or local government, most Americans are probably not directly or physically affected by the PATRIOT and Homeland Security acts. On the other hand, the average person traveling on a commercial airliner will be directly affected by changes brought about because of the establishment of the TSA.

Special thanks to Richard Hogan and Dawn L. Rothe for comments.

The TSA has been singled out for intense scrutiny, in large measure because of the inconveniences passengers must now endure when boarding, deplaning, and traveling on commercial airlines inside, and to and from, the United States. In addition to the restrictions and other measures air passengers encounter, there have been increased citizen criticisms surrounding the privacy rights that are curtailed every time they take a plane trip. These difficulties are not felt just by consumers but also by airline personnel and TSA workers who have also expressed their discontent. Consequently, the TSA has been singled out for intense scrutiny. However, it is not my intent to gauge how widespread these criticisms are, nor to undervalue the significant contributions that TSA personnel have made in protecting America (e.g., intercepting weapons, actual or potential), nor to downplay the real difficulties experienced by TSA officers (especially when dealing with rude and surly rude passengers), but simply to document the most salient complaints and some of the unintended consequences.

In order to contextualize the growth and development of the controversial security-related TSA policies and practices over the past six years, this chapter follows a relatively simple chronology, tracing the events that passengers might experience from getting to an airport to deplaning. It then briefly reviews the different kinds of theories of bureaucratic decision making that are applied to policy making, and concludes that to all intents and purposes, the TSA has been operating on an incremental decision-making basis.

## THE TSA AND AVIATION SECURITY IN THE POST–SEPTEMBER 11 ERA

There are numerous vulnerabilities in airline and airport safety that necessitate safeguards. Concerns about our country's air safety as a result of criminals, hijackers, and terrorists did not begin with September 11. There is a long history of individuals, traditional criminals, and terrorists commandeering passenger airplanes, and/or placing explosive devices on planes.[3] Naturally, there has been a considerable amount of scholarly research that has examined these incidents and the government and industry responses to them.

Since September 11, the passenger airline industry has focused its security efforts on four areas: "Airport security; passenger identification and screening; airport proximity security: aircraft security during take off and landings, [and] in-flight security."[4] In short, since September 11, in most of the large airports in the United States, security procedures have become more rigorous. The following sections point out these areas of concern and the numerous inconveniences passengers have experienced as a result.

### Dropping Off and Picking Up Passengers

Depending on the airport, picking up and dropping off passengers by car is now more inconvenient, and sometimes a more time-consuming and

expensive venture than pre–September 11. Those wishing to pick up passengers who are arriving or drop off passengers who are departing are no longer allowed to stand (i.e., stay in the vehicle with the motor running), wait, or park their cars (i.e., leave the vehicle unattended). Most big-city airports (in Chicago, Los Angeles, New York, and elsewhere) use local police, state police/troopers, or airport police to constantly and vigorously monitor the traffic and dissuade drivers from waiting for passengers at the curbside by threatening ticketing or towing. Some airport authorities, recognizing the inconvenience of these practices, have negotiated with companies that have leased parking facilities to let drivers park free for the first half hour. Other airport authorities have established or constructed cell-phone waiting areas, where drivers can temporarily park their cars and wait (typically up to an hour), until their loved ones, friends, colleagues, or clients call to be picked up at a designated place. Negotiating the dropping off of a passenger is only the beginning. The inconveniences for travelers do not appreciably diminish from curbside to ticketing counter (another post–September 11 security point).

### At the Ticketing Counter

Despite the advent of electronic ticketing, airline passengers are now required to check in at least an hour before their plane takes off for domestic flights and two hours for international flights. Unfortunately this practice can lead to inordinately long wait times. This is especially frustrating given the fact that in the past few years passengers have also witnessed significant increases in the number of late departures and/or cancellations. Once at the ticket counter, passengers must show more forms of identification and are still asked a number of security questions by airline personnel, such as, "Has anyone helped you pack your bag?" and "Has your bag been in your possession at all times?" These are not foolproof questions, as passengers can easily lie and there is little that airline personnel can do to detect this.

Because of increased baggage restrictions and screenings, checking baggage is more onerous. Airlines now restrict carry-on luggage to one item, either to increase their revenue by charging for baggage that passengers would in the past have normally taken as carry-on, or to minimize the items that could possibly be carried on to the plane and used as weapons. In another new measure, baggage handlers and screeners have been "federalized" and integrated into the TSA. In general, passenger and baggage screeners (there are now some 30,000 of them) are doing a more thorough job, including testing ticketed passengers' personal effects for gunpowder residue, using equipment with increased metal sensitivity, and making regular and random searches. In short, those responsible for baggage handling and inspection are said to be better trained and more experienced than pre–September 11 employees performing similar functions.

## Security Processes before Entering a Terminal

Many people, from passengers to TSA workers, believe that the procedures for screening ticketed customers range somewhere along a scale from pointless to ridiculous.

Procedures such as having 80-year-old women turn over nail files or treating quadriplegics as would-be terrorists simply to demonstrate impartiality in screening annoy passengers far more than they convey any sense of safety. Meanwhile, there appears to be considerable inconsistency with respect to items that are considered to be potential weapons, for example, not allowing nail clippers but permitting disposable razors, or not being able to take cigarette lighters on board, but being permitted to take three boxes of matches. Documentary film director Michael Moore captured these ironies well in his controversial 2004 movie *Fahrenheit 911*, when he showed all the items that could not be brought aboard aircraft and those that were permissible. These contradictions helped to lead to the reversal of the ban on carrying cigarette lighters.[5]

## Passenger Identification

Over the past six years, a number of different passenger prescreening programs have been implemented, often with little success. Many passengers have been unnecessarily searched and delayed because of ethnic profiling, being on watch lists because of certain types of employment, participation in public protests, and previous travel. The secret no-fly list once led to Senator Edward M. Kennedy (D-Mass.) being detained on his regular Washington to Boston flight and again on his attempt to fly back to Boston.

## Baggage Handling and Screening/Clearing Security

Although failures to intercept weapons and properly vet TSA personnel have repeatedly garnered media attention,[6] some of the biggest passenger complaints are connected to the screening procedures they experience while trying to clear security to enter the terminals on the way to their gates. This is usually caused by the increasing number of banned items, and the apparent randomness of decisions connected to specific individuals and items that are subjected to increased security.

In December 2001, Richard Colvin Reid, a British citizen, a recent convert to Islam with nebulous ties to al Qaeda, the terrorist group responsible for the September 11 attack, tried to blow up an American Airlines flight en route from Paris to Miami. The primitive bomb was located in his shoes. Only when passengers noticed that he was trying to light his shoes was he overpowered and the bomb discovered. This led to a revision of policies such that airline passengers are now required to take off their shoes while going through a gate check and have them placed on the conveyor belts on their way to the X-ray machines. Then belts were targeted, with the occasional person

seen walking through X-ray scanning devices grasping the waistband of his pants to prevent them from falling down around his shoeless feet. Passengers started to wonder what other kinds of clothing would be next.

Then, in August 2006, it was announced that al Qaeda was experimenting with carrying liquid explosives in water or perfume bottles. Almost immediately, the TSA banned passengers from carrying bottles in excess of four ounces, whether liquids, gels or pastes, in carry-on bags. In September 2006, the TSA lifted its ban on carrying liquids in favor of requiring travelers to carry only "travel-size toiletries (3.4 ounces or less) that fit comfortably in one quart-size, clear plastic, zip-top bag." Predictably, at least in the beginning, bags were not provided to passengers. And when travelers used wrong-size bags they were often chastised by TSA workers. Only later did the TSA or airport authorities start providing the bags. TSA workers who identify passengers carrying prohibited liquids and so on give travelers the opportunity to stow the items in their carry-on bags once the items have been thoroughly screened, but by that time most passengers are in a rush to board their planes, or do not want to incur the extra inconvenience of retrieving their bags, going back to the ticketing counter, and dealing with the airline personnel, and simply agree to have their prohibited items thrown in the garbage.

### Waiting in the Terminal

Since September 11, airports have adopted a "standard concentric circle security design," featuring increased security checkpoints that ticketed passengers and authorized personnel must go through before they are allowed to enter the terminals and gate areas, and eventually board the planes. "Prior to September 11 many airports were designed as mini-shopping centers."[7] Since the new security restrictions were implemented, a number of retail businesses located in the terminals and the parking facilities (usually leased by the airport authorities to private companies) have incurred significant losses in revenue. Some terminals have resembled veritable ghost towns on the American landscape.

### Revised Boarding Procedures

A number of changes have occurred with respect to boarding and onboard procedures as well. Nationwide, when boarding a plane, certain passengers can be taken aside to have their persons and their carry-on items completely searched.

### Onboard Security Processes

In addition, after the September 11 attacks, because of Ronald Reagan National Airport's close proximity to the Pentagon (one of the sites of the September 11 attacks), flights out of this airport were initially suspended,

then scaled back, and sky marshals were placed on all flights in and out of the airport. Moreover, passengers are not allowed to leave their seats for the first half hour after departure from or during the approach to Reagan Airport and nearby Dulles Airport in northern Virginia. In other decisions that were as arbitrary, in December 2003 the Federal Air Marshal Service was transferred from the TSA to the U.S. Bureau of Immigration and Customs Enforcement, and then in 2006 it was returned to the TSA.

Pilots are now allowed to carry guns (under the Federal Flight Deck Officer Program), and cockpit doors have been reinforced. The airlines no longer serve food on so-called short-haul trips; one would assume this last precaution has been introduced because utensils are potential weapons, and because not providing food makes up for the loss of income incurred immediately after September 11.

### Remaining Gaps in Security Provision

Despite the increased security, there is no point-to-point baggage checking. In other words, in many airports once your bag comes off the conveyer belt almost anyone can pick it up. Rarely are airline personnel or security guards in attendance to make sure that the bag you retrieve is yours. And there is criticism of the fact that cargo placed in the airplane's hold is either never screened at all, or not properly screened.

### Formal Responses to the Terrorist Threat: Passenger Identification Systems

One of the preferred measures to dealing with the evolving terrorist threat involves passenger identification systems.

1. CAPPS I. A considerable number of passenger identification procedures have been created that lie outside of the TSA's purview. "Recognizing the need for more effective screening and monitoring of foreign visitors, the United States has new visa requirements, new high-tech passport requirements, and the United States Visitor and Immigration Status Indicator Technology, or US VISIT program."[8] Within the TSA's domain, however, is the Computer Assisted Passenger Pre-screening System, or CAPPS.

As James A. Fagin points out, "In 1996, Northwest Airlines developed a refined system called Computer-Assisted Passenger Prescreening System or CAPPS. The system was operated by the airlines and based on their computer records about passengers. It did not compare passenger names to lists of potential terrorists kept by the State Department. In 1998, other airlines began to use CAPPS, as recommended by the White House Commission on Aviation Safety and Security. In 1999, CAPPS was no longer used to select passengers and their carry-on luggage for additional screening. After September 11 CAPPS was again used to screen passengers for additional security

screening but was still not connected to State Department watch list which has now expanded to include people not necessarily connected to or a part of terrorist organizations. The data used by CAPPS to select passengers for additional security screening did not accurately discriminate between passengers who were potential security risks and those who were not. As a result CAPPS flagged about 50 percent of the passengers for additional security screening in short-haul flights."[9]

2. CAPPS II. CAPPS did not prevent the September 11 attacks, and this fact together with "its poor record in discriminating between potential hijackers and ordinary passengers resulted in Congress authorizing the creation of a new system for determining who should receive additional security screening at airport checkpoints."[10] The new system, named CAPPS II, examines a passenger's travel history to determine if there are any "unusual" patterns. CAPPS "uses airline reservation computers to identify passengers who may pose a higher risk of being terrorists and subjects them to additional scrutiny."[11] CAPPS II "examines 26 aspects of a passenger's travel history," but we don't know exactly what those items are because "details are classified."[12]

Apparently in order to determine the utility of this process, the country's airlines gave the Federal Bureau of Investigation information on 10 million passengers. When news of this came to public attention there were "complaints of privacy violation, lawsuits, and warnings of infringement on privacy rights by various civil rights watchdogs. . . . CAPPS II was criticized as being not only a significant intrusion into privacy rights but also being ineffective in screening for terrorists."[13]

3. Secure Flight. Although CAPPS II was to be introduced in fall 2004, by then the number of problems connected to protecting the privacy of citizens and to "mission creep" forced Congress and the DHS to terminate the program. By that time, the government had already invested over $100 million in it. In its place, the DHS created Secure Flight. "Preliminary details of Secure Flight indicate that it would narrowly focus on screening for potential terrorists and would not screen passengers wanted for violent crimes. Secure Flight would rely primarily on government databases rather than commercial databases for its data mining, but would make some use of the latter."[14]

In 2004, Secure Flight was criticized by the American Civil Liberties Union (ACLU) as a violation of passenger rights, because of the unreasonable search and seizure practices to which it exposed airline passengers. The TSA changed its procedures. "In 2005, Congress prohibited the use of appropriated funds for CAPPS II or its successor, Secure Flight, until the government could certify that privacy requirements were being met, largely related to false positives and the sharing of private information."[15]

4. STAR System. In July 2007, it was announced that the FBI "is developing a computer-profiling system that would enable investigators to target possible terror suspects. . . . The System to Assess Risk, or STAR, assigns risk scores to possible suspects, based on a variety of information, similar to the way a credit bureau assigns a rating based

on a consumer's spending behavior and debt. The program focuses on foreign suspects but also includes data about some U.S. residents. A prototype is expected to be tested this year."[16] "STAR is being developed by the FBI's Foreign Terrorist Tracking Task Force, which tracks suspected terrorists inside the country or as they enter."[17]

5. Other Problematic Passenger Identification Systems. In tandem with the Secure Flight program, the TSA has developed registered traveler programs, better technology to read travel documents, and a no-fly list. The last item has run into severe difficulties. "The no-fly list is the government's secret list of passengers who are not allowed to board a commercial aircraft or who must go through extensive screening before boarding. It differs from the CAPPS-type screening programs in that it uses government databases and intelligence data from federal law enforcement and intelligence agencies to compile a list of names."[18]

## THEORIES OF DECISION MAKING

To better understand how TSA has evolved since its inception, it helps to look at the Agency's decision-making process. There are three major explanations of how people and by extension groups make decisions: rational, incremental, and cognitive. First, *rational* or *intellectual* approaches attempt to make broad-ranging diagnoses. This style of decision making involves obtaining definitions of the situation. Those using this style then attempt to collect a wide range of information. They tap different sources for information to minimize bias. Then they conduct an extensive search for policy options. These decision makers are open to new information, and they evaluate opportunity costs, compare costs and benefits, and estimate the usefulness of options. They choose the options that promise to give them the greatest benefits and the lowest costs. The rational process recognizes that it is difficult and to compare things of different magnitudes and to measure many constructs, and that the process is very time consuming. In reality people, from leaders to workers, have little time to make complicated decisions. Consequently, most people do not routinely engage in this sort of decision making, save for those paid to do it.[19]

The *incremental*, *mechanical*, *or cybernetic* approach involves the consideration of one option at a time.[20] This kind of decision making looks at the first available option that will satisfy the minimum needs. This process is also called *satisficing*. Options only differ to a small degree. This is why decision makers typically rely on standing operating procedures (SOPs). These may be set out in written form or may simply be informally accepted as the product of past experience. SOPs are usually based on trial and error experiences. The decision makers don't analyze, and don't weigh opportunity costs. The cybernetic model of decision making explains the phenomenon of conservatism (resistance to change). It assumes that decision makers have experience with situations and that crises are of a structured nature.

Finally, there are *cognitive* theories of decision making.[21] These show a better empirical fit between theory and practice. They compensate for weaknesses in the rational and cybernetic methods. Cognitive theories argue

that decision makers are bounded by constraints. Those who follow cognitive theories diagnose problems with prevailing beliefs, search for information and options that confirm prevailing beliefs, and ignore information that disconfirms them. The decision makers then use techniques of inconsistency management to support their decisions. Only when they are overwhelmingly wrong do these people change their behavior. In general, these decision-makers do not consider trade-offs but argue that their option is to be preferred and will meet all the objectives.

While the TSA has only been in operation for seven years, it seems their decision is mainly incremental. That is, each new threat or event is dealt with almost totally separate and apart from other happenings. This leads to a scattershot approach to security where long-term planning is lacking. In the absence of some sort of strategic planning, it seems that the TSA is operating in an incremental fashion. The TSA's practice of dealing with crises as they develop and scrambling to set in place policies and practices inevitably frustrates the public in general and commercial air travelers in particular, whose patience has worn thin over the last six years, and it decreases public confidence in the agency.

## NOTES

1. For a review of post–September 11 counterterrorism policies and practices, see, for example, Jeffrey Ian Ross, *Political Terrorism: An Interdisciplinary Approach* (New York: Peter Lang, 2006).
2. James A. Fagin, *When Terrorism Strikes Home: Defending the United States* (Boston, MA: Pearson Allyn & Bacon), 159.
3. See, for example, Edward McWhinney, *Aerial Piracy and International Terrorism: The Illegal Diversion of Aircraft and International Law*, 2nd rev. ed. (Chicago: Kluwer Law International, 1987).
4. Fagin, *When Terrorism Strikes Home*, 57.
5. Ryan Singel, *Airplane Lighter Ban Lifted; Michael Moore and Senate Democrats Crushed*, July 20, 2007, http://blog.wired.com/27bstroke6/2007/07/airplane-lighte.html.
6. Fagin, *When Terrorism Strikes Home*, 169.
7. Ibid., 158.
8. Ibid., 159.
9. Ibid., 160.
10. Ibid.
11. A. Levin and B. Morrison, "Security Plan Proposed Years Ago," *USA Today*, October 5, 0A.
12. Ibid.
13. Fagin, *When Terrorism Strikes Home*, 161.
14. Ibid., 162.
15. William Banks, Renee De Nevers, and Mitchel B. Wallerstein, *Combating Terrorism: Strategies and Approaches* (Washington, DC: CQ Press, 2008), 190.
16. Ellen Nakashima, "FBI Plans Initiative to Profile Terrorists," *Washington Post*, July 11, A8.
17. Ibid.

18. Fagin, *When Terrorism Strikes Home*, 163–64.

19. Max Weber, *Economy and Society* (Los Angeles: University of California Press, 1921/1978).

20. C. E. Lindblom, "The Science of Muddling Through," *Public Administration Review* 19, no. 2 (1959): 79–88.

21. John D. Steinbruner, *The Cybernetic Theory of Decision: New Dimensions of Political Analysis* (Princeton, NJ: Princeton University Press, 1974).

# CHAPTER 8

# In-Cabin Security

*David E. Forbes*

This chapter will present a picture of aviation security issues today and also predict what we can expect to experience in the future. It touches upon the effort to protect commercial airliners from terrorists, considering what can occur and how we might counter potentially lethal assaults within the passenger cabin environment. It also examines the current state of preparedness in this environment. As of this writing, November 2007, the public and private dialogue and the often contentious debate between the parties with an interest in commercial airline security are unceasing.

## A REACTIVE PROTECTION HISTORY

When we pose investigative questions about the security of the airliner cabin, it becomes clear that this is an area that is sorely neglected. Moreover, we are now in a period when our guard, specifically in the context of in-cabin security, is gradually slipping, going back to the self-deception of the "comfort zone" that has historically created opportunities for successful terror attacks.

Experience shows, and there is no greater example than that of the pivotal events of September 11, 2001, that it is the action of the aggressor, not the defender, that leads to changes in commercial aviation security. This pattern is demonstrated by the series of hijacking and bombing events that have spanned more than 70 years, starting with the first recorded hijacking in May of 1930, when a Pan American mail-carrying aircraft was seized and commandeered by revolutionaries in the skies over Peru. Since that time, with the exception of a limited number of acts designed for personal criminal gain,

unlawful interference with commercial airliners has placed passengers and crew at the mercy of terrorist groups.

When we examine the more intense periods of concentrated action against aviation, we can see that surges of activity and varied forms of assault generate two outcomes: first, the creation of new domestic and international regulations, protocols, and security processes; and second, a comparative lull of five to seven years in terrorist attacks on civil aviation. There is generally a third outcome, however—the surprise, dramatic, and usually lethal end to that lull.

In his book *Blind Spot—The Secret History of American Counter Terrorism*, Timothy Naftali claimed that in the 1960s

> The American public and US Government were willing to put up with a monthly rate of hijacking that appears almost absurd in the context of the post-9/11 world. At the time, all of the private-sector lobbies, including initially the Air Line Pilots Association, opposed even the most limited security measures.[1]

In the early 1960s, we saw a wave of hijackings, mostly affecting American air carriers, when would-be "escapees" from Castro's Cuban regime easily used aviation. When the United States introduced armed guards and the death penalty for hijackings in late 1961, this seemed to address the threat, but from 1968 through 1972 an epidemic of more than 350 hijackings occurred. International conventions, which were negotiated and ratified during the early 1970s to address criminal acts against civil aircraft, appeared to have the desired deterrent effect, in spite of lethal attacks in the years up to 1976. Such large numbers and such a high frequency of hijacking events have not been witnessed since. In 1985, however, the hijacking of a TWA plane between Athens and Beirut, and the Atlantic Ocean bombing of an Air India Boeing 747 that had originated in Vancouver, Canada, brought the world a rude reminder that the terrorist threat had not abated, at least not to such an extent that air travel could return to the relatively relaxed era of the previous 10 years.

The horror of the Pan Am Flight 103 Boeing 747 bombing over Lockerbie, Scotland, in December 1988 was followed by yet more energy and effort dedicated to international regulation and protection upgrades. There was also a renewed impetus to develop technological countermeasures to protect civil aviation, notwithstanding the false hopes generated by the rhetoric of a presidential commission.

In 2001, a Scottish court convicted a Libyan national in connection with the Pan Am 103 bombing. Later that year, the world witnessed the worst terrorist atrocity in commercial aviation history.

## After September 11

The National Commission on Terrorist Attacks on the United States, generally known as the 9/11 Commission, included remarks in its chapter titled

"Foresight and Hindsight" that are very pertinent to today's in-cabin security vulnerabilities:

> We believe the 9/11 attacks revealed four kinds of failure: imagination, policy, capabilities and management.[2]

Later in the same chapter we find further comments that continue to apply today:

> Neither the intelligence community nor aviation security experts analyzed systemic defenses within an aircraft or against terrorist-controlled aircraft, suicidal or otherwise. The many threat reports were passed to the FAA. While that agency continued to react to specific, credible threats, it did not try to perform the broader warning functions we describe here. No one in the government was taking on that role for domestic vulnerabilities.[3]

## Threats from Passengers

While researching this chapter, I spoke with many flight attendants. During one trans-Pacific crossing in July 2007, a senior cabin crew member told me that the short term emphasis on security issues has moved away from security knowledge and training, and that there are gaps in the teaching of countermeasure capabilities. This long-serving flight attendant supervisor said that cost and customer service pressures are dictating priorities, that competitive airlines are hyping service expectations, and that consequently growing percentages of passengers have become very demanding. This is creating difficulties that sometimes translate into physical security threats to the safety of the aircraft, passengers, and crew. My informant said that a combination of alcohol, consumed on board or before boarding, with drugs, prescribed medications, or substances of unknown legal status, is contributing to confrontational events in flight.

Coping with violent passengers is causing more than event-specific concern for the crew. Whereas occurrences involving irrational spontaneous conduct are not frequent, they highlight the even weaker position of cabin attendants in the circumstance of facing a premeditated and orchestrated attack from within the passenger cabin. The assertion that a dedicated custom-designed security training and technological support requirement is not being offered or met was consistent across a range of cabin crew, domestic and international, in Australia and the United States.

## The Neglect of Flight Attendant Security Training

On November 1, 2007, Patricia A. Friend, international president of the Association of Flight Attendants—Communications Workers of America (CWA), part of the American Federation of Labor—Congress of Industrial Organizations (AFL-CIO) gave testimony before the Subcommittee on Transportation Security and Infrastructure, Protection of the Homeland

Security Committee, U.S. House of Representatives. Ms. Friend pulled no punches when she effectively (albeit coincidentally) confirmed the cabin crew members' assertion:

> I'm here to tell you that for the over 100,000 flight attendants in this country, very little has changed since the attacks of September 11th. While this Congress and the Administration have taken steps for airline pilots, who are now safely barricaded behind reinforced doors and are in some cases armed with guns, and air marshals are on a higher percentage of flights than before September 11th, flight attendants are left in the cabin with no meaningful training or tools. This is an unacceptable situation and one which we, many aviation security experts and the 9–11 Commission have been urging a change to for well over six years now.[4]

I will return to Patricia Friend's testimony later in a discussion about the absence of, the potential for, and the apparent obstacles to flight attendant security training and tools. In addition, I will comment on what I believe to be the fallacy of Friend's perception that pilots are "safely barricaded behind reinforced doors."

Given the serious disquiet about the ability and even the willingness of government regulators and airlines to improve in-cabin security, students and practitioners might pause to cast a questioning glance at the better established, parallel, and security-convergent discipline of aviation safety. Why is security a poor cousin in relation to safety?

## Safety and Security—The Relationship

A long-standing, constantly evolving, and largely successful regulatory safety culture in air transportation has endured the complication of responding to the threat of terrorist attack over more than five decades. As blurred as the line may sometimes seem, the distinction between safety and security is important. The author is working from several basic assumptions:

- Multiple airline operations scenarios, technical, physical, and procedural, individually or in combination, including security occurrences, produce a safety threat outcome.
- In much smaller measure, limited in frequency, the converse position is true, that is, safety concerns may create security vulnerabilities. For example, a commercial airliner loaded with passengers, crew, baggage, cargo, and fuel, diverted or temporarily held on the ground due to technical safety checks, may be exposed to security vulnerabilities.
- Thus, exposure to safety vulnerability due to security-related events represents a relatively small percentage of all safety threat eventualities.
- Generally, and with considerable success, the aviation safety regulatory regime is respected, supported, and enforced on a significant scale.
- Security as a discipline or as a mandated compliance requirement is prone to arbitrary interpretation and discretion. The depth of knowledge and application

detail, notwithstanding the need for confidentiality, does not match that within safety disciplines. The penalty exposure for safety violations is subject to qualitative performance measurement of security. It is consequently elusive. Its effectiveness is constantly questionable by a much larger population compared with aviation safety.

- The audit and inspection systems applied by regulators throughout the world are more predictable and consistent for safety standards enforcement than the equivalent resources for maintenance of security protocols are. One factor playing into the security issue is that there is a larger and more diverse range, not always coordinated, of security audit, inspection, and enforcement agencies with sufficient counterterrorism jurisdiction and responsibilities to justify involvement with aviation security.

For the purpose of investment in "in-cabin security," passenger and crew safety is the assumed goal. Security measures consisting of policy practice and equipment applications make up the tool-kit for achieving that goal. The security system—and the threat dimension—is a blend of four components:

- People
- Equipment
- Regulation
- Processes

This is an expansive subject deserving of and unquestionably receiving longer and deeper discussion than this chapter will allow. Each of the four components delineates a key critical area for focused study and development of in-cabin security standards. Any expectation of improvement, for example, to the satisfaction of the cabin attendant community, can only be achieved by starting from an assessment of the status quo. Why do I not include pilots and passengers here? From constant conversations and e-mails with both groups over the past few years, it seems that only the flight attendants are prepared to be persistently vocal about inadequate in-cabin security. I have yet to meet a pilot who is passionate about the subject, and of the numerous private individuals I have engaged on this topic, none are prepared to dedicate any worthwhile effort toward improving security. I will not waste space here explaining my interpretation of the reasons for this apparent incongruity, except to say that the demand for affordable air travel and the convenience that this represents are dominant, diminishing daily the images of September 11.

## People and Equipment

The determinants of cabin security conditions are influenced by several categories of people including those who may remain physically "outside" the cabin. Some of these are dealt with peripherally later, but for the most part this section concerns the people who are present in the passenger cabin of a commercial aircraft. Most of my attention is given over to the front line of protection—the flight attendant. This means no disrespect to the air or sky

marshals, to whom I refer later in brief when discussing equipment. Flight attendants are always there, on every scheduled commercial flight. In my eyes, they are foremost in any analysis of in-cabin security. First, though, there is a category that we cannot ignore: the most influential category, both inside and outside the cabin, is that of the terrorist.

## The Specter of Terrorism

Using the CIT formula—capabilities, intention, timing—we apply a combination of historical indicators and human intelligence to try to determine what it is we are protecting the aviation system against, and how we can prevent a successful assault by motivated and organized aggressors. Unfortunately our prognostications have fallen short too often. We are left to intelligently estimate, or guess, terrorist group capabilities, that is, the weaponry they have and their ability to use it. We cannot absolutely and confidently provide an accurate accounting of terrorist capabilities worldwide at any given moment.

We can generalize about terror group aims, but we cannot be assured of specific detailed operational intentions 100 percent of the time, notwithstanding some impressive counterterrorism intelligence operations that have led to arrests in France, Germany, Spain, the United Kingdom, and the United States.

In March 2007, it was reported that the British authorities had discovered that al Qaeda had obtained fake identity papers when an estimated 10,000 passports had been issued to fraudsters between October 2005 and September 2006.[5] Close to 16,500 fraudulent applications had been received; therefore there was a criminal success rate of more than 30 percent. Dhiren Barot, a senior member of al Qaeda and a British national, had obtained two of these passports; a Moroccan national now serving 18 years imprisonment for terrorist offences had also obtained two. Barot actually had seven passports with his true identity and two false passports when he was arrested. In 2006, he pleaded guilty to conspiracy to murder, having planned to launch attacks in Washington, DC, New York, and Newark, NJ, as well as in Britain. It is unlikely that we will ever know the precise details of his intentions or the identities of the other people he would have relied on to carry out the attacks. We can only speculate on the intent of those who possess fake passports and have not been arrested. That also brings us to the question of timing, an equally elusive, unpredictable factor in any threat assessment. When and where might those passports be used and with what objective?

Why is the foregoing important in a discussion about in-cabin security? Because advance planning by terrorists takes account of and is designed to circumnavigate "No-Fly" lists, and because a successful hijacking attack can depend upon strategic seating arrangements intended to ensure a "position of dominance." This favors the first class, business class, and other front-end seat assignments; early seating assignment may not occur if certain names are used. A great deal of useful information can be gained by probing techniques, including checking names from boarding passes, to ensure that the false name adopted is not on a restrictions list.

The persistent challenge is to identify the terrorist within the multitudinous ranks of ticketed passengers and crew, and thereby prevent access to the aviation system by an aggressor. Other people with preflight access to the aircraft, including caterers, cleaners, and ramp workers, add to the exposure and vulnerability of the flight.

### Optimism Keeps Us Flying—For Now

Setting the voluminous topic of airport security aside, the in-flight crew complement is made up of air crew on the flight deck and flight attendants and passengers in the passenger cabin. In relation to the passenger cabin, the optimistic assumption on the part of legitimate travelers and crew is that armed sky marshals are on board, that passengers and carry-on bags have been screened, and that baggage and cargo have been screened. This provides an assurance of safety through effective counterterrorism procedures. This may not be true; any one of the protective measures may be less than perfect; but the absence of events challenging the assumptions of passengers and crew suggests that optimism is warranted for a time at least. Cynically stated, the lull involving a false sense of security, which was so horrifically demolished on September 11, 2001, has returned.

The word "facade" is a fairly common term used in Web blogs and occasionally in media articles referring to aviation security rules and their implementation. With large segments of developed world populations traveling by air, opinions about security are never in short supply. In my continual conversations with other passengers, mostly within the United States, it has been striking how often individuals have offered suggestions on gaps in the system, even improvised onboard weapons, that can still be used by terrorists. The submissive resignation witnessed in the lines of shoeless passengers heading into the walk-through at the security checkpoint and the steadily growing numbers of airline passengers worldwide tend to show that market forces are also contributing to a desire to believe that the terrorist threat is being safely contained. A deeper examination, however, brings the serious student back to the cold reality that terrorists are biding their time, watching, waiting, and planning.

Some of the measures brought in through post–September 11 regulation may actually contribute to the degree of shock and surprise that inevitably accompanies a lethal terrorist assault. Specifically, the physical and procedural restriction of access via the cockpit door has changed the dynamics of in-cabin and aircraft security. This is discussed later. For the purpose of this section, in the human context, the effect of the changed in-flight environment due to the separation of the flight deck from the passenger cabin is of significant interest. It also crosses over into an analysis of regulation and process components. The prospect of an attacker overcoming preflight countermeasures and being on board for more than the objective of probing for in-flight security weaknesses is frightening. It is the ultimate threat of a person-to-person, face-to-face physical confrontation. If equipment, regulation, and processes

are defeated, this is the cabin crew's most dreaded nightmare realized, broken down to minutes and seconds of survival decisions and actions.

In September 2005, with an independent authorized remit to review government program progress, the United States Government Accountability Office (GAO) published a 45-page report to congressional requesters on aviation security, focusing on the training of flight and cabin crew in the handling of potential threats against domestic aircraft.[6] The report's introduction made it clear that this is a responsibility that is shared between air carriers and the federal government. Many of the conclusions about unsatisfactory performance expressed in the report were directed at the Transportation Security Administration (TSA). The GAO recommended the establishment of strategic goals for crew security training, written procedures for monitoring air carriers' crew security training, and performance measures and a time frame for evaluating the effectiveness of voluntary self-defense training.

## Communications *and* Training?

More than two years after the GAO report cited above, on November 1, 2007, Patricia Friend was giving testimony to Congress, representing the views of flight attendants. In addition to the remarks quoted earlier, she told the House committee that in spite of several recommendations from various influential sources, including the Rapid Response Team for Aircraft Security, of which she had been an appointed member, security loopholes stemming from outdated and inadequate airline security training from before September 11 had not been remedied. She said that the flight attendants had repeatedly asked for training updates to include basic self-defense maneuvers and crew communications and coordination. In a damning statement she declared that

> Currently, there is no comprehensive training or explanation of what the three components of in-flight security—flight attendants, pilots and air marshals—are trained to do in case of an attack. Clearly, these three groups must be trained on how to work together as a team to be as effective as possible. Unfortunately, this is not happening.[7]

Ms. Friend went on to describe how varied and limited the carrier' security training was, with discrepancies that left many flight attendants unprepared for any future terrorist attack. She also alleged that airline management had been instrumental in attempting to sabotage flight attendant security training, especially during the 2003 federal legislative term, when various related bills were being prepared for passage. In one reference she talked of interference with the FAA reauthorization of Vision 100, when

> At the last minute, Continental Airlines went to Republican House Leader Tom DeLay and had him change one word in the security training provisions. He had the provision that said "TSA *shall* issue guidelines" changed to "TSA *may* issue guidelines." By changing this one word, he took away the ability to force TSA to issue these guidelines.[8]

This troubling picture is compounded by Ms. Friend's further statement that the current status (November 2007) of flight attendant security training programs remains unsatisfactory: these consist of an advanced, voluntary program provided by TSA, and basic mandatory training provided by the airlines. Reports from the air safety, health, and security representatives at her organization, drawn from carriers of all sizes, indicated that "*security training has been watered down year after year.*"[9]

## Cabin Crew and New Technologies

Based on my study of flight attendant training course content, I have my own concerns that can be added to those of the GAO, the flight attendants' representatives, and others. The in-flight world is morphing into a smart, convenient, cylindrical travel machine. The changing environment, new airlines, new aircraft, new materials inside and out, new interiors, new technologies, and the world shortage of pilots, engineers, and experienced flight attendants are being used to justify a low standard of cabin crew security training that the industry has not even begun to remedy.

Some of the new technologies are not unique to aviation. Electronic devices carried by passengers can easily become the new threat, joining the restriction on gels and liquids set in place by the regulators following the findings of the August 2006 terrorist plot investigations in the United Kingdom. Radio frequency devices, cell phones, remote model car and boat controls, garage door openers, and other types of apparatus ubiquitously employed in improvised explosive device (IED) bombings around the world are easily accessible to terrorists, who have a propensity to defeat sophisticated high technology defenses with low tech and sometimes crude weapons of mass destruction. With the constant interest in improving in-flight entertainment and communications options, do we have here a potential Trojan horse, in which in-hold bomb detonations and cabin fires can be induced by the action of a passenger? We are surely left with a choice, to train and equip flight attendants to recognize and somehow neutralize a suspect device, or to prohibit all electronic devices from being carried on to an aircraft? The former is unlikely to be a realistic or effective option; the latter, as tough a restriction as it sounds, is a distinct possibility.

Although international and domestic protocols still place the responsibility for safety of the aircraft passengers and crew with the pilot in charge (PIC), the secure cockpit door and separation from the passenger cabin imposes a much greater burden of responsibility, capability, and know-how on the cabin crew for security risk management. That fact is not reflected in the quality and content of flight attendant training.

What of the passengers? Is the "legitimate" passenger a dependable part of the layers of defense, a measurable asset to in-flight response to a terrorist attack? If we sensibly acknowledge the need for training but we are not training our flight attendants for security in their regular work environment, what chance is there that a passenger or passengers will take effective action?

Untrained intervention may actually increase the dangers to others. The romantic belief in passengers rising up to defeat an aggressor, while understandable, is not a security strategy to be recommended. Least of all does it excuse a lack of investment in flight attendant security training?

Some novel, strange, and almost laughable ideas have been floated about as countermeasures since September 11. I once received a suggestion that the captain of the flight upon becoming aware of an attack mounted in or from the cabin should release an anesthetic vapor or gas into the passenger cabin. Asked about the threat to passengers with heart conditions, asthma, and similar health issues, the person proffering the suggestion declared that this should be treated as acceptable collateral damage. Just as oddly, in her book *Jetliner Cabins*, Jennifer Coutts Clay wrote the following under the heading "Tableware":

> Following the 11 September 2001 terrorist attacks, for security reasons many airlines stopped carrying implements, such as ice picks and carving knives. They have also withdrawn all metal knives and forks, and are now flying plastic cutlery in all classes of service. Even in many gate lounge hospitality areas plastic cutlery is now the norm. There is, however an argument in favour of issuing metal steak knives to all adult passengers at the time of boarding: would potential hijackers with box-cutter blades dare to attack a crew member if they knew that large groups of passengers could, in a crisis situation, use their knives to fight back in a concerted way?[10]

Ms. Coutts Clay may have intended this to be a tongue-in-cheek inclusion. I certainly hope so.

### Cabin Crew Fatigue and Security

A special note is warranted here on those very important people, the flight attendants. The gradual increase in cabin crew fatigue is going to reveal itself in the not too distant future unless the regulators step in to mitigate the risks associated with this growing problem. This is a subject worthy of more detailed explanation, but I will leave it at this point by saying that the safety and security duties, passenger expectations, and effectiveness of flight attendants depend on the vigilance that comes from their good health, proper rest, and refreshment.

### Security-Relevant Equipment Knowledge

The commercial aircraft itself is often referred to as a piece of "equipment." In the context of in-cabin security, we will remain figuratively inside that upper part of the tubular section of the fuselage where the passengers sit, where the lavatories/washrooms are located, and where the flight attendants work from their galleys and flight jump seats. While some brand new, state-of-the-art aircraft are introduced, many older commercial airliners undergo an full or partial interior refit every five to seven years. Judging the in-cabin

security features and improvements may not therefore depend on the age of the originally manufactured airframe alone. Improvements in teaching flight crew about security risk can aid in carrying out duties which help to make the cabin safer. A pervasive, nagging impression from my years of study of threats against aviation is the inferiority of the equipment-related knowledge of the cabin crew, which increases their vulnerability when compared with the target-focused facts gathered by terrorist planners.

In 1997, a paper titled "Evaluation of Cabin Crew Technical Knowledge" was presented at an international symposium in Columbus, Ohio. The paper cites examples of aviation accidents that illustrate inadequate communications between the cabin crew and the flight deck, largely influenced by flight attendants' lack of knowledge about the aircraft and the airlines' lack of concern about cabin crew ignorance of the equipment. Two strong points were raised to justify closer examination of operating and training standards. The audience was reminded of the changes in flight operations that necessitate this action:

> First, automation has led to the proliferation of 2-pilot aircraft. As the position of flight engineer has been replaced by advanced technology, the flight crew has also lost the trained eyes and ears of an intermediary to information beyond the cockpit door. Second, flight attendants have not been trained to be technically aware nor articulate in order to facilitate effective information transfer.[11]

While the presentation did not specifically address security considerations, it offered a glimpse of the weaknesses in operational in-flight security communications practices that persist today. Although the paper discussed specific safety threats arising from excessively rigid application of the "sterile cockpit" restrictions on communications during takeoff and landing, the presenters did not know what would lead to the introduction of the secure cockpit. The post–September 11 separation of flight and cabin crew unquestionably strengthens the 1997 message on flight attendant awareness training.

The prospect of hijackers being able to modify standard aircraft interior fittings such as latches, handles, sections of plastic panel, and so forth, in order to conceal assault weapons is being addressed in modern aircraft through the use of new materials, and the softening, blending, and smoothing of openers and closers. The design of lavatory compartments, besides embracing improved aesthetics and user convenience, is taking into account the need to prevent the concealment of a device or weapon while also facilitating the efficient and speedy search protocols required of the crew. Current International Civil Aviation Organization (ICAO) protocols require a preflight search that includes life vest pouches, lavatories, and areas above stowage compartments.

Fire is one of the threats that air carriers have good reason to fear. This chapter will not enter into the detail of yet another large topic, but in addressing the security of the cabin and concerns about flight attendant training, we

cannot ignore the fact that weapons available to terrorists include self-igniting flammable materials. Behavioral observation by the cabin crew through trained situational awareness becomes vital when in flight. It is not sufficient to assume that the antihazard safety testing of cabin construction materials will prevent a significant fire on board. Wires concealed behind interior panels carry electric power, control systems, and signaling capabilities. The most advanced composite materials, engineering thermoplastics, make up the floor and ceiling panels, bulkheads, stowage bins, window surrounds, galley, and lavatory modular paneling, and even the food and drink carts.

On the ground at least, professional firefighters are training for faster response and special skills when called to an aircraft fire, because of the shift to the composite material construction of the airframe. It has been claimed that firefighters at Atlanta's Hartsfield–Jackson International Airport have three minutes to reach passengers in a fire on board a jet on the ground. The article explained that planes are now built from a composite material instead of aluminum; the outer skin is a five-layer composite material both lighter and stronger than aluminum. It does not perform in the manner of aluminum in a fire, expelling hydrogen cyanide when it burns. In a quoted comment about the very short response time, which should provoke questions about preventing and fighting a deliberately set fire on board and in flight, firefighter Rodney Cook told *USA Today:* "You train, you prepare, so that in an incident I don't freeze up."[12]

An interesting development presently still in the early stages of trial application is the introduction of intelligent fasteners. These are mechanical devices with security-encrypted embedded electronics. A large commercial aircraft is constructed with several hundred thousand variable but conventional mechanical fasteners. The potential of the intelligent fastener for the cabin is that maintenance panels and other equipment in aircraft interiors can be speedily secured and opened electronically, and may offer remote status diagnostics, thereby reducing the frequency of the need for close-up physical inspection. In October 2007, one manufacturer reported a successful flight trial of an intelligent fastener stowage application on a Boeing 737 customized business jet.

When such technological advances are applied to interior stowage areas, crew quarters and galleys, and even washrooms, it becomes possible to maintain an electronic audit record of openings and closings to enhance the security and integrity of cabin crew–managed equipment. It is believed that the removal of passenger seats for repair or replacement will in the near future be a task accomplished in about 2 minutes using intelligent fasteners, as opposed to 45 minutes using conventional tools to remove metal screws, bolts, and nuts. Advances of this nature, however, validate the question—do we need to train the cabin crew so that all are sufficiently aware of the technological makeup of their environment and are able to interpret circumstantial implications for in-cabin security?

## The Cockpit—Separation, Not Protection?

The so-called hardened cockpit door is something of an anachronism, in that it is an afterthought, compromise retrofit development not entirely congruous with its airframe and functional surroundings. It has long been taught in crime prevention circles that there is little purpose in fitting a locking mechanism that is physically stronger than the door it is meant to secure, or where the adjacent wall is weaker than the lock or door. By smashing through the wall, an intruder defeats the investment in the lock or the door. The bulkhead walls on either side of the locked door are frequently constructed of plastic or board, penetrable not only by bullets but by lightweight tools, and in some aircraft types via the forward lavatory. Penetration does not necessarily mean immediate bodily entry by an aggressor. The insertion of a tube pushed through from the lavatory and the use of an aerosol device can introduce a noxious vapor sufficient to adversely affect operations on the flight deck.

The foregoing assumes that the assailant has bypassed the screening controls intended to prevent the vaporized chemicals from being taken on board. Unfortunately this assumption has some merit. Between March 2007 and July 2007, in the course of a GAO system test, government investigators were able to take identifiable risk liquids unchallenged on board aircraft on several occasions.[13] The liquids and other bomb-making formulas designed formula information were found through easily accessible Web sources; and controlled tests later demonstrated that the offending test materials did indeed produce a lethal detonation. The resourcefulness of terrorist entities, however, should cause us to remember that there is more than one route to bringing lethal materials onto a commercial airplane.

Returning to the "hardened" cockpit, some airlines, notably United, have taken a further step and introduced a secondary barrier, which acts as a buffer zone on selected aircraft. This is a system of steel wires extending from the top of the cabin down to the floor, and then locked in place by a metal bar.

Some, if not most experts, in aviation security would remove the passenger access to a forward lavatory or even remove the lavatory entirely for reasons illustrated above, and also because it has already compromised the security of the cockpit. A Turkish Boeing 737 en route from Tirana, Albania, to Istanbul, Turkey, in March 2006 was hijacked when a large man forced his way into the cockpit just as a flight attendant was entering the flight deck. This access can be gained without the presence of a lavatory. The area of the cabin adjacent to the cockpit door requires best-quality surveillance, so that the door is opened only when there is no unauthorized person present or imminently able to gain access.

Underpinning the relatively primitive treatment of cockpit protection within a high-asset-value, sophisticated machine is the failure to mandate and provide best-quality crew communications and risk management surveillance options. There has been and continues to be much debate and formal examination of the implications of regulatory or voluntary decisions arising from

both needs. Little credit can be justifiably awarded to American carriers when their attitudes on this come under scrutiny, with some exceptions. Jet Blue, for example, has not waited for mandates to introduce in-cabin video surveillance. But when the exceptions are so limited, the serious security practitioner and the curious student are entitled to inquire as to the reasons.

In the United States, an FAA notice of proposed rulemaking (NRPM) and then the final rules published in the Federal Register are accompanied by explanations of the contributory opinions from the industry. The 9/11 Commission, berating the absence of imagination, capabilities, policy, and management, should perhaps send a copy of that statement each year to each of the negotiating parties—the FAA and the Air Transport Association, representing the airlines, for starters. Those who have knowledge in the field of security and communications technologies and who take time to read some of the NPRMs may be amused and more than disappointed at the lack of understanding of what good, homegrown, patriot-driven, technological products have to offer.

One example of the many sources of September 11–triggered solutions is CAPS, a discreet, wireless alert communications device. In a two-hour test flight aboard a Boeing 747–400, it performed perfectly and sent signals from transmission locations throughout the aircraft. It was developed by Capitol Electronics of St. Paul, Minnesota, and the owner of this company, Jane Pahl, spent years trying to persuade the industry and its regulators that this was a good investment for in-cabin security. The culmination of the process came in October 2007 with the Federal Aviation Regulations (FAR) "Final Rule on Flightdeck Door Monitoring and Crew Discreet Alerting Systems."

The final rule concerned procedures for and means of compliance with surveillance near and safe opening of the locked cockpit door. My interest is, however, drawn toward the part of the rule concerning crew discreet alerting systems. In the published explanation of current practice, in which the crew interphone is the method of communication, and in remarks addressing more discreet smart systems of communications, I found the following excerpts incredible to read:

> The FAA notes that the interphone system is not intended to be an encrypted or a secure communications means, rather it is a way for all crewmembers to be able to communicate among themselves throughout the passenger cabin and the flight deck. Nevertheless, if a crewmember uses the existing technology of the interphone systems while adhering to the procedures, discreet communication may be maintained.[14]

The FAA acknowledged the fact that "some commenters, including the Professional Flight Attendants Association and the Association of Professional Flight Attendants, recommended that flight attendants carry or have in their possession a wireless device to contact the flight deck."[15]

Then came an astonishing statement: "The FAA does not believe requiring flight attendants to carry or have in their possession a wireless device to contact the flight deck is a good idea. A wireless device that is carried on the person (in a pocket or around the neck) may be problematic because an attacker could threaten or assault the flight attendant in order to obtain the wireless device and then use the device fraudulently to gain access to the flight deck."[16]

This extraordinary display of ignorance of capabilities, disdain for the "can-do" spirit, and further evidence of "failed imagination" yet again validates the conclusions of the September 11 Commission. In her November 2007 testimony cited earlier, Patricia Friend criticized the limitations of the interphone for use in security emergencies:

> when various federal agencies conducted a mock terrorist attack onboard an aircraft in June of 2005, referred to as "Operation Atlas," one of the first things that the mock terrorists did was to cut the phone cord on the aft interphone, thereby restricting communication between the cabin and cockpit.[17]

She added that

> AFA-CWA, along with other unions representing flight attendants at major carriers in this country have repeatedly called for a cost effective, wireless communication device for flight attendants to use onboard the aircraft. . . . AFA-CWA believes that it is well past time that hands-free, discreet, wireless devices should be made mandatory for all flight attendants.[18]

This demand for discreet wireless alert communications equipment also surfaced during the ICAO's 36th Assembly in September 2007.

## Hope from the Rest of the Aviation World?

After being immersed in the mire of U.S. aviation security, it is somewhat refreshing to realize that there is another, potentially more progressive galvanization of the future aviation security scene. Global growth in aviation, as seen in new aircraft orders, new airlines, new routes, and the accompanying infrastructure planning dynamics, suggests in 2007 that American dominance of commercial aviation may be waning. Industry operators, carrier and aviation sector employee associations, regulators, and air frame manufacturers are beginning to offer different perspectives on the future of safe and efficient air travel.

The European Union (EU) and non-American Asia Pacific players are taking the lead in many aspects of aviation; and we have some indications of the creativity and energy devoted to aviation security. Specifically related to in-cabin security, the work of the National Aerospace Laboratory (NLR) in Amsterdam, the Netherlands, is encouraging. At the European Aircraft Cabin Safety Symposium, held in Prague in June of 2006, three contributors from

NLR presented their report on onboard security and interaction with the cabin crew. The presenters showed that leading European companies and institutes joined forces on the Security of Aircraft in the Future European Environment (SAFEE) project: "SAFEE envisages constructing advanced aircraft security systems designed to assess on-board threats and to provide a response advice to the flight crew."[19]

Their report also included a reference to the threat assessment and response management system (TARMS). This concept is designed to gather information from onboard sensors and databases. The SAFEE program and the development of TARMS appear to restore faith in the imagination factor.

SAFEE is offered as a modular system, with subsystems available for short-term installation. TARMS is designed to provide an onboard decision support system. It offers high quality connectivity and process flow capability that will bring greater efficacy, uniting the security preparedness and response coordination of the flight crew, the cabin crew, and where applicable, sky marshals. TARMS, however, has been developed without the need to rely on a sky marshal. The following is a brief summary of TARMS:

> TARMS plays a central role in the analysis of threat identification since it is of direct influence to the user response. Three successive stages can be distinguished in the information processing by TARMS: information analysis, scenario analysis and response management. All these steps require external knowledge from databases and sensors. The outcome of these stages is communicated to relevant connected systems, to onboard users and in some cases to external actors (e.g. Air Traffic Control or Airline Operations Centre). TARMS can thus be considered as the coordinating component for the interaction between the sensors, the acting systems, the primary users and the external actors.[20]

## Completing the Blend—Regulations and Processes

While aboard aircraft in flight, cabin crews are virtually alone with their security responsibilities for the safety of the flight, each time getting to know from scratch the security status of the equipment—the plane and its interior and the passengers and crew. The security status cannot be safely assumed as constantly stable. Regulation and the procedures mandated by governments and international protocols provide some security guidelines but there is undoubtedly a disconnect, demonstrated by the remarks of the FAA, cited earlier. Some processes are developed to a standard above the minimum regulatory requirements, but not many.

In a confidential exchange with a qualified regular aviation security surveillance expert, I posed this question: "If from your professional observations you were to categorize the contemporary status of three protective layer dimensions—cabin crew awareness, crew security application competence, and evidence of up-to-date security training preparedness, (a) what overall measure would you give these, say from 10 at best to 1 at worst? and (b) what descriptive words, stated honestly, adequately describe the present profile of

in-cabin security when all human and technological conditions are considered? For example, viewing the range of variables, are the words "primitive" and/or "advanced" or "efficient" justifiable in this context?"

The response contained some sensitive comment that is not repeated here. The responder gave a security performance opinion rating of American carriers, applied to domestic operations. No carrier was awarded 10 points, and only two received a rating of 8 points. At the other end of the scale, two carriers each were given 2 points and were described as having "pathetic ground and in-flight security." The priorities suggested to bring standards up to an acceptable level were stated as follows:

1. Cabin crew awareness
2. Crew security application process
3. Up-to-date security awareness training

For the airlines at the top end of the rating, the descriptive words were as follows: "forward looking," "security conscious," "research development," and "efficient." For the airlines with the worst ratings, the descriptions were: "pathetic," "scary," "complacent," "rude," "counterproductive," and "arrogant."

## Conclusions

This chapter contains less than 5 percent by volume and possibly less than 10 percent of potential analysis outcome from the research source material, constrained as it is, understandably, by practicalities and editorial direction. Overall, I conclude that there is an enormous gap between what the aviation regulators and operators consider acceptable for in-cabin security on the one hand and what cabin crew and security experts believe on the other.

In my discussions with my peers, and with technology developers, it is easy to conclude that involvement of the full range of stakeholders is more a token effort than an honorable, respectful appreciation of the front line—the flight attendants—and their credibility, opinion, and contributory worth. While this applies to other countries as well, the United States bears much responsibility for it because of its leading aviation position. ICAO Annex 6 (Safety and Security Training), and 17 (Security) appear to contain good foundation precepts that are weakened by cherry-picking among member states.

In an information paper presented to the ICAO's 36th Assembly in September 2007, the International Transport Workers' Federation (ITF) attempted to follow up on its submission to the 35th Assembly three years earlier. The ITF represents unionized aviation workers around the world and claims to speak for millions of aviation workers globally. The ITF's paper at the 36th Assembly dealt with cabin crew members as safety and security professionals. The principal objective of this submission was to seek further progress on an ITF proposition that cabin crew should be subject to certification, applying standardized training requirements. Reiterating its 2004 position, the paper

stated that "The ITF continues to believe that licensing/certification in the aviation industry must include cabin crews to avoid one side of the safety triangle of parts, providers and personnel remaining vulnerable."[21]

In 2003, Andrew Thomas *Aviation Insecurity—The New Challenges of Air Travel* described flight attendant training, using words that still apply in 2007:

> Nearly a year after the 9/11 attacks, the Association of Flight Attendants surveyed twenty-six airlines and found that training for flight crew ranged from two to sixteen hours. Sometimes the training involved little more than lectures or video tapes. One training program even taught "verbal judo" designed to redirect behavior through language.[22]

Most disturbing is the almost unassailable deduction that within the influential sphere of the U.S. aviation industry, the poor standard of in-cabin security preparedness will only be addressed after another significant terrorist attack on the passenger airline system. It is reasonable to hope that the good work now going on in Europe will help to redress the imbalances in global security and safety influences.

The prevailing image of procrastination and even obfuscation surrounding progress in in-cabin security is reminiscent of historical preparedness failings. In a 1935 speech to the British Parliament, Winston Churchill, later hailed as one of the world's great statesmen, warned an apparently naïve Europe:

> Want of foresight, unwillingness to act when action would be simple and effective, lack of clear thinking, confusion of counsel until the emergency comes, until self-preservation strikes its jarring gong—these are the features which constitute the endless repetition of history.[23]

No further words seem necessary to describe the threatening status of in-cabin security, more than six years after an event that itself came about through the same lack of foresight.

## NOTES

1. Timothy Naftali, *Blind Spot—The Secret History of American Counter Terrorism* (New York: Basic Books, 2005), 312.
2. *The 9/11 Commission Report Including Progress Reports by the 9/11 Pubic Discourse Project* (New York: Barnes & Noble Publishing, 2006), 339.
3. *The 9/11 Commission Report*, 347.
4. Patricia A. Friend, Testimony before the Subcommittee on Transportation Security and Infrastructure, Protection of the Homeland Security Committee, U.S. House of Representatives, November 1, 2007, http://homeland.house.gov/SiteDocuments/20071101164934–12623.pdf.
5. James Sturke and agencies, "Al-Qaida Gets Fake Papers as Home Office Issues 10,000 Passports to Fraudsters," *Guardian Unlimited*, March 20, 2007, http://www.guardian.co.uk/terrorism/story/0,,2038442,00.html.

6. General Accountability Office, GAO-05–781, *Aviation Security Flight and Cabin Crew Member Security Training Strengthened but Better Planning and Internal Controls Needed*, September 2005, http://www.gao.gov/new.items/d05781.pdf.

7. Friend, Testimony.

8. Ibid.

9. Ibid.

10. Jennifer Coutts Clay, *Jetliner Cabins*, 2nd ed. (Chichester, England: Wiley-Academy, 2006), 73.

11. Melisa G. Dunbar, Rebecca D. Chute, and Kevin Jordan, "Evaluation of Cabin Crew Technical Knowledge," *Proceedings of the 9th International Symposium on Aviation Psychology* (Columbus, OH: 1997), 527–31, http://www.cabinfactors.com/pages/FATechnical_Knowledgerev.htm.

12. Larry Copeland, "Fast Firefighting Required for New Jets," *USA Today*, September 16, 2007, http://www.usatoday.com/news/nation/2007–09–16-airportfires_N.htm.

13. General Accountability Office, GAO-08–48T, *Aviation Security Vulnerabilities Exposed through Covert Testing of TSA's Passenger Screening Process*, November 2007, http://www.gao.gov/new.items/d0848t.pdf.

14. Federal Aviation Administration, 14 CFR Part 121 (Docket No. FAA-2005–2249; Amendment No. 121–334), "Flightdeck Door Monitoring and Crew Discreet Alerting Systems," *Federal Register*, August 15, 2007, effective October 15, 2007, http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgFinalRule.nsf/0/C953A8E95055FB9886257338005 17FE1?OpenDocument.

15. Ibid.

16. Ibid.

17. Friend, Testimony.

18. Ibid.

19. A.J.J. Lemmers, T.J.J. Bos, and L.J.P. Speijker, *An On-Board Security System and the Interactions with Cabin Crew*, Report NLR-TP-2006–378 (National Aerospace Laboratory, Amsterdam, The Netherlands: National Aerospace Laboratory, August 2007 (based on a presentation at the European Aircraft Cabin Safety Symposium, Prague, June 2006).

20. Lemmers, Bos, and Speijker, *On-Board Security System*, 7.

21. International Transport Workers' Federation, Agenda Item 30: Other Safety Matters, "Cabin Crew as Safety and Security Professionals," presented to the International Civil Aviation Organization Assembly, 36th Session, September 2007, http://www.icao.int/icao/en/assembl/a36/wp/wp164_en.pdf.

22. Andrew R. Thomas, *Aviation Insecurity—The New Challenges of Air Travel* (Amherst, NY: Prometheus Books, 2003), 177.

23. Winston Churchill, speech, House of Commons, May 2, 1935, *Winston S. Churchill: His Complete Speeches, 1897–1963*, ed. Robert Rhodes James, vol. 6, (New York: Penguin Books, 1974), 5592.

# CHAPTER 9

# Cabin Crew Functioning in a High-Stress Environment: Implications for Aircraft Safety and Security

*Michael Tunnecliffe*

The role of cabin crew and flight attendants in general has been given sporadic attention in the aviation literature. The portrayals of the flight attendant role have been largely left to pop culture, particularly movies and TV, where they have been many and varied. These have ranged from comedy to more malevolent roles, as in the Jodie Foster movie, *Flightplan*, in which a flight attendant is cast as the villain. This movie triggered a protest from the Association of Flight Attendants and the Transport Workers Union.[1] Few of the portrayals do justice to the diversity of roles and the variety of demands that cabin crew deal with on a regular basis.

An examination of the flight attendant role reveals one in which fatigue, interpersonal problems, airline requirements, passenger demands, medical emergencies, health consequences, and security threats all add up to a stressful work environment.[2] This notion is reinforced by a plethora of publications by former flight attendants giving anecdotal accounts of incidents that range from humorous to life-threatening. Titles such as *The Smile High Club*,[3] *Flying by the Seat of my Pants*,[4] and *Around the World in a Bad Mood*[5] convey a picture of a high-stress occupational role that can have significant consequences for flight attendants.

The increasingly stressful environment is exacerbated by the fact that commercial carriers worldwide are looking to cut costs. It's been reported that around 22 percent of all flight attendants in the United States have been laid off since September 11, 2001.[6] Yet carriers insist that flight attendants maintain even greater vigilance in relation to security and safety issues. The implications of the high-stress work environment are even more significant in the light of research, which suggests that there is a negative impact on tasks requiring high vigilance when motivation and choice are reduced.[7]

A general review of the literature reveals a number of key factors that impact on the functioning of flight attendants by increasing stress levels. These are as follows:

- The interpersonal relationships between all crew on board the aircraft
- The demands of the customer service role
- Medical emergencies and critical incidents
- The health and physical well-being of flight attendants
- Safety and security responsibilities.

## INTERPERSONAL RELATIONSHIPS BETWEEN ALL CREW ON BOARD THE AIRCRAFT

While most air crews build good working relationships, the variance in role and long-standing traditions often promote some form of distancing between flight crews and cabin crews.[8] While most cabin crews tend to maintain good collegial relationships, it would be naive to suggest that flight attendants are immune to the conflicts and interpersonal pressures of any regular workplace. In fact, the enclosed space of the aircraft cabin, the nature of the customer service role, the time constraints within which duties need to be performed, and the rotation of colleagues suggest a work environment that has a greater propensity for conflict and disagreement than most others.

While there have often been anecdotal accounts of friction between flight crews and flight attendants,[9] in recent times similar comments have been made about the presence of air marshals traveling anonymously on flights. Many flight attendants have reported feeling devalued and expendable because of negative comments attributed to flight crew members and air marshals.[10]

The diversity of culture, educational background, personality, beliefs, values, and motivations is a prime factor in crew disharmony. Even a failed attempt at humor or a sarcastic remark can be the trigger for crew members to avoid duties or each other.[11] When these situations are combined with time pressures, demanding customers, and fatigue factors, incidents of displaced stress between flight attendants are not uncommon.[12] Displaced stress is the tendency to focus stress reactions on a third party, rather than address the issue directly with the person who is the source of the stress. Psychologists often characterize such reactions as passive-aggressive.[13] Given the work environment of flight attendants and the overt customer service function they perform, often for a demanding and sometimes belligerent clientele, it's not surprising that displaced stress can become a significant work pressure.

## THE DEMANDS OF THE CUSTOMER SERVICE ROLE

In the early days of flights carrying paying passengers, the first flight attendants employed were nurses, such was the belief about the impact of flying on the average person and the need to be prepared for any untoward events.[14]

While flight attendants recognize the significance of their customer service role, the vast majority will cite the duties of safety, security, and the well-being of passengers over the importance of serving tea, coffee, and meals.[15] Yet airline advertising gives prominence to customer comfort and satisfaction rather than safety and security. In contrast, there are increasing numbers of low-cost and budget airlines around the world that have emphasized economy while glossing over the cuts in customer comforts. This can become a source of friction, especially when the traditionally free cup of coffee has to be paid for. The combination of factors likely to elevate levels of flight attendant stress and pressure becomes even more significant when cutbacks in cabin crews and increasing service demands from the passenger population are included.[16] Once more, anecdotal reports of difficult passenger behavior are numerous, and there is every reason to believe that incident reports detailing passenger misconduct are a significant underrepresentation of the true state of affairs.[17]

Episodes of customer service pressure are almost legend among cabin crew, with most flight attendants having their favorite story about the most obnoxious person they have dealt with. These range from passengers who come on board with well oversized hand luggage; passengers who refuse to take their allocated seats; or those who are a source of complaint from others on board because of intoxication, body odor, obscene language, or generally creating a nuisance to their fellow travelers when various problems are combined: the physical constraints of close proximity of the seating, inadequate legroom, and the claustrophobic environment, and the heightened anxiety of flying phobia or the emotional contagion that air travel may cause.[18]

Managing passenger complaints has become a major issue for flight attendants, and in many cases, the problem has escalated into the phenomenon generally referred to as "air rage."[19] Air rage, the direction of verbally or physically aggressive behavior toward airline staff or other passengers, is often triggered by general dissatisfaction with the service or flight conditions. The situation is frequently compounded by intoxication, mental health problems of passengers, or the air travel system, which tends to create passenger expectations that cabin crew cannot meet, often due to a lack of resources or factors outside of cabin crew control, such as flight cancellations due to weather conditions, malfunctioning entertainment systems, or changes in operational priorities.

Anecdotal reports describe numerous incidents of verbal abuse, food being thrown, sexual innuendo directed toward flight attendants, and, in more serious cases, incidents of passengers attacking each other and physically assaulting members of the cabin crew.[20] The source of such behavior is occasionally the behavior of celebrities or well-known people who see themselves as immune from consequences if they are unhappy about conditions onboard or an instruction from a flight attendant.[21] The situation becomes even more difficult when the flight attendant is caught between the pressure of delivering a high level of customer service to maintain the carrier's image and the need to deal with a situation that may create a risk to personal safety.[22] One

comparative study found that female flight attendants were more likely to experience sexual harassment, bullying, violence, and threatening behavior than nurses or teachers.[23] Such behavior contributes to an increasing body of evidence suggesting that violence toward customer service personnel is escalating in most developed countries.[24] However, the increase in aggressive behavior toward staff in the airline industry may be more significant than in other customer service areas. Some writers contend that the real reason behind air rage is not the traditional explanations used by the airline industry management (intoxication and cigarette deprivation) but the cost-cutting practices of maintaining poor cabin air quality and decreasing leg room between seats.[25] Although no comparative data is available, it's not hard to speculate that the pressure on flight attendants has increased with the introduction of no-frills, budget airlines.

## MEDICAL EMERGENCIES AND OTHER CRITICAL INCIDENTS

Flight attendants prefer trips that are uneventful, allowing them to do their job without disruption and delay while enjoying the interaction with passengers and fellow crew members.[26] Flights are not always uneventful, as medical emergencies and other critical incidents are bound to be part of an industry that transports large volumes of people over great distances each year. It's the flight attendant's role to deal with such situations, as an aircraft cabin at more than 30,000 feet above the ground is not a place where paramedics can be called to assist.

A 30-year review of medical events on aircraft revealed that more than a third (36 percent) involved musculo-skeletal or head injuries, usually resulting from falls, turbulence factors, luggage dislodged from lockers, or injuries caused by food carts. The next largest group of medical events involved heart attacks (15 percent), with fatalities resulting from only 3 percent of these events. While the study revealed that most recorded events would not be classified as emergencies, more than one-third led to aircraft diversions, causing disruption to schedules and pressure on passengers and crew.[27]

Another constant source of pressure for flight attendants is the presence of passengers who may have mental health issues.[28] Given that many people in society function well with underlying mental health challenges, it's important not to stigmatize passengers with mental health–related problems. With appropriate assistance, many people travel without difficulty. Problems may arise for cabin crew, however, when the combination of changes in routine, crowded conditions, the unfamiliar environment, and confusion about expectations result in behaviors that are demanding for flight attendants and passengers, most of whom expect the flight attendant to take control and manage the situation.[29]

Rough weather, thunderstorms, and midair turbulence caused by changes in temperature or wind, or sudden jolts caused by the wake of other aircraft,

are significant factors in injuries to flight attendants.[30] This is especially so when the seatbelt rules for passengers and for cabin crew differ. In fact, some airlines insist that passengers must continue to be served unless a member of the flight crew actually instructs flight attendants to take their seats, regardless of the seatbelt sign being illuminated.[31] This policy has been a prime cause of serious injury to flight attendants and remains a continual source of concern for cabin crew with some carriers.[32]

Medical emergencies, episodes of air rage, weather, operational disruption, and a host of other critical incidents are all issues that have some potential to create undue stress on cabin crew and compromise the safety of passengers. What may be of greater stress to flight attendants is the feeling that their concerns about these issues are going unrecognized by their employers.[33]

## HEALTH AND PHYSICAL WELL-BEING OF FLIGHT ATTENDANTS

Flight attendant concerns about lack of support with regard to in-flight stress factors, such as air rage and medical emergencies, are compounded by what the Association of Flight Attendants (AFA) sees as a lack of interest in the health challenges faced by their members. Various issues are cited as impacting on physical and mental well-being. These include cabin air quality and exposure to noise, temperature fluctuations, vibration, noxious odors, and concerns about the effects of solar radiation and exposure to radioactivity.

Perhaps the most common health risk referred to is fatigue.[34] Accounts of flight attendant fatigue are numerous, and almost every publication relating to stress and pressure among cabin crew makes mention of this factor. Airlines are in constant motion. In the United States alone, there are estimated to be between 2,000 and 4,000 commercial flights in operation at any one time.[35] Although not all of these flights carry cabin crew, many do.

Fatigue can come from many sources, not the least of which is the requirement to fly great distances across numerous time zones in a single shift.[36] Often referred to as jet lag, the impact of disruption to the circadian rhythm of the body can be highly debilitating.[37] There is now a significant body of research indicating that jet lag results in chronic sleep disturbances, irritability and mood swings, inattentiveness, and a host of potential ailments.[38] Sleep derivation alone has significant implications for both mental and physical health, and this is frequently underestimated when employers make demands upon personnel in occupations that require the disruption of normal sleep cycles.[39]

Compounding the problems caused by scheduling requirements is any disruption to those schedules. Flight cancellations, changes in turnaround times, forced layovers and short-notice crew changes are not uncommon in an industry that is subject to the demands of weather, equipment malfunction, personnel availability, industrial action, and commercial decisions. These factors can all have implications for flight attendant well-being that go well beyond

the physical.[40] Social disruption and being away from home and family can result in a range of relationship issues, as many flight attendants struggle to maintain what most people would call a "normal life" and its parenting and family responsibilities. There is speculation that this disruption leaves flight attendants with greater risk of marital problems because of the time away from home.[41] Efforts to cope with such circumstances frequently involve potentially addictive habits, such as alcohol use. Evidence of lowered job satisfaction, resentment, and increasing lack of interest in customer service paints a picture consistent with a high level of cumulative stress. This trend is reinforced by reports of people leaving the industry and increased use of employee assistance counseling by airline personnel, including flight attendants.[42]

Another significant contributor to fatigue is the quality of air in the cabin, which has long been a source of complaint. The problems can range from hypoxia, the effects of lowered levels of oxygen on passengers and crew, to flight attendant illness generated by the toxicity of the cabin air. An example of the extreme impact of air quality problems occurred in 2000 among cabin crew operating BAE 146 passenger jets.[43] Some flight attendants experienced significant problems, including headaches, memory loss, lowered concentration, and coordination difficulties. The airline involved at first attempted to avoid any liability, until legal action taken by flight attendants forced the company to address the issue.

The overall concerns about the impact of hypoxia on flight attendants continue. The air quality in the cabin of the aircraft is regulated either by an automatic setting or by flight crew adjustment. It's been reported that the cockpit receives up to 10 times more oxygen than do passengers and flight attendants in the cabin.[44] The effects on the body can be serious, yet the individual may not immediately notice any change, as the onset of problems will vary from person to person. Given the brain impairment that can accompany hypoxia, the implications for alcohol-consuming passengers and fatigued flight attendants are significant and have led to numerous anecdotal reports by passengers and cabin crew. The outcomes in extreme cases can be disastrous. In August 2005, a Helios Airways Boeing 737 crashed in mountainous terrain north of Athens, Greece, resulting in the deaths of 121 passengers and crew. This tragedy occurred as a result of hypoxia, when all on board were rendered unconscious due to a switch on the flight deck, which controls the airflow, being left in the "manual" position.[45]

Claims by airline personnel that they have also been subjected to a range of noxious chemicals have been documented by major airlines worldwide and led to the emergence of the word "skypoxia," used by some flight attendants.[46] Weight is added to these contentions when it's appreciated that prior to starting work with an airline, flight attendants require a complete medical clearance. Concern is increased by the knowledge that the effect of toxins on the human organism is cumulative.

Added to the stress of physical demands is the concern that flight attendants generally have about how they are seen by their employer. Airline policies

can be harsh and punitive. There have been many changes to the pay, conditions, and employment of flight attendants, involving moving jobs offshore and cost-saving restructuring within the commercial operations of carriers, as they seek to maintain services at reduced cost and their major concern becomes the business of flying.[47] The impact on cabin crew is particularly felt when the job role they originally took on no longer fits with their needs, ambitions, or lifestyle. This alone may prompt maladaptive coping behaviors, resulting in cumulative stress, which then triggers a wide range of physical and emotional problems.[48]

The fatigue issues of flight attendants have been recognized and discussed. A report by the NASA Ames Research Center concluded that data gathered on fatigue are generally ad hoc, with a lack of centralized collation within the industry. There also appears to be some confusion as to which factors are the major predictors of fatigue, resulting in recommendations for further research, validation of models for assessing flight attendant fatigue, review of international policies and practices on this issue, and consideration of further training requirements.[49]

## SAFETY AND SECURITY RESPONSIBILITIES

Any discussion of health issues pertaining to a particular industry or occupational group is bound to illustrate a range of at-risk situations and potential areas of health concern. The implications of impaired functioning in flight attendants are likely to be particularly serious, because their role is seen by their employer and themselves as more than just ensuring good customer service and passenger comfort.

The training of flight attendants and in-flight protocols place emphasis on safety issues above all other cabin crew duties.[50] In the post–September 11 environment, this has been highlighted by the use of air marshals, the greatly increased security screening at airports, the restrictions on what passengers can carry on board, and the certification of flight attendants.

The industry now clearly expects flight attendants to act as safety professionals.[51] However, it has been claimed that the customer service role is often valued more than the safety role by some sections of the industry.[52] This point becomes especially important when the demands of passengers put pressure on flight attendants to forgo safety requirements. Again, numerous anecdotal accounts have been written about the experiences of cabin crew dealing with passengers who simply refuse to obey the airlines' safety procedures, often because the instruction comes from a flight attendant.[53] These incidents include passengers refusing to take their assigned seats, fasten seatbelts, secure hand luggage in overhead lockers, bring seats into an upright position for landing, return to their seats when the seatbelt sign is illuminated, or refrain from smoking in an aircraft toilet. The United Kingdom Department of Transport cited "smoking in the aircraft's toilet" as the most common significant incident reported by cabin crew.[54]

While alcohol is often cited as the cause of such problems, not all passengers who refuse to acknowledge a flight attendant's safety role are intoxicated or have any other contributory cause for their behavior, apart from not wanting to obey a legitimate instruction from an airline staff member. In fact, some passengers go so far as to take legal action against the airline when their name is cited in a complaint or incident report.[55] It causes significant frustration to flight attendants when it appears their role and viewpoint are ignored in favor of the paying passenger.[56]

The ultimate price airlines pay for poor safety is the loss of an aircraft and the deaths of passengers and crew. Air crashes are unforgiving in the toll taken on those who work in the industry and use its services. While, in comparative terms, aviation is a relatively safe form of transport, problems in the industry are continually highlighted but not all are acted upon.[57] As a number of accounts have illustrated, the experience of an air crash is the one flight attendants fear most.[58] This serves to highlight the frustration flight attendants experience when they believe their concerns are ignored, often by an administration more concerned about the immediate cost rather than dealing with the foreseeable risk.

Parallel to the important safety role of flight attendants are the more onerous responsibilities associated with security. After the aviation industry worldwide was stunned by the events of September 11, 2001, flight attendants acquired a new role, partly by carrier planning and partly assumed by the flight attendants themselves. Much of this was in response to what some in the industry describe as a "viral fear" of being victimized by terrorism.[59] It's believed that increasing global threats and heightened terror alerts are causing many to question aviation security.

On board an aircraft, security is not an activity confined to a single crew member. The tasks of screening, observing, and maintaining continual vigilance have become essential for cabin crew. This is because once passengers have boarded the aircraft and the door to the flight deck is locked, the flight attendants are the only staff members in a position to maintain the security of the aircraft. Incidents are recorded every year that reinforce the security role of the flight attendant. Rather than emanating from hijackers or terrorists, such events are more likely to come from an intoxicated passenger who attempts to open an aircraft door in flight, or someone who, in a state of mental disturbance, attacks and wounds cabin crew members, as happened in Australia on a Qantas domestic flight in 2003.[60] During this incident, two flight attendants were stabbed with wooden stakes by a passenger who attempted to break into the cockpit and attack the pilots. Although wounded, the flight attendants subdued their assailant and averted disaster with assistance from other passengers.

While significant incidents such as this receive ample attention, newspapers also highlight incidents of poor judgment,, such as the breastfeeding mother removed from a Delta Airlines flight for continuing to breastfeed her child, and claims of perceived bias[61] when six Muslim clerics claimed

they were racially profiled, detained, and barred from boarding a US Airways flight in 2006. According to flight attendants, these incidents reinforce their claims that inadequate attention is given to the training needs and overall preparation of cabin crews that would assist them to meet the raised expectations of their employers and the traveling public. While most passengers take security on board for granted, there are some who question if flight attendants are as well equipped as one would hope to deal with any threat that may arise.[62]

Handling security requirements and dealing with suspicious passenger behavior has become an everyday part of the flight attendant role, yet there are claims by the Association of Flight Attendants that the Transport Security Administration (TSA) is overreliant on the air marshal program and flight deck partitioning, to the extent that comprehensive security and counterterrorism training for cabin crew has been slow to come into operation.[63] In 2005, an AFA-CWA–sponsored submission by Candace Kolander to the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the Homeland Security Committee highlighted these same problems.[64] Numerous anecdotal accounts illustrate the ways in which FAA-certified flight attendants are subjected to excessive scrutiny at airports and not afforded the same level of speedy processing as their colleagues on the flight decks, despite having undergone the same level of background checks and receiving the same level of security clearances. Emphasis was placed on appropriate recognition for flight attendants and the need for training in counterterrorism, which would include extensive background information, self-defense skills, and first-responder expertise, which would allow flight attendants to become a fully integrated part of a team that would also include flight deck officers and air marshals.

There is ample evidence of the stressful nature of the flight attendant role. Yet flight attendants comprise an occupational group that has not been afforded a degree of scientific review similar to that provided by the appraisal of health and ergonomic factors impacting on flight deck officers. In a world where flight attendants are simply there to maintain a primary role of customer service to the paying public, this would be understandable. But this is not the real world of commercial air travel today.

There are three competing demands on flight attendants that airlines have to be able to balance. These are service, safety, and security. These tasks can only be undertaken by a workgroup that is healthy and well trained. Health concerns, risk exposure, and training requirements are areas where the various professional associations of flight attendants have sought attention from commercial carriers and government agencies, with varying degrees of success. The harsh realities of the business world are likely to produce inconsistencies in the ways the needs of flight attendants are addressed.

The task of setting health standards, reducing risk exposure, and mandating appropriate levels of training largely relies on legislative requirements, which can involve a slow and cumbersome process. To maintain attention to

their needs, flight attendants will need to look at three key initiatives. First, they should continue to source good reliable data to reinforce their claims. Anecdotal information is interesting, descriptive, and helps to rouse sentiment, but it tends to be ignored when it's not supported by quantitative, scientific research. Second, they should continue to lobby for legal safeguards against exposure to risk from unhealthy aspects of their work conditions and physical environment, and from the threat posed by unruly or dangerous passengers. While various jurisdictions around the world have responded differently to these problems, the need to address the issues in a consistent, meaningful way still remains a priority. Third, those who set security policy should recognize the essential safety and security tasks within the flight attendant role and provide appropriate training to meet the requirements of that role. Many of the major commercial carriers have already gone a long way toward putting appropriate and consistent training in place. However, the economic reality is that unless forced by legislation, there are others who will cut cost sand the crew and the passengers will get only what their carrier is prepared to pay for.

More people than ever before are traveling around the globe by air, and carriers are expanding their fleets and purchasing bigger aircraft. It's important not to be seduced by size and speed. Airlines are staffed by people and achieving the safety, security, and overall integrity of the passenger-carrying aircraft is a team effort. It's essential that the role of the cabin crew members within that team is not overlooked or underestimated.

## NOTES

1. Diane Clarkson, "Jodie Foster Movie Outrages Flight Attendants," *Jupiter Research*, September 29, 2005, http://weblogs.jupiterresearch.com/analysts/clarkson/archives.
2. Drew Whitelegg, *Working the Skies* (New York: New York University Press, 2007).
3. Allan Zullo and Kathy Nelson, *The Smile High Club* (Kansas City, MO: Andrews McMeel Publishing, 2002).
4. Marsha Marks, *Flying by the Seat of My Pants* (Colorado Springs, CO: Waterbrook Press, 2005).
5. Rene Foss, *Around the World in a Bad Mood* (New York: Hyperion, 2002).
6. Francine Parnes, "For Flight Attendants, Stress Comes with the Job," *New York Times*, August 12, 2003.
7. J. Szalma and P. Hancock, "Performance, Workload, and Stress in Vigilance: The Power of Choice," in Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting, Maui, Hawaii, 2006, p. 1609.
8. Whitelegg, *Working the Skies*, 106.
9. Elliott Hester, *Plane Insanity* (New York: St Martin's Griffin, 2001).
10. Whitelegg, *Working the Skies*, 110.
11. Nattanya Anderson, *Broken Wings* (Coquitlam, BC, Canada: Avia Publishing, 1997).
12. Foss, *Around the World in a Bad Mood*, 28.

13. Tim Murphy and Loriann Hoff Oberlin, *Overcoming Passive-Aggression* (New York, Marlow and Company, 2005).
14. Whitelegg, *Working the Skies*, 107.
15. Mark Coldebella, "Enroute Emergency," *Flight Safety Australia*, January–February 2000.
16. Caroline Kelleher and Sinead McGilloway, "Study Finds High Levels of Work-Related Stress among Flight Attendants," Flight Safety Foundation, *Cabin Crew Safety*, November–December 2005.
17. Gary Stoller, "Flight Attendants Feel the Wrath of Flyers," *USA Today*, October 6, 2007.
18. Geoffrey Thomas, Christine Forbes Smith, Guy Norris, and Tom Ballantyne, *Passengers Who Make Your Flight Hell* (Perth, Australia: APTI, 2007).
19. Anonymous and Andrew Thomas, *Air Rage, Crisis in the Skies* (Amherst, NY: Prometheus Books, 2001),
20. Marks, *Flying by the Seat of My Pants*, 116; Hester, *Plane Insanity*, 64.
21. Anderson, *Broken Wings*, 208.
22. Angela Dahlberg, *Air Rage, The Underestimated Safety Risk* (Aldershot, England: Ashgate, 2001).
23. Holmfridur Gunnarsdottir et al., "Lifestyle, Harassment at Work and Self-Assessed Health of Female Flight Attendants, Nurses and Teachers," *Work* 27 (2006): 165–72
24. Martin Gill, Bonnie Fisher, and Vaughan Bowie, *Violence at Work* (London: Willan Publishing, 2002),
25. Anderson, *Broken Wings*, 210; Thomas, *Air Rage*, 90.
26. Farrol Kahn, *Arrive in Better Shape: The Long-Haul Passenger Handbook* (San Francisco: Thorsens, 1995).
27. Rick Darby, "Is There a Doctor Aboard?" Flight Safety Foundation, *Aerosafety World*, March 2007.
28. Anonymous and Thomas, *Air Rage*, 70.
29. "Psychiatric Emergencies," *Flight Safety Australia*, March–April 2003.
30. Whitelegg, *Working the Skies*, 107.
31. Anderson, *Broken Wings*, 58.
32. Diana Fairechild, *Strategies for the Wise Passenger* (Anahola, HI: Flyana, 2003).
33. Whitelegg, *Working the Skies*, 115.
34. Corey Caldwell, "AFA-CWA Raises Awareness of Flight Attendant Fatigue in Congress," press release relating to the testimony of AFA-CWA International president, Patricia Friend, before the House Transportation and infrastructure Aviation Subcommittee, June 6, 2007.
35. Daniel Baker, "Did You Know You Can Find IFR Rules for an Upcoming Flight," July 22, 2006, http://www.flightaware.com.
36. Whitelegg, *Working the Skies*, 119.
37. Farrol Kahn, *The Curse of Icarus: The Health Factor in Air Travel* (London: Routledge, 1990).
38. Anderson, *Broken Wings*, 229.
39. William Avison and Ian Gotlib, *Stress and Mental Health* (New York: Plenum, 1994).
40. Whitelegg, *Working the Skies*, 173.
41. Annie Baxter, "Some Flight Attendants Wonder Whether the Job Is Worth It," *Minnesota Public Radio—Morning Edition*, August 7, 2006.

42. Barbara De Lollis, "Job Stress Beginning to Take Toll on Some Airline Workers," *USA Today*, November 29, 2004.

43. Adrienne Lowth, "CASA Attacked over Handling of Toxic Fume Complaints," transcript from press release, *Australian Broadcasting Commission*, October 12, 2000.

44. Diana Fairechild, *Air Travel Health News*, March 2003, http://www.flyana.com/air.html.

45. *Accident Database*, August, 2005, http://www.airdisaster.com.

46. Diana Fairechild, "Skypoxia: Toxins on Board," *Jet Smart Newsletter*, March, 2004.

47. "Qantas Strikes a Deal with FAAA," *MSN*, November 2007, http://money.ninemsn.com.au/article.

48. Michael Tunnecliffe, *How to Understand and Manage Stress* (Palmyra Australia: Bayside Books, 1999).

49. *Flight Attendant Fatigue*, report prepared by the Fatigue Countermeasures Group, Human Factors Research and Technology Division, NASA Ames Research Centre, Moffett Field, California, September 2005, http://stint.dtic.mil/oai/oaifuerb=getRecordmetadataprefix=html8identifier=ADA471470.

50. Anderson, *Broken Wings*, 77.

51. Kathleen Barry, *Femininity in Flight: A History of Flight Attendants* (Durham, NC: Duke University Press, 2007).

52. Whitelegg, *Working the Skies*, 114.

53. Anonymous and Thomas, *Air Rage*, 43.

54. Department of Transport (United Kingdom), *Disruptive Behaviour On Board UK Aircraft*, April 2002–March 2003, http://www.dft.gov.uk/pgr/aviation/hci/db/disruptivebehaviouronboarduk2954.

55. Hester, *Plane Insanity*, 61.

56. Whitelegg, *Working the Skies*, 117.

57. Stephen Barlay, *The Final Call: Air Disasters. When Will They Ever Learn?* (London: Arrow Books, 1991).

58. Sandy Purl, *Am I Alive? A Surviving Flight Attendant's Struggle and Inspiring Triumph over Tragedy* (Ellicott City, MD: Chevron Publishing, 1997).

59. Kathleen Hall, "Terrorist Stress Is Paralyzing Our Lives," media release, August 2006, http://wwwdrkathleenhall.com.

60. Padraic Murphy and Phillip Hudson, "Heroes Foil Qantas Hijack Attack," *The Age*, May 30, 2003.

61. Emily Bazar and Sam Hemingway, "Nursing Mom Files Complaint against Airlines," *USA Today*, November 16, 2006; Leslie Miller, "At National Airport, Prayers against Profiling," *Washington Post*, November 28, 2006.

62. Rick Guy, "Aviation Security—The Thinning Frontlines," *Jagwa Forbes Group*, June 2007, http://www.jagwaforbes.com.au/aviation-security-thinning-frontlines.

63. "Flight Attendants Lament Lack of Training, Poor Security," Transportation Security online exclusive, October 30, 2003, http://www.transportationsec.com/microsites/newsarticle.asp.

64. Candace Kolander, Association of Flight Attendants—CWA, Testimony before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the Homeland Security Committee, House of Representatives, Washington DC, May 13, 2005.

# CHAPTER 10

# An Assessment of Aviation Security Costs and Funding in the United States

*Clinton V. Oster, Jr., and John S. Strong*

This chapter examines the costs of aviation security, both those borne by the federal government and those borne by airlines, airports, and travelers. It discusses how these activities are financed, and funding issues and options for the future.

## FEDERAL POLICY AND SPENDING ON HOMELAND SECURITY

The terrorist attacks on September 11, 2001, prompted a fundamental change in how transportation security in the United States is organized and funded. On November 19, 2001, the Transportation Security Administration (TSA) was created within the U.S. Department of Transportation (DOT) by the Aviation and Transportation Security Act (Public Law 107–71). TSA took on responsibility for many aviation security activities, some of which had been housed elsewhere in government and some of which had previously been provided through private organizations under contract to airlines, airports, or aviation authorities. Passenger and baggage screening were the most visible of these activities, but TSA responsibilities also include air cargo security, the Federal Air Marshal Service, transportation employee background checks and roles, and the security of rail, urban transit, port, and maritime activities. On November 25, 2002, the Department of Homeland Security (DHS) was created by the Homeland Security Act of 2002 (Public Law 107–296), and in March 2003, TSA was moved from DOT to DHS. In addition, DHS also includes the Coast Guard, the Federal Emergency Management Agency (FEMA), Customs, Immigration, and Border Protection, and the U.S. Secret Service.

Federal spending on homeland security activities has grown from a little under $44 billion in FY 2002 to a little over $58 billion in FY 2007, as Figure 10.1 shows.[1] This spending is spread throughout the government, but the bulk of the activities are found in the recently formed Department of Homeland Security and the Department of Defense (DOD). Figure 10.2 shows the

**Figure 10.1**
**Federal Funding of Homeland Security Activities**

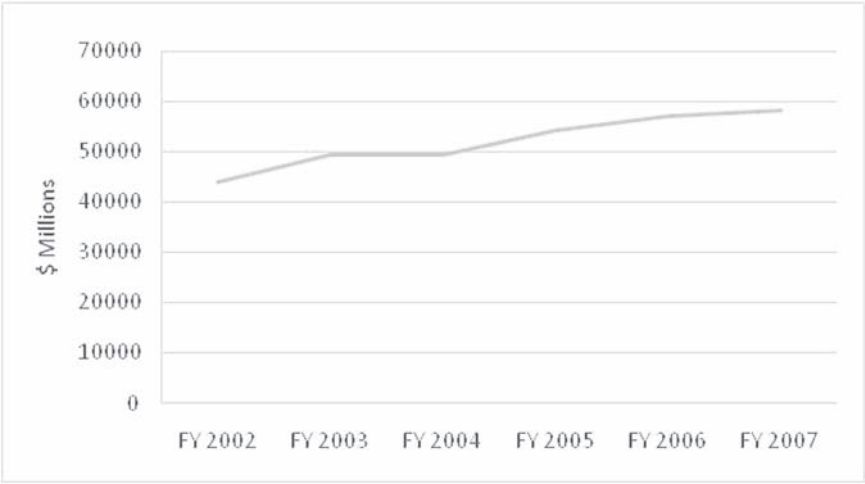



**Figure 10.2**
**Federal Homeland Security Funding by Agency FY 2007**

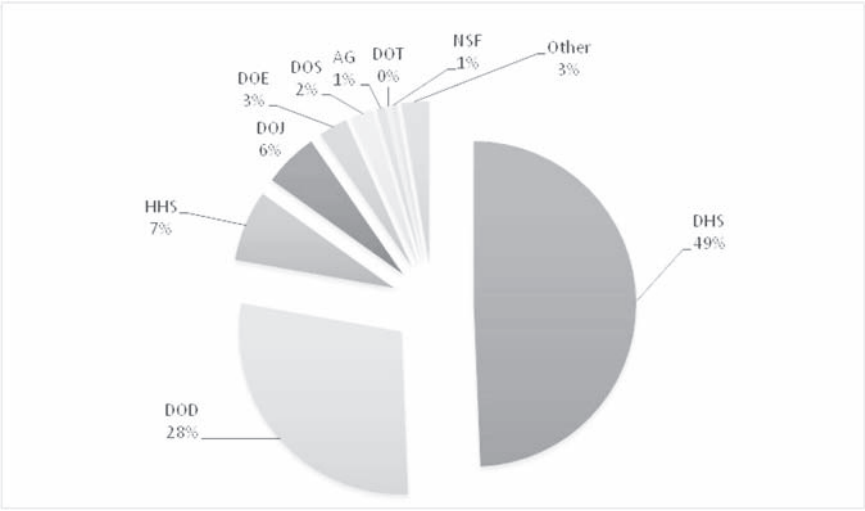
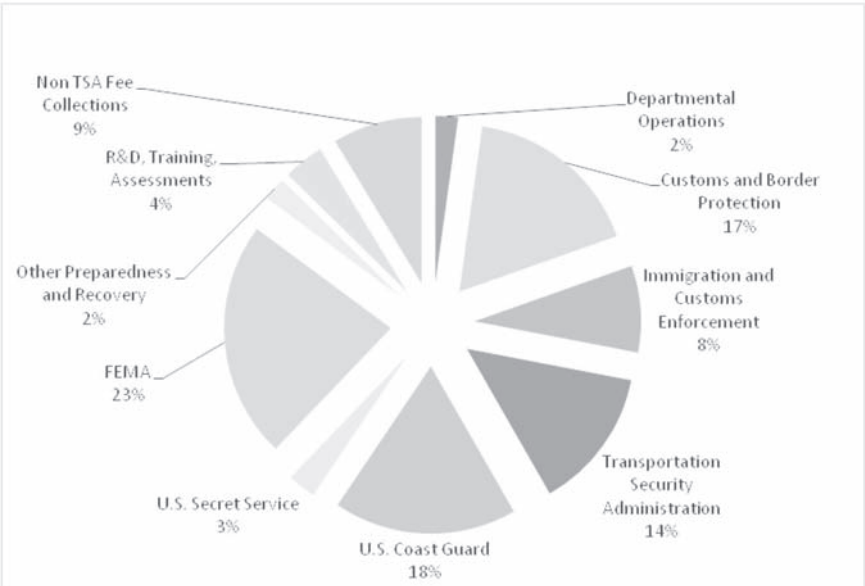


**Figure 10.3**
**DHS Appropriations by Activity**




breakdown of federal funding of homeland security activities. As can be seen in the figure, nearly half the funding, 49 percent, is in DHS and another 28 percent is in DOD.

DHS responsibilities go well beyond both aviation security and the broader category of transportation security. Figure 10.3 shows the breakdown of DHS appropriations by activity. Within DHS, the Transportation Security Administration accounts for only 14 percent of the budget.

## AVIATION SECURITY ACTIVITIES

TSA was given three initial mandates: (1) take responsibility for security for all modes of transportation; (2) recruit, assess, hire, train, and deploy security officers for 450 commercial airports from Guam to Alaska in 12 months; and (3) provide 100 percent screening of all checked luggage for explosives by December 31, 2002. Meeting these mandates was a difficult challenge, but TSA was able to hire, train, and deploy a federal workforce of over 50,000 passenger and baggage screeners and install equipment at more than 400 commercial airports to allow screening of all checked baggage.

As TSA has moved beyond its initial mandates, some of its other goals have proven more difficult to achieve. In August 2007, the Government Accountability Office (GAO) reported that DHS, through TSA, had generally achieved 17 of 24 of GAO's performance expectations in aviation security.[2] Among the expectations that had been met were those related to developing a

strategic approach for aviation security functions; hiring, training, and deploying an aviation security workforce; developing and implementing checkpoint screening processes; and carrying out checked baggage screening. Among the expectations generally not achieved were those related to establishing effective airport perimeter security, controlling access to airport secured areas, developing the advanced prescreening system (Secure Flight, discussed below), and developing technologies to screen air cargo.

Table 10.1 shows the TSA's FY 2007 budget and the FY 2008 budget requested by the administration and passed by the House and Senate. The primary difference between the A\administration's FY 2008 request and the FY 2007 budget is the absence of the $250 million in funding for the Aviation Security Capital Fund that provided grants to airports for constructing in-line

**Table 10.1**
**Transportation Security Administration Budget by category ($ million)**

| | *FY 2007 Enacted* | *FY 2008 Administration* | *FY 2008 House* | *FY 2008 Senate* |
|---|---|---|---|---|
| Aviation Security | 5122 | 4953 | 5199 | 5043 |
| Screening | 3268 | 3266 | 3364 | 3262 |
| Explosives Detection Systems/Explosives Trace Detection | 786 | 704 | 824 | 786 |
| Regulation and Other Enforcement | 218 | 224 | 224 | 224 |
| Airport Management, Information Technology, and Support | 666 | 656 | 652 | 646 |
| Air Cargo Security | 135 | 56 | 73 | 66 |
| Other | 48 | 50 | 57 | 54 |
| Aviation Security Capital Fund | 250 | 0 | 0 | 0 |
| Federal Air Marshal Service | 719 | 722 | 722 | 722 |
| Threat Assessment and Credentialing | 40 | 78 | 64 | 67 |
| Credentialing Fees | 76 | 83 | 83 | 83 |
| Surface Transportation Security | 37 | 41 | 41 | 41 |
| Transportation Security Support/Administration | 525 | 525 | 527 | 522 |
| Recision | –67 | | | |
| Total | 6702 | 6402 | 6636 | 6478 |

*Note:* FY 2007 Enacted column includes FY 2007 Supplemental.

*Source:* Authors' calculations, based on data from CRS Report for Congress, Homeland Security Department FY 2008 Appropriations, RL 3404, updated August 20, 2007.

explosives detection systems (EDS). The authority for this fund had been set to expire at the end of FY 2007, but a provision to extend it through 2028 was included in P.L. (Public Law) 110–53.[3] (The issue of EDS/ETD funding will be discussed below.) Another notable change in the administration's budget is an increase in funds for threat assessment and credentialing, intended to support the long-delayed Secure Flight program. Secure Flight is intended to establish a centralized system to prescreen airline passengers against terrorist watch lists. Finally, the administration budget proposes an increase in surface transportation security funding, intended for the hiring of additional inspectors and canine teams for both rail and mass transit.

The budgets passed by the House and Senate differ from the administration request in three major ways. First, both the House and Senate include substantially more for explosives detection and trace detection. As discussed later in this chapter, the United States faces a difficult challenge with regard to baggage explosives detection systems. Most of the systems currently in use were installed in 2002 and 2003. These systems are not as capable as the newer systems, either in terms of detection capability or in terms of baggage throughput. Given their age and level of utilization, they also are becoming increasingly expensive to maintain. At the same time, TSA has to evolve to respond to potential threats beyond those in checked baggage, and is field testing new technologies including whole body imaging, explosives trace detection portal machines, bottled liquid scanners, and improved X-ray and explosives detection systems for carry-on baggage. These new systems bring with them the challenge of how to fund their acquisition, installation, and operation at the nation's 500-plus commercial airports.

The second difference is that both the House and the Senate included significantly more for air cargo security. The basic dispute reflected in these budget differences is that the administration favors a risk-based targeting system based on the current known shipper program, while the House and to a lesser extent the Senate want to increase the share of air cargo that is physically inspected, particularly the cargo placed on passenger aircraft. Also, the House and Senate included funding to improve airport perimeter security, a program element that was not included in the administration's request.

The third difference is that neither the House nor the Senate has appropriated nearly as much for the Secure Flight program, reflecting frustration throughout Congress with TSA's failure "to fully articulate the goals, objectives, and requirements for the program."[4] Overall, the differences in budget proposals reflect different priorities as well as differences in defining fundamental approaches to aviation security policy.

## FUNDING AVIATION SECURITY

The aviation security activities of TSA are funded by a combination of specific taxes and the general fund. Table 10.2 shows the amounts collected from

**Table 10.2**
**Transportation Security Fee Collections ($ millions)**

| | *2002* | *2003* | *2004* | *2005* | *2006* | *2007* | *2007 Share* |
|---|---|---|---|---|---|---|---|
| September 11 Security Fee (Passengers) | 1,000 | 1,200 | 1,600 | 1,750 | 1,600 | 1,900 | 76.3% |
| Aviation Security Infrastructure Fee (Air Carriers) | 140 | 250 | 290 | 305 | 310 | 570 | 22.9% |
| Hazmat Threat Assessment | | | | 4.1 | 13 | 14 | 0.6% |
| Alien Flight Student Pilot Fee | | | | 1.8 | 2.3 | 3.3 | 0.1% |
| Indirect Air Carrier (Air Cargo) | | | | | | 3 | 0.1% |
| Registered Traveler Fee | | | | | | 0.6 | 0.0% |

*Source:* Transportation Security Administration, http://www.tsa.gov/research/fees/fee_data.shtm.

the specific taxes used to fund TSA. By far the largest fee in terms of revenue is the September 11 Security Fee, which is imposed on airline passengers at the rate of $2.50 per enplanement with a maximum of two enplanements per one-way trip. Thus a passenger making a connection on both the outbound and inbound portions of a trip would pay a total fee of $10.00. As can be seen in the far right-hand column of the table, this fee accounted for over 76 percent of all transportation security fee collections in 2007. In the past, this fee has been a point of contention between Congress and the administration. Prior to the FY 2008 budget request, the administration had repeatedly sought an increase in this fee, but Congress had not supported the request. In the FY 2008 administration budget request, no increase in this fee was sought.

The other significant fee, in terms of revenue collected, is the Aviation Security Infrastructure Fee, which amounted to $570 million in 2007, or nearly 23 percent of the total collected. This fee is collected from the airlines and is intended to reflect costs related to functions taken over by TSA that had previously been provided by the airlines. The fee is designed to reflect the costs of passenger and baggage screening in 2000, to the extent that the September 11 Security Fee was insufficient to cover TSA's costs for aviation security.[5]

There are four other transportation security fees, three related to aviation and one to surface transport. Taken together, they amounted to less than 1 percent of all transportation security fees collected in 2007. The three aviation related fees are the Alien Flight Student Pilot Fee, a charge of $130 to

conduct a background check for each non-U.S. citizen seeking flight training, the Indirect Air Carrier Management System Fee for freight forwarders, and the Registered Traveler Fee. The only transportation security fee not related to aviation is a fee to participate in the HAZMAT Endorsement Threat Assessment Program, which conducts threat assessments for any driver seeking to obtain a hazardous materials endorsement on a state-issued commercial driver's license.

## COSTS BORNE BY AIRPORTS

The traffic declines in the wake of September 11 disrupted a long-sustained period of growth in airport volumes. This resulted in lower revenues and passenger facility charges. This had major effects on airport economics, as a successful airport business model combines a high rate of asset utilization with a strong nonaeronautical revenue stream. In 2000, the Airports Council International reported that average airport profits after tax were about 2 percent of gross operating revenues; in 2001, airports essentially broke even, with many airports reporting losses for the first time ever. In the United States, the FAA estimated that operating profit margins were cut in half at hub airports overall.[6] In monetary terms, this represented a decline of about $820 million in operating profits for the 508 commercial airports in the United States between 2000 and 2002. By 2004, however, traffic volumes had recovered, along with airport revenues.

However, airports have experienced higher ongoing security costs that have not been reimbursed by the federal government or recouped from airline charges.[7] Estimation of ongoing security operating costs for airports is made difficult because of the variety of organizational and financial structures under which they operate. For example, residual financing structures obligate the airlines to make payment of all costs not offset by nonairline revenue sources. Other airports operate on a not-for-profit status, in which public funds are appropriated to cover funding shortfalls, or charges are designed based on a pass-through basis. The ultimate incidence of security costs is sometimes difficult to identify.

Airport financial reports and associated press releases that attempt to separate out security-related costs indicate that such expenditures represent about one-fourth of major airports' income. The identified costs range from 3 percent to just over 7 percent of operating revenues. Data from the Federal Aviation Administration Compliance Activity Tracking System (CATS) reports show that the 508 commercial service airports in the United States had 2006 operating revenues of $13.5 billion.[8] A mid-point estimate of security costs of 5 percent indicates that operating expenses for security were approximately $675 million. It should be noted that this estimate does not represent incremental spending since September 11, but rather total amounts. While incremental costs are hard to calculate, industry analysts suggest that these costs are 30–50 percent higher than previously.

The other major effect on airports is the significant and ongoing capital expenditures required to meet new security regulations, including retrofits of terminal spaces for explosives screening equipment and efforts to make property perimeters and access points more secure. Historically, capital expenditures on security-related items had averaged about $50–$60 million per year; during FY 2002 (following September 11), security projects from the FAA's Airport Improvement Program (AIP) represented 17 percent of the total AIP grants, equal to $560 million.

For 2001–5, the FAA estimated that planned capital development at airports eligible for federal aid would total $46 billion or approximately $9 billion annually.[9] The Airports Council International—North America (ACI-NA) estimated that total capital spending during the 2002–6 period for all commercial airports (not just federally eligible ones) would total $75 billion, or about $15 billion per year.[10] On the basis of types of investments, ACI-NA estimates that 3 percent of capital spending is specifically for safety and security projects. This represents about $1.4 billion over 2002–6, or just under $300 million annually. This amount is likely understated, as many of the investments defined as capacity enhancements or to meet regulatory standards have a security component as well. If 5 percent of these other categories were of this type, it would indicate a security-related capital program on the order of $500 million annually. Looking ahead, ACI-NA estimates that airport capital spending will need to rise to $87.4 billion for 2007–11 ($17.5 billion annually) to meet industry growth and standards.[11] The security-related portion of this five-year sum is expected to rise to 5.3 percent of total capital spending, representing approximately $4.7 billion, or about $940 million annually.

## COSTS BORNE BY AIRLINES

The airlines have served as intermediaries for many of the fees and charges levied for security. The direct charge for the September 11 fee on passengers was $1.9 billion in FY 2007, while the airline payment of the Aviation Security Infrastructure Fee (ASIF) had risen to $570 million in FY 2007. In addition, Immigration and Customs Inspection Fees paid by the airlines totaled approximately $1 billion in FY 2007. In total, direct fee payments were approximately $3.5 billion, having risen from $2.5 billion in FY 2004. The demand-reducing effect of these fees is also significant. Rossiter and Dresner indicate that in 2002, just over 2 million passengers diverted from air to auto travel as a result of the new security fee.[12] This represents approximately $380 million in lost airline revenues; at a 5 percent operating margin, this translates into foregone operating profits of about $20 million annually.

A second financial impact on airlines is the costs of certain security requirements, including freight and mail restrictions and the provision of seats for air marshals, that prevent air carriers from collecting these revenues from business operations. The Air Transport Association estimated these items at $518 million in FY 2004.[13] If we adjust for yield growth between 2004 and 2007 for

cargo, mail, and passengers, we estimate that these foregone revenues totaled approximately $560 million in FY 2007. Since these services were already being performed, the incremental profits would be a significant proportion of these foregone revenues.

A third impact and financial burden on airlines is the cost of regulatory mandates that are not reimbursed. For example, the requirement to harden cockpit doors to restrict access to the flight decks has been estimated to cost $300 million, only about one-third of which was reimbursed. Additional ramp security, aircraft inspections, passenger document verification, and enhanced employee background screening added significant costs as well. The Air Transport Association estimated these additional expenditures at $739 million in calendar year 2004.[14] We estimate that more than half of these items are recurring expenses; with inflation, these costs are calculated at more than $400 million in FY 2007.

## THE COST TO DOMESTIC TRAVELERS OF ENHANCED SECURITY MEASURES

Travelers have had to bear the costs of enhanced security in the wake of September 11 in a variety of forms. Perhaps the greatest cost component on travelers is the added time they must spend at airports in anticipation of the potential delays in going through security checkpoints. Passengers have always varied in their behavior in terms of how long before to their flight they arrived at the airport, with some tending to arrive just before departure and others arriving well in advance. Prior to September 11, a common rule of thumb for passengers was to arrive at the airport an hour before a domestic flight was scheduled to depart. After September 11, the Transportation Security Administration (TSA) recommendation was to arrive two hours before flight time.

Recently, TSA has worked to bring average security wait times down, but there is still considerable variability in how long passengers can expect to wait at any given airport. When TSA was formed within the Department of Transportation, the secretary established a goal that passengers be processed through passenger screening checkpoints in 10 minutes or less.[15] TSA has made progress in bringing down the waiting times at security checkpoints, and by FY 2006, the average peak wait time for all categories of airports was 8.2 minutes.[16]

However, this figure is misleading for travel planning purposes for several reasons. First, at large airports where most of the travel takes place, the wait times are longer. In FY 2006, the average peak wait time at so-called Category X airports was 12.6 minutes and at Category I airports it was 10.4 minutes.[17] Second, these averages conceal considerable variation from airport to airport, from day to day, and from hour to hour. Using TSA's website to check expected wait times, one finds that at almost all of the largest airports, there are maximum wait times on some days at some times that often exceed 25 to

**Table 10.3**
**Time Costs for Domestic Travelers Because of Anticipated Security Delays ($ million)**

| *Year* | *Large Hub Originations* | *Medium Hub Originations* | *Delay Cost to Travelers (ATA VOT)* | *Delay Cost to Travelers (FAA VOT)* | *Delay Cost to Travelers (Minumum VOT)* |
|---|---|---|---|---|---|
| 2006 | 357,438,106 | 101,963,067 | $ 24,391 | $ 19,692 | $13,312 |
| 2005 | 355,454,890 | 103,065,117 | $ 23,588 | $ 19,044 | $ 12,874 |
| 2004 | 339,124,899 | 98,656,464 | $ 21,713 | $ 17,530 | $ 11,851 |
| 2003 | 324,815,977 | 80,543,475 | $ 19,536 | $ 15,773 | $ 10,662 |
| 2002 | 312,661,338 | 88,868,797 | $ 18,582 | $ 15,003 | $ 10,142 |
| Total | 1,689,495,210 | 473,096,920 | $ 107,809 | $ 87,043 | $ 58,841 |

*Source:* Authors' calculations.

40 minutes.[18] Finally, the time TSA measures as wait time is not the time it takes to get through the security checkpoint or even the time it takes to get to the screening equipment. Rather, it is the time that elapses between when a traveler gets in line at security and when the traveler reaches the point where he or she is assigned to a lane for screening. At many airports, the wait once you've been assigned to a lane can be considerable.

Table 10.3 summarizes an analysis of the costs imposed on travelers in domestic markets due to the added time they must spend at airports to allow for increased potential delays at security checkpoints. The goal of the analysis was to estimate the order of magnitude of these costs, and several assumptions were made in order to do that. The assumptions were intended to be conservative. First, it was assumed that there were additions to wait time only at large hub and medium hub airports and that the average added time spent at the airport at large hubs was 45 minutes and at medium hubs 30 minutes. In light of the actual experiences with delays at large and medium hub airports, these seem like conservative assumptions for the period. Second, it was assumed that the historical pattern that 70 percent of enplanements at large and medium hub airports were of passengers originating at that airport, as opposed to connecting passengers, prevailed during the years 2002 to 2006.[19]

The guidelines used by the U.S. Department of Transportation (DOT) for the value of time is to value time at the wage rate for intercity business travel and at 70 percent of the wage rate for intercity personal travel.[20] For domestic airline travel, the Air Transport Association assumes that 41 percent of travel is for business and 59 percent is for leisure or personal travel.[21] For the wage rates, three different approaches were taken in the table. The first was to use wage rates based on surveys done by the Air Transport Association in 1996 and then adjusted to 2006 using Bureau of Labor Statistics (BLS) Wage Indices. The second approach was to use the wage rates that the FAA used in 2006 in its analysis of congestion at LaGuardia airport. These wage rates were then adjusted for the prior years using the BLS Wage Indices.[22] This

approach probably gives the best estimate of the costs to travelers. Finally, a third approach was taken to try to give a lower boundary by using the BLS hourly wage rate for the category of "management, professional, and related" for business travel and the category of "all civilians" for leisure travel. These figures almost certainly understate the average wage rates for business and leisure air travelers.

As can be seen in the table, the costs to travelers are substantial, even using the minimum value of the time figures. For 2006, these costs were at least $13 billion and could have been as high as $24 billion. For the entire five-year period from 2002 through 2006, the total costs ranged between $59 billion and $108 billion. Even the lowest of these figures is twice as large as the TSA budget during these years.

There are additional costs imposed on travelers due to enhanced security. One obvious cost is the added tax of $2.50 per flight segment (up to a maximum of $5.00 per one-way trip) discussed elsewhere in this chapter. The out-of-pocket costs for taxes are substantially less than the time costs. Another cost is the added inconvenience of travel because of the increased restrictions over what can be placed in carry-on luggage. Restrictions such as those on the quantity of liquids and gels that can be carried on have caused some travelers to check baggage that, absent those restrictions, they would have carried on.[23] Checking baggage, of course, incurs additional delays while waiting for it to be brought to baggage claim and still greater delays and inconvenience if the baggage is lost.

Because of the added time costs of air travel coupled with the added out-of-pocket costs in the form of security fees, some travelers have opted to substitute highway travel for air travel, particularly for relatively short-haul trips. Highway travel is less safe than air travel, and the result of these diversions could well be additional highway fatalities. Rossiter and Dresner have done a careful analysis of the potential added highway deaths from such passenger diversions.[24] They conclude that due to the segment fee of $2.50 and an added wait time at the airport of 20 minutes, there would be a little over three added deaths per year from the diversion from short haul air travel to auto travel. Even if their results were to be adjusted to the longer added wait times that we project, the effect of added security time and cost on transportation fatalities is likely to be quite small.

## FINANCIAL IMPACTS OF SECURITY IMPROVEMENTS

The United States faces some significant financial investments if it's to improve the security of air travel. TSA has estimated that it will cost over $23 billion just to install inline explosives detection systems for checked baggage in the 250 largest airports in the United States.[25] Of this amount, about $6 billion is in capital costs while the remainder is in personnel, operations, and maintenance costs. Moreover, cost reductions are difficult to achieve even if implementation is scaled back. For example, were the scope of these

installations to be reduced to only the top 100 airports, the costs would decrease by only about $120 million, less than 1 percent, over the life of the project.[26] Expenditures of this magnitude are not easily accommodated in TSA's budget. Indeed, if the current rate of spending is maintained, the completion of the installation of the systems would not occur until well after 2020.[27]

Explosives detection systems for checked baggage aren't the only investments that will be needed. Improved systems are needed for checking carry-on bags and passengers for explosives and weapons. It also seems likely in the future that there will be increased pressure to install biometric systems to screen passengers. These systems will also likely be expensive and further stretch TSA's capability to invest.

A contentious question is how the costs of these systems will be shared between airports and the federal government. In addition to purchasing the equipment, systems such as in-line explosives detection systems can have large up-front costs for the airport modifications needed to accommodate the systems. To help defray these costs, the initial approach, in 2003, was for Congress to authorize TSA to reimburse airports up to 75 percent of the cost to install these systems by entering "letter of intent" (LOI) agreements. An LOI was not a binding commitment of federal funding, but instead represented TSA's intent to provide the agreed-upon funds in future years if the agency receives sufficient appropriations to cover the agreement. TSA issued eight letters of intent, but has issued none since 2004. The process has not gone entirely smoothly. As GAO reported,

> In September 2003, TSA and the City of Los Angeles signed an LOI and an attached memorandum of agreement (LOI/MOA) in which TSA agreed to pay an amount not to exceed 75 percent of the agreed upon estimated total project cost of $341 million (about $256 million) to install in-line checked baggage screening systems at both Los Angeles (LAX) and Ontario (ONT) International Airports. However, in December 2003, officials from the City of Los Angeles' airport authority—Los Angeles World Airports (LAWA)—informed TSA that aspects of the design concept were infeasible and that additional construction modifications would be needed. LAWA subsequently submitted a revised cost estimate to TSA in April 2005 and requested that TSA amend the LOI/MOA to increase the federal reimbursement by about $122 million. TSA has not amended the LOI to provide for additional reimbursements; however, as of February 2007, TSA had obligated the $256 million for the City of Los Angeles LOI/MOA in accordance with the schedule agreed to in the LOI and had reimbursed LAWA for about $26 million in expenses.[28]

The working group that advised TSA on baggage screening investment noted that checked baggage screening is a federal responsibility under the Aviation and Transportation Security Act of 2001 (ATSA) (Public Law 107–71). Not surprisingly, the airline and airport members of the group felt that the federal government should be responsible for all of the funding necessary to achieve this mandate, including replacing or upgrading the initially deployed systems that are not up to the desired standards. Others in the working

group felt that there should be more cost sharing, and no agreement was reached on a specific cost-sharing formula. The working group's final report, however, showed the airports and airlines covering 12 percent of the capital costs and 53 percent of the operating and maintenance costs, or 15 percent of the overall costs of the projects.[29]

The airports' position on cost sharing is clear. Their trade organization, Airports Council International (ACI), takes the view that costs should be borne by the government agency and not the airport. ACI goes on to maintain that airports are within their rights to charge a rental fee to the government agencies for the use of airport facilities and infrastructure.[30] This view recognizes that airport space is scarce and valuable, in that it can be rented out for various concessions, and so there is an opportunity cost to the space occupied by security devices.

## FUNDING OPTIONS FOR LARGE CAPITAL INVESTMENTS

Irrespective of what the federal government's precise share of these investments should be, the federal government is almost certain to have to shoulder the burden of paying for most of the security improvements, so it will be faced with having to make large capital investments. The methods used to finance large capital investments are typically very different in the private sector than in the federal government. Private-sector organizations typically finance large capital investments by borrowing some or all of the required funds from a bank or other lending institution, by using their own financial resources, or by using some form of third-party financing or equity arrangement. They may also use alliances with other firms, joint ventures, sale-and-leaseback, and public-private partnerships. All of these approaches involve varying levels of risk, and some incur debt.

In the federal government, significant capital or facilities investments are primarily funded from the annual budget. With very few exceptions, individual departments and agencies may not borrow funds or otherwise incur debt to finance facilities. They must receive authorization from Congress for up-front funding to cover the full design and construction or purchase costs in a specific fiscal year's budget. Similarly, leases can be used only under carefully controlled circumstances, which generally follow this same up-front funding approach.

From the federal budget perspective, the requirement for full, up-front funding of federal facilities is intended to do the following:

1. Give adequate scrutiny to the initial costs and proposed benefits of an investment;
2. Avoid the risk of allowing projects to be started through incremental funding before they are adequately scrutinized;
3. Give Congress the flexibility to respond to changing circumstances and priorities;

4. Provide for transparency in the budget by making sure the investment proposal is understandable to a range of constituencies; and
5. Allow for the informed participation of those constituencies.

Under current procedures, requests to design and construct a new facility, to fund the major renovation of an existing facility, or to purchase a facility outright are scored up front in the year requested, even though the actual costs may be incurred over several years. Thus, the projected costs are counted against the agency's overall budget request for a given fiscal year. The requirement for full, up-front funding typically results in a spike in a department's or agency's budget request. If the agency is subject to spending caps and if it is to stay within its cap, a request for a significant facility investment will force cuts in other programs or activities within the department or agency, causing tension among the various in-house decision-making and operating groups.

These scorekeeping procedures used by budget agencies may have some unintended consequences. In spite of the intentions of the budget agencies, up-front scoring of major capital projects does not typically disclose the full costs of these investment decisions. It only discloses the projected design and construction costs. Facilities operation, maintenance, repair, and disposal costs are accounted for in different functional areas of the budget and are not linked to the decision to build or acquire specific facilities. Scorekeeping procedures create incentives for agencies to drive down the initial costs of facilities investments—even at the expense of life-cycle costs—in order to lessen their apparent impact on the current year's budget. In rewarding such behavior, the scorekeeping procedures can indirectly increase the long-term operation and maintenance costs of facilities—which can account for 90 to 95 percent of their life-cycle costs—and decrease the operating efficiencies that might result from additional initial investment.[31]

Recognizing some of the difficulties of providing adequate funding for required facilities investments through the annual budget process, legislation has been enacted over the years on a case-by-case basis for individual departments and agencies to allow the use of alternative approaches to acquiring or making investments in facilities. Legislation allowing the use of these approaches on a government-wide basis has not occurred, largely because of the strong and continuing opposition of government-wide oversight groups—Office of Management and Budget (OMB), Congressional Budget Office (CBO), and Congress.

In this environment, it's not surprising that the working group that examined baggage screening investments leaned heavily toward pay-as-you-go financing in making four financing recommendations:

1. tax credit bonds;
2. continued appropriations for the procurement and installation of EDS machines;

3. combined line items for the purchase and installation of EDS machines in order to provide TSA with increased flexibility in directing the funding where it is most needed; and
4. enhanced eligibility for the Passenger Facility Charge (PFC).[32]

The last three options are essentially pay-as-you-go approaches. Only the first, tax credit bonds, would be considered an investment strategy in which the capital is installed up front but the payments to cover the cost of that capital are spread over the useful life of the investment. Tax credit bonds are a relatively new form of debt that has gained some favor as a means to finance public capital expenditures for transportation (and other programs). The bonds, whose use must be specifically authorized by Congress, allow investors to receive a nonrefundable tax credit against their federal income tax liability instead of a cash interest payment. In essence, these bonds would provide a federal subsidy outside of the normal budget process.

While using tax-credit bonds would be more expensive than borrowing from the Federal Financing Bank, they would be of the same or lower cost than tax-exempt municipal or authority bonds. (The cost would be lower because they would be issued at the federal rather than the state or local level.) Bondholders would report the tax credit as income, but then would subtract the amount of the credit from the tax due. While the issuer would not receive annual interest payments, it would be required to establish a reserve for eventual principal repayment.

Tax-credit bonds have been proposed for use in school modernization and for green space acquisition—two activities that may have understood benefits but lack clearly defined and secured revenue streams. They also were proposed for use by Amtrak and for investment in high-speed rail. However, they have been opposed by the Treasury, and the way they would be "scored" is not clear. The Federal Financing Bank has centralized control of agency borrowing through its on-lending policy. The FFB does offer cheaper terms than private capital markets, but it appears restricted in its availability to TSA. In order for TSA to be a significant user of the FFB facility, congressional authorization is likely to be required.

In the current environment, bond financing for transportation security investments does not appear to hold much promise. Direct access to private long-term debt markets by TSA or DHS is limited by congressional authority, by budget scoring rules, and by the lack of a bankable organizational and financial/economic structure. For TSA to have options in the bond market, key policy considerations would have to be met. In particular, there would be a need for a legally independent structure, the ability to transfer assets to serve as collateral, and the ability to dedicate clear funding streams. As a government agency with a largely regulatory function, it seems unlikely that TSA would be organized along these lines. As a result, funding the next generation of security technologies across the entire aviation system remains a huge and unsolved problem.

## SUMMARY AND CONCLUSIONS

The costs and burdens of aviation security have been borne by a variety of stakeholders, including airlines, airports, and taxpayers through government fees and charges. We estimate that recurring capital and operating costs related to aviation security as of 2007 are on the order of $10–$15 billion annually. In addition, another major cost of additional security screening has been delay costs imposed on passengers, which we estimate at approximately $13–$24 billion annually. We would not expect any of these costs to decrease significantly in the medium term; in fact, replacement of screening and detection equipment and additional capacity to keep up with the growth in air commerce is likely to result in higher costs going forward.

However, we should note five important caveats with regard to our estimates. First, we have tried to focus on the ongoing costs of aviation security, rather than measure the shorter-term economic dislocations from September 11. Second, security is typically not a line item in budgets or in accounts, so that estimating such costs requires extensive assumptions. Even the Department of Homeland Security budget contains programs that cut across security and non-security-related activities. Third, security spending has both capital and operating components. We have attempted to estimate capital costs on an annual basis. However, the high technology component of much of the capital investment means that these are not assets with especially long lives. This implies that the costs of aviation security should include significant recurring capital expenditures. Fourth, the ultimate burden of aviation security costs may not be on the entity that actually makes the payment of a tax or charge. For example, the extent to which airline or airport security costs can be passed on to customers may vary both in degree and over time. This issue is at the heart of discussions of the appropriate allocation of security costs between industry, users, and society overall. Finally, the estimation of security costs here does not attempt to estimate corresponding benefits, or the degree to which enhanced activities have increased aviation security.[33]

## NOTES

1. Year-to-year comparisons, particularly using FY 2002, may not be directly comparable, because over time, agencies have improved their ability to distinguish between homeland security and non–homeland security activities.

2. Government Accountability Office, *Aviation Security: DHS Has Made Progress in Securing the Commercial Aviation System, but Key Challenges Remain*, Statement of Cathleen A. Berrick, Director Homeland Security and Justice Issues, GAO-08–139T (Washington, DC: GAO, October 2007).

3. *CRS Report for Congress, Homeland Security Department: FY 2008 Appropriations*, updated August 20, 2007 (Washington, DC: Congressional Research Service, 2007), 42.

4. Ibid., 48.

5. For more detail on this fee, see Transportation Security Administration, http://www.tsa.gov/research/fees/aircarrier_fee.shtm.

6. Hub airports are defined as all airports enplaning more than .0 percent of total U.S. passenger traffic. This represents 134 airports that serve more than 90 percent of U.S. passenger traffic.

7. For a review of these issues from the industry perspective, see Airports Council International, *The Economic Impact of September 11 on Airports* (Geneva: ACI, January 2002).

8. See FAA, http://cats.airports.faa.gov/. The database reports financial statements for commercial airports for the 1996–2007 period.

9. See General Accountability Office, *Airport Finance: Observations on Planned Airport Development Costs and Funding Levels and the Administration's Proposed Changes in the Airport Improvement Program*, Report, GAO-07–885, (Washington, DC: GAO, June 2007).

10. See Airports Council International–North America, *Airport Capital Development Costs 2007–2011* (Washington, DC: ACI-NA, May 2007), http://www.aci-na.org/docs/Capital%20Needs%20Survey%20Report%202007%20FINAL.pdf.

11. Ibid.

12. Adrianna Rossiter and Martin Dresner, "The Impact of the September 11th Security Fee and Passenger Wait Time on Traffic Diversion and Highway Fatalities," *Journal of Air Transport Management* 10, no. 4 (July 2004): 225–30.

13. See *Statement of James C. May, President and CEO, Air Transport Association, before the United States Senate Commerce, Science, and Transportation Committee*, June 22, 2004, http://www.airlines.org/government/testimony/ATA+Testimony+-+Oral+Statement+from+ATA+President+and+CEO+James+C+May+Concerning+Aviation+Security.htm.

14. Ibid.

15. Government Accountability Office, *Aviation Security: TSA's Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed*, Report to Congressional Committees, GAO-07–299 (Washington, DC: U.S. GPO, February 2007), 26.

16. Ibid., Table 2.

17. Taken together, Category X and Category I airports are roughly equivalent to FAA-designated Large Hub and Medium Hub airports.

18. See Transportation Security Administration, "Security Checkpoint Wait Times," http://waittime.tsa.dhs.gov/index.html.

19. Bureau of Transportation Statistics, U. S. Department of Transportation, http://www.bts.gov/programs/airline_information/air_carrier_traffic_statistics/airtraffic/annual/1981–2001.html.

20. Bureau of Transportation Statistics, U. S. Department of Transportation, http://ostpxweb.ost.dot.gov/policy/Data/VOT97guid.pdf.

21. Bureau of Transportation Statistics, U. S. Department of Transportation, http://www.airlines.org/economics/specialtopics/Econ+FAQs.htm.

22. Bureau of Transportation Statistics, U. S. Department of Transportation, http://www.bls.gov/web/echistrynaics.pdf.

23. Bureau of Transportation Statistics, U. S. Department of Transportation, http://www.tsa.gov/travelers/airtravel/prohibited/permitted-prohibited-items.shtm.

24. See Rossiter and Dresner, "The Impact of the September 11th Security Fee and Passenger Wait Time on Traffic Diversion and Highway Fatalities."

25. United States Government Accountability Office, Testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of

Representatives, *AVIATION SECURITY: TSA Has Strengthened Efforts to Plan for the Optimal Deployment of Checked Baggage Screening Systems, but Funding Uncertainties Remain*, Statement of Cathleen A. Berrick, Director Homeland Security and Justice Issues, GAO-06–875T, June 29, 2006.

26. *Working Group Report, Baggage Screening Investment Study*, prepared for: Aviation Security Advisory Committee, prepared by Baggage Screening Investment Study Working Group, August 9, 2006, http://www.aci-na.org/docs/BSIS%20Working%20Group%20Report_Final_080906%20wb.pdf.

27. "Airports Praise H.R.1 Language for More Security Funding," *Aviation Daily*, January 12, 2007, 6.

28. United States Government Accountability Office, GAO Report to Congressional Committees, *AVIATION SECURITY: Cost Estimates Related to TSA Funding of Checked Baggage Screening Systems at Los Angeles and Ontario Airports*, GAO-07–445, March 2007.

29. See Table 1–1 in *Working Group Report, Baggage Screening Investment Study.*

30. *The Application of Biometrics at Airports*, position paper (Geneva: ACI World Headquarters, November 2005).

31. National Research Council, *Investments in Federal Facilities: Asset Management Strategies for the 21st Century* (Washington, DC: National Academies Press, 2004).

32. *Working Group Report, Baggage Screening Investment Study.*

33. For a discussion of these issues, see General Accounting Office, *Aviation Security: Progress since September 11, 2001, and the Challenges Ahead*, Report, GAO-03–1150T (Washington, DC: GAO, September 9, 2003); General Accountability Office, *Aviation Security: DHS Has Made Progress in Securing the Commercial Aviation System, but Key Challenges Remain*, Report, GAO-08–139T (Washington, DC: GAO, October 16, 2007). For a critique of aviation security policy, see Robert Poole and James Carafano, *Time to Rethink Airport Security*, Backgrounder Report no. 1955 (Washington, DC: Heritage Foundation, July 26, 2006).

# CHAPTER 11

# Future of Aviation Security: "Fast, Cheap, and Out of Control"

*Mark B. Salter*

Fast, reliable, seamless, profitable, efficient, and secure mobility is a sine qua non of contemporary globalization. Civil aviation is a vital artery for global civil society, politics, diplomacy, international relations, and economics. Through exponential reductions in average transportation and communication costs, the aviation sector consistently trends toward growth. Passenger volumes have increased steadily across the twentieth century, taking massive leaps with each new generation of jetliner, wide-body, and stretch jets, jumbo jets, and new larger aircraft. Large amounts of high-value, low-weight cargo, as well as perishables, are shipped by global air freight. Passenger and cargo traffic are predicted to increase nearly 5 percent per year in the foreseeable future, according to IATA figures. The current civil aviation sector is operating at 80–90 percent capacity, and the imminent increases in passenger, cargo, and aircraft movements will necessitate a fundamental rethinking of business models, regulations, and infrastructure.[1] Global trends toward privatization, deregulation, and neoliberalism have led to a revolutionary decentralization of the sector, in an increasingly complex network of networks. These dynamics are structured by public norms, in other words, the balance of risk, freedom, mobility, rights, and privacy that the public is willing to accept. Aviation security is fundamental to the success of global civil aviation—without customers, there is no aviation sector.

Aviation security is a complex, interdependent system of systems, in which international, national, local, and commercial interests shape expectations, norms, measures, and policies. In an environment of incredible density, networked security is dependent on the least-equipped police force, the most over-taxed screener, the greediest operator, the least comprehensible

regulations, and the most nefarious plans. The network is at once integrated and decentralized: air cargo system, civil aviation systems, and airports. We must also consider the integrity of the communication, information, and navigation systems that manage those flows. The primary historical driver of change in aviation security has been reaction to failure, and we cannot predict with any great success the place or kind of the next great failure. This chapter identifies three axes of change that will shape the future of aviation security: technology, governance, and public norms.

The history of aviation security measures clearly demonstrates the degree to which disasters, crises, and threats have driven innovation.[2] Successful and unsuccessful attacks can have an equal impact on policies, perceptions, and acceptable practices. Walk-through X-ray portals were adopted after widespread hijacking in the United States; explosive detection devices were implemented after the attempted bombing by Richard Reid; limits on liquid and gels were implemented after the planned transatlantic attacks. Since terrorists and criminals are faster entrepreneurs than governments and corporations, we cannot predict new attacks, the next generation of technologies, or the subsequent public responses.

Security has both objective and subjective conditions. We can objectively measure threats against civil aviation, the number and kind of system failures, and the number of failed or successful attacks. But equally important is the *subjective perception* of security by the general public, the flying public, commercial actors, corporate boards, shareholders, regulators, professional risk managers, insurers, and policing experts. It is important to understand that future aviation security will be determined not only by the limits of technology or governance, but also, importantly, by the limits of public acceptance and market tolerance of risk. When faced with invasive security screening, regulative strangulation, complexity or ambiguity, or impossibly thin profit margins, the aviation industry could suffer a death by a thousand cuts. To understand the future of aviation security, we must focus equally on the *objective* integrity of the system and the *imagined* or *perceived* integrity of the system. Within this chapter, we can lay out some of the determinants, some of the possible avenues of change.

## KEY ISSUES

To plot the possible future of aviation security, we can point to three axes of change: technology, governance, and public norms. Technology is central for the detection of dangerous and prohibited items, the tracking and the identification of individuals and cargo, and the administration of the system as a whole. Private and public security regimes take their shape from corporate governance norms, national regulatory regimes, and international standards and recommended practices. And, as argued above, all of these factors are dependent on the needs and attitudes of the public.

## Technology

There are three technological drivers of aviation security: miniaturization, radical increases in computing power and the ability to store and share data, and the predominance of flexible designs. We see an increasing trend of horizontal and vertical technological integration, where security systems increasingly talk to one another. Integrated gateways can use biometric authentication for frequent-flyer identification, travel authorization, document verification, and explosives and narcotics detection. Similarly, integrated baggage, millimeter-scan or backscatter X-rays, and document verification systems provide a single go/no go message for operators, based on a multilevel analysis of triggers.

One of the predominant trends in technological innovation has been miniaturization: the size of processors, memory, and detection equipment has decreased exponentially in the past decade. The new standards in biometric passports are possible because of advances in chip, RFID, and contactless reader technology, advances that have also been applied to airside security.[3] Rather than a simple machine-readable numerical code, today's passports contain a great deal of personal information. The trial of RFID chips in luggage handling is also made possible due to miniaturization, and allows a refined and robust tracking system,[4] including the policing of sterile areas. Similarly, miniaturization drives the new advances in millimeter-scan and backscatter X-rays, explosives detection systems, and CAT scanners. While of each of these technologies has improved the detection capacity of many nodes in aviation security, the human factor remains the slowest—but most flexible—part of the screening process.

One of the prime drivers of global integration, and one that is characteristic of contemporary globalization, is the increase in processing power and storage capacity, and the corresponding decrease in telecommunications costs. Governments, corporations, and private actors have access to much more data, which can be analyzed quickly and easily, and communicated across the globe instantaneously. In the new security environment, governments and even some airlines are generating "no-fly" or security watch lists, integrating public and government data.[5] The exchange of API/PNR (advance passenger information and passenger name record) data between the European Union and the United States is emblematic of these new trends. More data is being gathered and the ability of risk algorithms and "fuzzy-logic" programs to sift through this data is increasing.

A second key revolution in technology and design is the standardization of global regulations, practices, and policies, which allows for flexibility and intelligent designs. For example, the standardization of the shipping container led to a dramatic reduction in global transportation costs. E-mail and "Voice over Internet Protocols" have led to a dramatic reduction in global communication costs. While airports are fixed nodes in the global civil aviation system, within those sites, airport and security authorities are becoming increasingly flexible

in the way they arrange screening points and other security measures. Along with legacy hub-and-spoke systems, new point-to-point systems are emerging that make the aviation network more flexible and more adaptable. There is a problem corresponding to this integration of transportation, information, communication, and infrastructure networks. The greater the integration of systems, the greater the efficiency, the less slack, but also the more vulnerable the systems are. A tight transportation network will suffer more greatly from a single attack than a loose network.[6] In legacy systems or designs, one could designate a single clear chokepoint at which to complete security screening. Within a complex system, there is no single chokepoint, which makes the system more robust but more vulnerable. Technological change, changes in regulations, and market imperatives are driving the global aviation system toward more efficiency and more flexibility, which makes the task of aviation security that much more difficult.

## Governance

The international civil aviation system has always been governed by sovereign states, who agree by necessity on certain global "standards and recommended practices" (SARPs) set by the International Civil Aviation Organization (ICAO). ICAO is the organization formed by the Chicago Treaty, consisting of 188 contracting states. It is a functional international organization aimed at facilitating global travel, rather than a political organization such as the United Nations Security Council or the World Trade Organization, both of which may impose sanctions.[7] The standards for global aviation security are set in Annex 17 of the Chicago Treaty, which has been amended 11 times and explained in the *ICAO Security Manual* (Doc. 8973).[8] Two crucial innovations in the description and governing of aviation have come about as a result of major disasters. After the successful bombing of Pan Am 103 over Lockerbie, Scotland, ICAO convened the Aviation Security Panel of Experts. The panel reports to the ICAO Secretariat and Council on the risks, threats, and trends in aviation security. The *Aviation Security Plan of Action*, resolved and implemented after the September 11 attacks, established the ICAO Universal Security Audit Program. Under this program, all contracting states are audited by an international ICAO team of security experts, although at present the results are confidential and shared only with the designated national aviation security authority. Sovereign states also have the absolute right to deviate from the Annex 17 SARPs with a notification of noncompliance. Within these dynamics, sovereign states are exclusively responsible for aviation security, although ICAO establishes global norms. The aviation system regime is consequently based on a foundation of similar norms, but in practice is composed of a set of over 200 different systems, each with national variations according to culture, language, capacity, and inclination. Accepting that the ICAO SARPs are norms, rather than laws, we can still make some generalizations about the national regulation of aviation security.

From the patchwork of national regulations, we can identify neoliberalism as the dominant trend in the governance of aviation security. Neoliberalism is a method of governance assuming that the government itself is less efficient than the marketplace at providing services. While government intervention is needed in areas of market failure, such as education, environmental protection, judicial processes, and national security, the market is better at providing health, insurance, natural resources management, infrastructure, and so forth. Within aviation security, examples of this are the privatization of air traffic control in Canada or the pre–September 11 privatization of airport security in the United States.[9] This follows the deregulation and privatization of national aviation infrastructures. American airspace deregulated in 1978, European in 1997, and major Asian markets, such as China, India, New Zealand, Japan, and Australia have deregulated in turn to varying degrees. The privatization of airports themselves has also accelerated in recent years.[10] As a consequence, a number of important airport, airside services, and information/communications management companies are coming to dominate the global market.[11]

These trends have two consequences for aviation security, demonstrating both centrifugal and centripetal forces. Aviation security is a service, and subject to the same pressures and tensions of the global marketplace as any other international service (such as insurance, banking, or consulting). Ownership of key airports and airlines is both consolidating and proliferating. While the privatization of the industry is allowing for more varied and diffuse ownership, key service providers are consolidating in dominant firms like Fraport/British Airport Authorities, Swissport, SITA/General Electric, Smiths, or L3. Because aviation security is provided at catering facilities, airside checkpoints, fixed-base operations such as aviation fuel farms, air traffic installations, and various cargo and off-site check-in locations, we see an increase in the number of sites of security. In this delocalization of the airport/aviation security, the behavior of governments, firms, and the public becomes a crucial variable.

## Public Behavior

The aviation sector can succeed only with the cooperation and support of the general and flying public: people must be willing to fly, to ship by air freight, and to accept the risks of civil aviation. Despite advances in communication and information technology, global business still depends on the mobility of the transnational business elite (whose members account for a large proportion of regular passenger numbers). Passenger numbers dropped radically after the September 11 attacks because of a perceived decrease in security (even if the actual statistical risk of flying remained lower than that of similar travel by automobile).[12] Three segments of the public need to be convinced that aviation security works: the business elite, the general flying public, and the experts (insurers, risk managers, regulators, etc.).

The global "road warrior" or business elite provides a constant motor for wide-scale international travel. Though counting for only 10 percent of the

total volume of international travel, business travelers were responsible for 28 percent of total revenue in 2002.[13] We must also take note that there is no divide between legacy and budget carriers in their dependence on business travel: 40–80 percent of all budget travelers were on business.[14] The demand has remained relatively static, or at least has been following sector-wide demand, since the 1980s. Thus, while we can expect that demand will remain consistent with general trends (to increase 5 percent over the next 10 years). Despite the rise of teleconferencing and virtual offices, there is a still a persistent culture of face-to-face business that is indispensable to doing business. Aviation security does not rank highly among business travelers' concerns, since their primary drivers are economic—in terms of cost and convenience. And, since there is no additional security premium attached to sitting in first or business class, the price differential is accounted for by other means. Demographically, nearly 90 percent of business travelers are men, although there is not a great deal of data to examine whether this proportion is changing.[15]

The rise of the jet, the long-haul jet, and more recently budget carriers has led to a variable demand for the use of air travel for tourism among the general public. Successful terror attacks have had effects on the overall use of air travel and on willingness to endure long-haul travel. Again, cost and convenience are the main drivers of tourist demand.

A final category of the public that must be convinced of the security of the civil aviation system is that of experts, namely, insurers, risk managers, regulators, economists, and so forth. It is these experts who determine rates of insurance, appropriate risk management or security management systems, and national standards for aviation security.[16] They are influenced by statistical data, industry norms, and ultimately the appetite for risk/cost/security of the regulators and markets.

A major issue in the public's perception of aviation security is that of cost and risk. In no other sector do passengers pay such a large proportion of the security costs, and so visibly (the various aviation security charges). It is a fundamental challenge to sell the public on aviation security. In addition, operators are reluctant to reveal security data—spending, services, or performance—for fear of alienating customers or informing potential attackers. There is an unfortunate silence in the public debate about airport security, which is dominated by post-facto audits of disasters.[17]

We can point to three general trends in the public face of aviation security: the move toward self-service, the rise of registered traveler services, and the use of prescreening. The underlying logic of these developments is risk management: the apportioning of resources (human, capital, and technological) to those elements of the system that pose the most risk (either because of known risk factors or precisely because the information is unknown). Since airport and aviation security is a complex network of interdependent systems, the central chokepoints, such as passenger, baggage, or cargo screening, establish the efficiency and effectiveness of the system. In an effort to systematically distribute the stress on these chokepoints, by weeding out the vast majority

of travelers and the vast bulk of cargo and bags that pose no risk whatsoever, operators throughout the aviation sector are attempting to delocalize security operations. The use of off-site check-in and self-service counters attempts to avoid the peaks and valleys of passenger/cargo transit. Registered traveler programs (such as Privium at Schiphol, Clear in the United States, or the NEXUS program across the Canada-U.S. border) channel low-risk passengers into dedicated pathways that rely on preclearance (usually with additional security checks). Prescreening of passengers through carrier sanctions and remote visa approval systems (such as the Australian Advance Passenger Program or the U.S.-Canada preclearanc' agreement) locates the board/no board decision in the country of origin rather than at the destination. Thus, air carriers and customs and immigration agents make preemptive decisions about admissibility and security risk.

The dark counterpart to these programs, which rely on self-policing and self-registration, are the "no-fly" lists that have proliferated since September 11. Setting aside the actual efficacy of these programs, the confidence of the public in them is a necessary part of the public perception of aviation security. The rise and fall of the proposed CAPPS II system (Computer Assisted Passenger Prescreening System) provides an illustration.[18] Public resistance to no-fly lists and to additional screening measures imposed by governments is a liability for the aviation sector. Again, the same fundamental problem reappears: air operators do not wish to discuss security with their investors and their customers, and so the public debate is driven by anecdote or by failure.

The key dynamic is that security accounts for a significant proportion of costs in the aviation sector, but none of the important actors wish to engage in public discussion about the efficiency, efficacy, or risk associated with security measures. In this, the aviation sector is lagging behind other sectors of the economy, such as communications technology, insurance, or banking. The public must be educated about risk and threat in aviation security if costs continually increase without tangible benefit. Over the past few years, there has been an emerging consensus that security and facilitation are not competing goals but rather complementary aims, demonstrated by the success of the Simplifying Passenger Travel Interest Group. But, this needs to be further promoted.

## PROBLEMS AND OPPORTUNITIES

Under the umbrella of Annex 17 of the Chicago Treaty and the ICAO security manual, there are of course fundamental national differences. Because of the slow speed of change in ICAO's SARPs (standards and recommended practices), aviation security is most often reactive and based on the lowest common denominator of acceptance. In the future of aviation security, three areas of current friction could intensify. There are fundamental problems in the areas of capacity, technology, and regulation and enforcement. These problem areas arise in the interface between the four major geographical

centers of civil aviation: the United States, the European Union, Asia, and the rest of the world (RoW).

In terms of capacity, the American civil aviation market processes 1.3 billion passengers per year, with Europe trailing slightly at 989 million. The Asian market is expanding extremely rapidly. China alone is predicted to reach 950 million passengers within 15 years—comparable to the current European market. There are 133 large airports in China with 55 more anticipated to open before 2020.[19] There is a general concern that passenger volumes will exceed global capacity, especially at hub airports and within high-growth areas like East and South-East Asia.

In terms of technology and regulation, a core concern for the integrity of the global civil aviation security regime has to be the limited technological and governmental capacity of developing states, a central concern for ICAO. The results of ICAO's Universal Security Audit Program are confidential, but one of the reasons for covering all parts of the world was a specific concern about the global uniformity of security standards.

Technologies are not standard, despite the increasing concentration among security technology providers. The differing standards are most easily demonstrated in the current difference between American and European models of hold baggage screening. ICAO made 100 percent hold baggage screening mandatory by January 1, 2006 (Annex 17, Standard 4.4.8). The American policy is to screen each bag with a computed tomography–based, automated explosive detection system.[20] The European model uses a five-level system in which alarms trigger more intense scrutiny. Even with some consensus on the type of detection technology, U.S. and European regulators have different ways of managing risk, and different ways of interpreting the same data. The cultural differences between European and American regulators are minor, however. Equally pressing is the ability of governments to purchase the required technology and provide the required bureaucratic support for civil aviation security. While technology has the potential to be a force multiplier, without the governmental capacity to purchase, manage, and maintain technological systems, the resulting security will be thin.

## FAST, CHEAP, AND OUT OF CONTROL

Brooks and Flynn, both MIT professors of robotics, propose that (to investigate other planets, for example) we should build robots that are "fast, cheap, and out of control," instead of single, complex, expensive, and delicate robots.[21] They argue that in the past we have been fascinated by the idea of creating a simulacrum of the perfect human—focusing on bipedal, autonomous robots—and we have ignored less ambitious projects that would be more efficient, feasible, and robust. We must fundamentally rethink our assumptions about the goals of innovation. Brooks realizes one day that the ants that are successfully invading his picnic are not superintelligent, stable, or strategic: they are fast, cheap, and out of control. Fast, because they are

concerned with flexibility and not stability; cheap because they are small, disposable, and have a single function; and out of control because they are not centrally coordinated but rather function as a self-organizing system with a shared purpose but no prescribed solutions. Rather than adding more and more complex technologies, systems of remote control and surveillance, and redundancy and multiple checks in our security systems, we should understand that "Simplicity increases reliability."[22] In this spirit, we can imagine a future for aviation security that is flexible, decentralized, and self-organizing.

To date, however, aviation security has proceeded in fits and starts, driven by a short public attention span and spectacular failures. Innovations in organizational risk management, screening technologies, and business practices have the potential to harness the best aspects of governmental and corporate governance to provide a distributed, secure global civil aviation system. Crucial to this success will be the education of the flying public and its members' inclusion as active participants in aviation security.

## NOTES

1. For example, see the American government's "Next Generation Air Transportation System" project, headed by the Joint Planning and Development Office, and the European Union's "Single European Sky" project.

2. M. H. Bazerman and M. Watkins, "Airline Security, the Failure of 9/11, and Predictable Surprises," *International Public Management Journal* 8 (2005): 376–77.

3. The Canadian Air Transport Security Authority and Transport Canada have recently implemented the RAIC (Restricted Area Identity Card), which uses biometrics to authenticate access to sterile areas at Canada's chief airports.

4. This system is currently in place at McCarran Airport in Las Vegas, Hanover Germany, and Pudong Airport in Shanghai, among others.

5. C. J. Bennett, "Comparative Politics of No-Fly Lists in the United States and Canada," in *Politics at the Airport*, ed. M. B. Salter (Minneapolis, MN: University of Minnesota Press, 2008), 88–122.

6. This is evident when a key global airport (such as O'Hare, New York, Heathrow, or Changi) suffers weather, air traffic control, or other problems. See N. Elhefnawy, "Societal Complexity and Diminishing Returns in Security," *International Security* 29 (2004): 152–74.

7. M. Zacher with B. Sutton, *Governing Global Networks: International Regimes for Transportation and Communications* (Cambridge: Cambridge University Press, 1996).

8. P. S. Dempsey, "Aviation Security: The Role of Law in the War on Terror," *Columbia Journal of Transnational Law* 41 (2003): 649–733.

9. J. Hainmüller and J. M. Lemnitzer, "Why Do Europeans Fly Safer? The Politics of Airport Security in Europe and the US," *Terrorism and Political Violence* 15 (2003): 1–36.

10. A. Advani and A. Borins, "Managing Airports: A Test of the New Public Management," *International Public Management Journal* 4 (2001): 91–107.

11. British Airport Authorities, Fraport, Swissport, and Vancouver International Airport, among others, all operate foreign airports in whole or in part. M. B. Salter, "Managing the Global Airport," in *Politics at the Airport*, ed. M. B. Salter (Minneapolis, MN: University of Minnesota Press, 2008).

12. A. Ghobrial and W. A. Irvin, "Combating Air Terrorism: Some Implications for the Aviation Industry," *Journal of Air Transportation* 9 (2004): 75.

13. K. J. Mason, "Observations of Fundamental Changes in the Demand for Aviation Services," *Journal of Air Transport Management* 11 (2005): 19–25.

14. Ibid., 21.

15. K. J. Mason, "Marketing Low-Cost Airline Services to Business Travelers," *Journal of Air Transport Management* 7 (2001): 105.

16. M. B. Salter, "SeMS and Sensibility: Security Management Systems and the Management of Risk in the Canadian Air Transport Security Authority," *Journal of Air Transport Management* 13 (2007): 389–98.

17. Standing Senate Committee on National Security and Defence, *The Myth of Security at Canada's Airports* (Ottawa: Senate of Canada, 2003); Standing Senate Committee on National Security and Defence, *Canadian Security Guidebook: An Update of Security Problems in Search of Solutions. Airports* (Ottawa: Senate of Canada, 2007); J. Wheeler, A*n Independent Review of Airport Security and Policing for the Government of Australia* (Melbourne: Commonwealth of Australia, 2005); G. D. Kutz and J. W. Cooney, *Aviation Security: Vulnerabilities Exposed through Covert Testing of TSA's Passenger Screening Process*, Testimony before the Committee on Oversight and Government Reform, House of Representatives, Government Accountability Office, GAO-08–48T, 2007.

18. A. Barnett, "CAPPS II: The Foundation of Aviation Security? *Risk Analysis* 24 (2004): 909–16; see also Bennett, "Comparative Politics of No-Fly Lists in the United States and Canada."

19. Aviation Technology.com, *Creating Capacity in China*, http://www.airport-technology.com/features/feature560/.

20. See G. Kauvar, B. Rostker, and R. Shaver, *Safer Skies: Baggage Screening and Beyond with Supporting Analyses* (Santa Monica, CA: Rand Corporation, 2002).

21. R. A. Brooks and A. M. Flynn, "Fast, Cheap and Out of Control: A Robot Invasion of the Solar System." *Journal of the British Interplanetary Society* 42 (1989): 478–85.

22. Ibid., 478.

## REFERENCES

Advani, A., and A. Borins. 2001. "Managing Airports: A Test of the New Public Management." *International Public Management Journal* 4: 91–107.

Barnett, A. 2004. "CAPPS II: The Foundation of Aviation Security?" *Risk Analysis* 24: 909–16.

Bazerman, M. H., and M. Watkins. 2005. "Airline Security, the Failure of 9/11, and Predictable Surprises." *International Public Management Journal* 8: 376–77.

Bennett, C. J. 2008. "Comparative Politics of No-Fly Lists in the United States and Canada." In *Politics at the Airport*, ed. M. B. Salter, 88–122. Minneapolis, MN: University of Minneapolis Press.

Brooks, R. A., and A .M. Flynn. 1989. "Fast, Cheap and Out of Control: A Robot Invasion of the Solar System." *Journal of the British Interplanetary Society* 42: 478–85.

"Creating Capacity in China." 2005. Aviation Technology.com. Available at: http://www.airport-technology.com/features/feature560/.

Dempsey, P. S. 2003. "Aviation Security: The Role of Law in the War on Terror." *Columbia Journal of Transnational Law* 41: 649–733.

Elhefnawy, N. 2004. "Societal Complexity and Diminishing Returns in Security." *International Security* 29: 152–74.

Ghobrial, A., and W. A. Irvin. 2004. "Combating Air Terrorism: Some Implications for the Aviation Industry." *Journal of Air Transportation* 9: 67–86.

Hainmüller, J., and J. M. Lemnitzer. 2003. "Why Do Europeans Fly Safer? The Politics of Airport Security in Europe and the US." *Terrorism and Political Violence* 15: 1–36.

Kauvar, G., B. Rostker, and R. Shaver. 2002. *Safer Skies: Baggage Screening and Beyond with Supporting Analyses.* Santa Monica: Rand Corporation.

Kutz, G. D., and J. W. Cooney. 2007. "Aviation Security: Vulnerabilities Exposed through Covert Testing of TSA's Passenger Screening Process." Testimony before the Committee on Oversight and Government Reform, House of Representatives. Government Accountability Office (GAO-08–48T).

Mason, K. J. 2005. "Observations of Fundamental Changes in the Demand for Aviation Services." *Journal of Air Transport Management* 11: 19–25.

Mason., K. J. 2001. "Marketing Low-Cost Airline Services to Business Travelers." *Journal of Air Transport Management* 7: 103–9.

Salter, M .B. 2007. "SeMS and Sensibility: Security Management Systems and the Management of Risk in the Canadian Air Transport Security Authority." *Journal of Air Transport Management* 13: 389–98.

Salter, M. B. 2008. "Managing the Global Airport." In *Politics at the Airport*, ed. M. B. Salter, 25–71. Minneapolis, MN: University of Minnesota Press, 25–71.

Standing Senate Committee on National Security and Defence. 2003. *The Myth of Security at Canada's Airports.* Ottawa: Senate of Canada.

Standing Senate Committee on National Security and Defence. 2007. *Canadian Security Guidebook: An Update of Security Problems in Search of Solutions. Airports.* Ottawa: Senate of Canada.

Wheeler, J. 2005. *An Independent Review of Airport Security and Policing for the Government of Australia.* Melbourne: Commonwealth of Australia.

Zacher, M., with B. Sutton. 1996. *Governing Global Networks: International Regimes for Transportation and Communications.* Cambridge: Cambridge University Press.

# DHS Has Made Progress in Securing the Commercial Aviation System, but Key Challenges Remain

*Statement of Cathleen A. Berrick, Director*
*Homeland Security and Justice Issues*

Madam Chair and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing to discuss the Department of Homeland Security's (DHS) progress and challenges in securing our nation's aviation system. The Transportation Security Administration (TSA), originally established as an agency within the Department of Transportation in 2001 but now a component within DHS, is charged with securing the transportation network while also ensuring the free movement of people and commerce. TSA has primary responsibility for security in all modes of transportation and since its inception has developed and implemented a variety of programs and procedures to secure the commercial aviation system. Other DHS components, federal agencies, state and local governments, and the private sector also play a role in aviation security. For example, the U.S. Customs and Border Protection (CBP) has responsibility for conducting passenger prescreening—in general, the matching of passenger information against terrorist watch lists prior to an aircraft's departure—for international flights operating to or from the United States, as well as inspecting inbound air cargo upon its arrival in the United States. In accordance with TSA requirements, airport authorities are responsible for implementing measures to secure access to restricted airport areas as well as airport perimeters, while air carriers are responsible for inspecting air cargo, among other things.

My testimony today will focus on: (1) the progress TSA and other DHS components have made in securing the nation's commercial aviation system and (2) challenges that have impeded DHS's (and, as they relate to transportation security, TSA) efforts to implement its mission and management functions. My comments are based on issued GAO reports and testimonies

addressing the security of the nation's aviation system, including an August 2007 report that highlights the progress DHS has made in implementing its mission and management functions.[1] In this report, we reviewed the extent to which DHS has taken actions to achieve performance expectations in each of its mission and management areas that we identified from legislation, Homeland Security Presidential Directives, and DHS strategic planning documents. Based primarily on our past work, we made a determination regarding whether DHS generally achieved or generally did not achieve the key elements of each performance expectation. An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation; however, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, an assessment of "generally not achieved" indicates that DHS has not yet taken actions to satisfy most elements of the performance expectation. In determining the department's overall level of progress in achieving performance expectations in each of its mission and management areas, we concluded whether the department had made limited, modest, moderate, or substantial progress.[2] These assessments of progress do not reflect, nor are they intended to reflect, the extent to which actions by DHS and its components have made the nation more secure. We conducted our work in accordance with generally accepted government auditing standards.

## SUMMARY

Within DHS, TSA is the agency with primary responsibility for securing the transportation sector and has undertaken a number of initiatives to strengthen the security of the nation's commercial aviation system. In large part, these efforts have been driven by legislative mandates designed to strengthen the security of commercial aviation following the September 11, 2001, terrorist attacks. In August 2007, we reported that DHS had made moderate progress in securing the aviation transportation network, but that more work remains.[3] Specifically, of the 24 performance expectations we identified for DHS in the

1. GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: August 2007); GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-1081T (Washington, D.C.: September 2007); and GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-1240T (Washington, D.C.: September 2007).

2. Limited progress: DHS has taken actions to generally achieve 25 percent or less of the identified performance expectations. Modest progress: DHS has taken actions to generally achieve more than 25 percent but 50 percent or less of the identified performance expectations. Moderate progress: DHS has taken actions to generally achieve more than 50 percent but 75 percent or less of the identified performance expectations. Substantial progress: DHS has taken actions to generally achieve more than 75 percent of the identified performance expectations.

3. GAO-07-454.

area of aviation security, we reported that it has generally achieved 17 of these expectations and has generally not achieved 7 expectations.

DHS, primarily through TSA, has made progress in many areas related to securing commercial aviation, and their efforts should be commended. Meeting statutory mandates to screen airline passengers and 100 percent of checked baggage alone was a tremendous challenge. To do this, TSA initially hired and deployed a federal workforce of over 50,000 passenger and checked baggage screeners, and installed equipment at the nation's more than 400 commercial airports to provide the capability to screen all checked baggage using explosive detection systems, as mandated by law. TSA has since turned its attention to, among other things, strengthening passenger prescreening—in general, the matching of passenger information against terrorist watch lists prior to an aircraft's departure; more efficiently allocating, deploying, and managing the transportation security officer (TSO)—formerly known as screener—workforce; strengthening screening procedures; developing and deploying more effective and efficient screening technologies; and improving domestic air cargo security. In addition to TSA, CBP has also taken steps to strengthen passenger prescreening for passengers on international flights operating to or from the United States, as well as inspecting inbound air cargo upon its arrival in the United States. DHS's Science and Technology (S&T) Directorate has also taken actions to research and develop aviation security technologies.

While these efforts have helped to strengthen the security of the commercial aviation system, DHS still faces a number of key challenges that need to be addressed to meet expectations set out for them by the Congress, the Administration, and the Department itself. For example, TSA has faced challenges in developing and implementing its passenger prescreening system, known as Secure Flight, and has not yet completed development efforts. As planned, this program would initially assume from air carriers the responsibility for matching information on airline passengers traveling domestically against terrorists watch lists. In addition, while TSA has taken actions to enhance perimeter security at airports, these actions may not be sufficient to provide for effective security. TSA has also begun efforts to evaluate the effectiveness of security-related technologies, such as biometric identification systems. However, TSA has not developed a plan for implementing new technologies to meet the security needs of individual airports and the commercial airport system as a whole. Further, TSA has not yet deployed checkpoint technologies to address key existing vulnerabilities, and has not yet developed and implemented technologies needed to screen air cargo.

A variety of cross-cutting issues have affected DHS's and, as they relate to transportation security, TSA's efforts in implementing its mission and management functions. These key issues include agency transformation, strategic planning and results management, risk management, information sharing, and stakeholder coordination. In working towards transforming the department into an effective and efficient organization, DHS and its components have not always been transparent, which has affected our ability to perform

our oversight responsibilities in a timely manner. They have also not always implemented effective strategic planning efforts, fully developed performance measures, or put into place structures to help ensure that they are managing for results. In addition, DHS and its components can more fully adopt and apply a risk management approach in implementing its security mission and core management functions.[4] They could also better share information with federal, state, and local governments and private sector entities, and more fully coordinate its activities with key stakeholders.

## BACKGROUND

The Aviation and Transportation Security Act (ATSA), enacted in November 2001, created TSA and gave it responsibility for securing all modes of transportation.[5] TSA's aviation security mission includes strengthening the security of airport perimeters and restricted airport areas; hiring and training a screening workforce; prescreening passengers against terrorist watch lists; and screening passengers, baggage, and cargo at the over 400 commercial airports nation-wide, among other responsibilities. While TSA has operational responsibility for physically screening passengers and their baggage, TSA exercises regulatory, or oversight, responsibility for the security of airports and air cargo. Specifically, airports, air carriers, and other entities are required to implement security measures in accordance with TSA-issued security requirements, against which TSA evaluates their compliance efforts.

TSA also oversees air carriers' efforts to prescreen passengers—in general, the matching of passenger information against terrorist watch lists—prior to an aircraft's departure. TSA plans to take over operational responsibility for this function with the implementation of its Secure Flight program initially for passengers traveling domestically. CBP has responsibility for conducting passenger prescreening for airline passengers on international flights departing from and bound for the United States,[6] while DHS's Science and Technology Directorate is responsible for researching and developing technologies to secure the transportation sector.

---

4. A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives.

5. Pub. L. No. 107-71, 115 Stat. 597 (2001).

6. Currently, air carriers departing the United States are required to transmit passenger manifest information to CBP no later than 15 minutes prior to departure but, for flights bound for the United States, air carriers are not required to transmit the information until 15 minutes after the flight's departure (in general, after the aircraft is in flight). See 19 C.F.R. §§ 122.49a, 122.75a. In a final rule published in the *Federal Register* on August 23, 2007, CBP established a requirement for all air carriers to either transmit the passenger manifest information to CBP no later than 30 minutes prior to the securing of the aircraft doors (that is, prior to the flight being airborne), or transmit manifest information on an individual basis as each passenger checks in for the flight up to but no later than the securing of the aircraft. See 72 Fed. Reg. 48,320 (Aug. 23, 2007). This requirement is to take effect on February 19, 2008.

## DHS Has Made Progress in Securing the Nation's Commercial Aviation System, but More Work Remains

DHS, primarily through the efforts of TSA, has undertaken numerous initiatives since its inception to strengthen the security of the nation's commercial aviation system. In large part, these efforts have been affected by legislative mandates designed to strengthen the security of commercial aviation following the September 11, 2001 terrorist attacks. These efforts have also been affected by events external to the department, including the alleged August 2006 terrorist plot to blow up commercial aircraft bound from London to the United States. For example, TSA has undertaken efforts to hire, train, and deploy a screening workforce; and screen passengers, baggage, and cargo. Although TSA has taken important actions to strengthen aviation security, the agency has faced difficulties in implementing an advanced, government-run passenger prescreening program for domestic flights, and in developing and implementing technology to screen passengers at security checkpoints and cargo placed on aircraft, among other areas. As shown in table 1, we identified 24 performance expectations for DHS in the area of aviation security, and found that overall, DHS has made moderate progress in meeting these expectations. Specifically, we found that DHS has generally achieved 17 performance expectations and has generally not achieved 7 performance expectations. We identified these performance expectations through reviews of key legislation, Homeland Security Presidential Directives, and DHS strategic planning documents.

### *Aviation Security Strategic Approach*

We concluded that DHS has generally achieved this performance expectation. In our past work, we reported that TSA identified and implemented a wide range of initiatives to strengthen the security of key components of the commercial aviation system. These components are interconnected and each is critical to the overall security of commercial aviation.[7] More recently, in March 2007, TSA released its National Strategy on Aviation Security and six supporting plans that provided more detailed strategic planning guidance in the areas of systems security; operational threat response; systems recovery; domain surveillance; and intelligence integration and domestic and international outreach. According to TSA officials, an Interagency Implementation Working Group was established under TSA leadership in January 2007 to initiate implementation efforts for the 112 actions outlined in the supporting plans.

7. For more information, see GAO, *Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain*, GAO-06-371T (Washington, D.C: April 2006).

**Table 1**
**Performance Expectations and Progress Made in Aviation Security**

| | *Assessment* | | |
|---|---|---|---|
| *Performance expectation* | *Generally achieved* | *Generally not achieved* | *No assessment made* |
| **Aviation security strategic approach** | | | |
| Implement a strategic approach for aviation security functions | | | |
| **Airport perimeter security and access controls** | | | |
| Establish standards and procedures for effective airport perimeter security | | | |
| Establish standards and procedures to effectively control access to airport secured areas | | | |
| Establish procedures for implementing biometric identifier systems for airport secured areas access control | | | |
| Ensure the screening of airport employees against terrorist watch lists | | | |
| **Aviation security workforce** | | | |
| Hire and deploy a federal screening workforce | | | |
| Develop standards for determining aviation security staffing at airports | | | |
| Establish standards for training and testing the performance of airport screener staff | | | |
| Establish a program and requirements to allow eligible airports to use a private screening workforce | | | |
| Train and deploy federal air marshals on high-risk flights | | | |
| Establish standards for training flight and cabin crews | | | |
| Establish a program to allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts | | | |

| | | | |
|---|---|---|---|
| **Passenger prescreening** | | | |
| Establish policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action | | | |
| Develop and implement an advanced prescreening system t o allow DHS to compare domestic passenger information to the Selectee List and No Fly List | | | |
| Develop and implement an international passenger prescreening process to compare passenger information to terrorist watch lists before aircraft departure | | | |
| **Checkpoint screening** | | | |
| Develop and implement processes and procedures for physically screening passengers at airport checkpoints | | | |
| Develop and test checkpoint technologies to address vulnerabilities | | | |
| Deploy checkpoint technologies to address vulnerabilities | | | |
| **Checked Baggage screening** | | | |
| Deploy explosive detection systems (EDS) and explosive trace detection (ETD) systems to screen checked baggage for explosives | | | |
| Develop a plan to deploy in-line baggage screening equipment at airports | | | |
| Pursue the deployment and use of in-line baggage screening equipment at airports | | | |
| **Air cargo security** | | | |
| Develop a plan for air cargo security | | | |
| Develop and implement procedures to screen air cargo | | | |
| Develop and implement technologies to screen air cargo | | | |
| **Total** | **17** | **7** | **0** |

*Source:* GAO analysis.

### *Airport Perimeter Security and Access Controls*

We concluded that DHS has generally achieved one, and has generally not achieved three, of the performance expectations in this area. For example, TSA has taken action to ensure the screening of airport employees against terrorist watch lists by requiring airport operators to compare applicants' names against the No Fly and Selectee Lists.[8] However, in June 2004, we reported that although TSA had begun evaluating commercial airport perimeter and access control security through regulatory compliance inspections, covert testing of selected access procedures, and vulnerability assessments at selected airports, TSA had not determined how the results of these evaluations could be used to make improvements to the nation's airport system as a whole. We further reported that although TSA had begun evaluating the controls that limit access into secured airport areas, it had not completed actions to ensure that all airport workers in these areas were vetted prior to being hired and trained.[9] More recently, in March 2007, the DHS Office of Inspector General, based on the results of its access control testing at 14 domestic airports across the nation, made various recommendations to enhance the overall effectiveness of controls that limit access to airport secured areas.[10] In March through July 2007, DHS provided us with updated information on procedures, plans, and other efforts it had implemented to secure airport perimeters and strengthen access controls, including a description of its Aviation Direct Access Screening Program. This program provides for TSOs to randomly screen airport and airline employees and employees' property and vehicles as they enter the secured areas of airports for the presence of explosives, incendiaries, weapons, and other items of interest as well as improper airport identification. However, DHS did not provide us with evidence that these actions provide for effective airport perimeter security, nor information on how the actions addressed all relevant requirements established by law and in our prior recommendations.

Regarding procedures for implementing biometric identification systems, we reported that TSA had not developed a plan for implementing new technologies to meet the security needs of individual airports and the commercial airport system as a whole.[11]

---

8. For more information, see GAO, Aviation Security: Transportation Security Administration Has Made Progress in Managing a Federal Security Workforce and Ensuring Security at U.S. Airports, but Challenges Remain, GAO-06-597T (Washington, D.C.: April 2006) and GAO, Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls, GAO-04-728 (Washington, D.C.: June 2004).
9. GAO-06-597T and GAO-04-728.
10. Department of Homeland Security Office of Inspector General, Audit of Access to Airport Secured Areas (Unclassified Summary), OIG-07-35 (Washington, D.C.: March 2007).
11. GAO-06-597T and GAO-04-728.

In December 2004 and September 2006, we reported on the status of the development and testing of the Transportation Worker Identification Credential program (TWIC)[12]—DHS's effort to develop biometric access control systems to verify the identity of individuals accessing secure transportation areas. Our 2004 report identified challenges that TSA faced in developing regulations and a comprehensive plan for managing the program, as well as several factors that caused TSA to miss initial deadlines for issuing TWIC cards. In our September 2006 report, we identified the challenges that TSA encountered during TWIC program testing, and several problems related to contract planning and oversight. Specifically, we reported that DHS and industry stakeholders faced difficult challenges in ensuring that biometric access control technologies will work effectively in the maritime environment where the Transportation Worker Identification Credential program is being initially tested. In October 2007, we testified that TSA had made progress in implementing the program and addressing our recommendations regarding contract planning and oversight and coordination with stakeholders. For example, TSA reported that it added staff with program and contract management expertise to help oversee the contract and developed plans for conducting public outreach and education efforts.[13] However, DHS has not yet determined how and when it will implement a biometric identification system for access controls at commercials airports. We have initiated ongoing work to further assess DHS's efforts to establish procedures for implementing biometric identifier systems for airport secured areas access control.

### *Aviation Security Workforce*

We concluded that DHS has generally achieved all 7 performance expectations in this area. For example, TSA has hired and deployed a federal screening workforce at over 400 commercial airports nationwide, and has developed standards for determining TSO staffing levels at airports. TSA also established numerous programs to train and test the performance of its TSO workforce, although we reported that improvements in these efforts can be made. Among other efforts, in December 2005, TSA reported completing enhanced explosives detection training for over 18,000 TSOs, and increased its use of covert testing to assess vulnerabilities of existing screening systems. TSA also established the Screening Partnership Program which allows eligible airports to apply to TSA to use a private screening workforce. In addition, TSA has trained and deployed federal air marshals on high-risk flights; established standards for training flight

12. GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (Washington, D.C.: December 2004), and *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: September 2006).
13. GAO, *Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Seaports*, GAO-08-86T (Washington, D.C. October 4, 2007).

and cabin crews; and established a Federal Flight Deck Officer program to select, train, and allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts. Related to flight and cabin crew training, TSA revised its guidance and standards to include additional training elements required by law and improve the organization and clarity of the training. TSA also increased its efforts to measure the performance of its TSO workforce through recertification testing and other measures.

### *Passenger Prescreening*

We reported that DHS has generally achieved one, and has not generally achieved two, of the performance expectations in this area. For example, TSA established policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action. Specifically, TSA requires that air carriers check all passengers against the Selectee List, which identifies individuals that represent a higher than normal security risk and therefore require additional security screening, and the No Fly List, which identifies individuals who are not allowed to fly.[14] However, TSA has faced a number of challenges in developing and implementing an advanced prescreening system, known as Secure Flight, which will allow TSA to take over the matching of passenger information against the No Fly and Selectee lists from air carriers, as required by law.[15] In 2006, we reported that TSA had not conducted critical activities in accordance with best practices for large-scale information technology programs and had not followed a disciplined life cycle approach in developing Secure Flight.[16] In March 2007, DHS reported that as a result of its rebaselining efforts, more effective government controls were developed to implement Secure Flight and that TSA was following a more disciplined development process. DHS further reported that it plans to begin parallel operations with the first group of domestic air carriers during fiscal year 2009 and to take over full responsibility for watch list matching in fiscal year 2010. We are continuing to assess TSA's efforts in developing and implementing the Secure Flight program. We have also reported that DHS has not yet implemented enhancements to its passenger prescreening process for passengers on international flights departing from and bound for the United States.[17] Although CBP recently issued a final rule that will require air carriers

14. In accordance with TSA-issued security requirements, passengers on the No Fly List are denied boarding passes and are not permitted to fly unless cleared by law enforcement officers. Similarly, passengers who are on the Selectee List are issued boarding passes, and they and their baggage undergo additional security measures.

15. See 49 U.S.C. § 44903(j)(2)(C).

16. GAO, *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program*, GAO-06-864T (Washington, D.C.: June 2006).

17. GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains*, GAO-07-448T (Washington, D.C.: February 2007) and GAO, *Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain*, GAO-07-346 (Washington, D.C.: May 2007).

to provide passenger information to CBP prior to a flight's departure so that CBP can compare passenger information to the terrorist watch lists before a flight takes off, this requirement is not scheduled to take effect until February 2008. In addition, while DHS plans to align its international and domestic passenger prescreening programs under TSA, full implementation of an integrated system will not occur for several years.

### *Checkpoint Screening*

We reported that DHS has generally achieved two, and has not generally achieved one, of the performance expectations in this area. For example, we reported that TSA has developed processes and procedures for screening passengers at security checkpoints and has worked to balance security needs with efficiency and customer service considerations.[18] More specifically, in April 2007, we reported that modifications to standard operating procedures were proposed based on the professional judgment of TSA senior-level officials and program-level staff, as well as threat information and the results of covert testing. However, we found that TSA's data collection and analyses could be improved to help TSA determine whether proposed procedures that are operationally tested would achieve their intended purpose. We also reported that DHS and its component agencies have taken steps to improve the screening of passengers to address new and emerging threats. For example, TSA established two recent initiatives intended to strengthen the passenger checkpoint screening process: (1) the Screening Passenger by Observation Technique program, which is a behavior observation and analysis program designed to provide TSA with a nonintrusive means of identifying potentially high-risk individuals; and the (2) Travel Document Checker program which replaces current travel document checkers with TSOs who have access to sensitive security information on the threats facing the aviation industry and check for fraudulent documents. However, we found that while TSA has developed and tested checkpoint technologies to address vulnerabilities that may be exploited by identified threats such as improvised explosive devices, it has not yet effectively deployed such technologies. In July 2006, TSA reported that it installed 97 explosives trace portal machines—which use puffs of air to dislodge and detect trace amounts of explosives on persons—at 37 airports. However, DHS identified problems

18. For more information, see GAO, Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved, GAO-07-634 (Washington, D.C.: May 2007); GAO, Aviation Security: TSA's Change to Its Prohibited Items List Has Not Resulted in Any Reported Security Incidents, but the Impact of the Change on Screening Operations Is Inconclusive, GAO-07-623R (Washington, D.C.: April 2007); GAO, Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining, GAO-03-1173 (Washington, D.C.: September 2003); and GAO, Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain, GAO-06-371T (Washington, D.C.: April 2006).

with these machines and has halted their deployment. TSA is also developing backscatter technology, which identifies explosives, plastics and metals, giving them shape and form and allowing them to be visually interpreted.[19] However, limited progress has been made in fielding this technology at passenger screening checkpoints. The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), enacted in August 2007, restates and amends a requirement that DHS issue a strategic plan for deploying explosive detection equipment at airport checkpoints and requires DHS to expedite research and develop efforts to protect passenger aircraft from explosives devices.[20] We are currently reviewing DHS and TSA's efforts to develop, test and deploy airport checkpoint technologies.[21]

### *Checked Baggage Screening*

We concluded that DHS has generally achieved all three performance expectations in this area. Specifically, from November 2001 through June 2006, TSA procured and installed about 1,600 Explosive Detection Systems (EDS) and about 7,200 Explosive Trace Detection (ETD) machines to screen checked baggage for explosives at over 400 commercial airports.[22] In response to mandates to field the equipment quickly and to account for limitations in airport design, TSA generally placed this equipment in a stand-alone mode—usually in airport lobbies—to conduct the primary screening of checked baggage for explosives.[23] Based in part on our previous recommendations, TSA later developed a plan to integrate EDS and ETD machines in-line with airport baggage conveyor systems. The installation of in-line systems can result in considerable savings to TSA through the reduction of TSOs needed to operate the equipment, as well as increased security. Despite delays in the widespread deployment of in-line systems due to the high upfront capital investment required, TSA is pursuing the installation of these systems and is seeking creative financing solutions to fund their deployment. In March 2007, DHS reported that it is working with airport and air carrier stakeholders to improve checked baggage screening solutions to enhance security and free up lobby space at airports. The installation of in-line baggage screening systems continues to be an issue

19. GAO-06-371T

20. See Pub. L. No. 110-53, §§1607, 1610, 121 Stat. 266, 483-85 (2007).

21. For more information, see GAO-06-371T.

22. Explosive detection systems (EDS) use specialized X-rays to detect characteristics of explosives that may be contained in baggage as it moves along a conveyor belt. Explosive trace detection (ETD) works by detecting vapors and residues of explosives. Human operators collect samples by rubbing swabs along the interior and exterior of an object that TSOs determine to be suspicious, and place the swabs in the ETD machine, which then chemically analyzes the swabs to identify any traces of explosive materials.

23. For more information, see GAO, *Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened*, GAO-06-869 (Washington, D.C.: July 2006), GAO-06-371T, and GAO-07-448T.

of congressional concern. For example, the 9/11 Commission Act reiterates a requirement that DHS submit a cost-sharing study along with a plan and schedule for implementing provisions of the study, and requires TSA to establish a prioritization schedule for airport improvement projects such as the installation of in-line baggage screening systems.[24]

### *Air Cargo Security*

We reported that TSA has generally achieved two, and has not generally achieved one, of the performance expectations in this area. Specifically, TSA has developed a strategic plan for domestic air cargo security and has taken actions to use risk management principles to guide investment decisions related to air cargo bound for the United States from a foreign country, referred to as inbound air cargo, but these actions are not yet complete. For example, TSA plans to assess inbound air cargo vulnerabilities and critical assets—two crucial elements of a risk-based management approach—but has not yet established a methodology or time frame for how and when these assessments will be completed.[25] TSA has also developed and implemented procedures to screen domestic and inbound air cargo. We reported in October 2005 that TSA had significantly increased the number of domestic air cargo inspections conducted of air carrier and indirect air carrier compliance with security requirements. However, we also reported that TSA exempted certain cargo from random inspection because it did not view the exempted cargo as posing a significant security risk, although air cargo stakeholders noted that such exemptions may create potential security risks and vulnerabilities since shippers may know how to package their cargo to avoid inspection.[26] In part based on a recommendation we made, TSA is evaluating existing exemptions to determine whether they pose a security risk, and has removed some exemptions that were previously allowed. The 9/11 Commission Act requires, no later than 3 years after its enactment, that DHS have a system in place to screen 100 percent of cargo transported on passenger aircraft.[27] Although TSA has taken action to develop plans for securing air cargo and establishing and implementing procedures to

24. See Pub. L. No. 110-53, § 1603-04, 121 Stat. at 480-81.

25. For more information, see GAO, Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security (Washington, D.C.: October 2005) and GAO, Aviation Security: Federal Efforts GAO-06-76*to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be Strengthened*, GAO-07-660 (Washington, D.C.: April 2007).

26. GAO-06-76.

27. See Pub. L. No. 110-53, § 1602, 121 Stat. at 477-79.This provision defines screening as a physical examination or non-intrusive method of assessing whether cargo poses a threat to transportation security that includes the use of technology, procedures, personnel, or other methods to provide a level of security commensurate with the level of security for the screening of passenger checked baggage. Methods such as solely performing a review of information about the contents of cargo or verifying the identity of a shipper of the cargo, including whether a known shipper is registered in TSA's known shipper database, do not constitute screening under this provision.

screen air cargo, DHS has not yet developed and implemented screening technologies. DHS is pursuing multiple technologies to automate the detection of explosives in the types and quantities that would cause catastrophic damage to an aircraft in flight. However, TSA acknowledged that full development of these technologies may take 5 to 7 years. In April 2007, we reported that TSA and DHS's S&T Directorate were in the early stages of evaluating and piloting available aviation security technologies to determine their applicability to the domestic air cargo environment. We further reported that although TSA anticipates completing its pilot tests by 2008, it has not yet established time frames for when it might implement these methods or technologies for the inbound air cargo system.[28]

## Cross-cutting Issues Have Hindered DHS's Efforts in Implementing Its Mission and Management Functions

Our work has identified homeland security challenges that cut across DHS's mission and core management functions. These issues have impeded the department's progress since its inception and will continue as DHS moves forward. While it is important that DHS continue to work to strengthen each of its mission and core management functions, to include aviation security, it is equally important that these key issues be addressed from a comprehensive, department-wide perspective to help ensure that the department has the structure and processes in place to effectively address the threats and vulnerabilities that face the nation. These issues include: (1) transforming and integrating DHS's management functions; (2) establishing baseline performance goals and measures and engaging in effective strategic planning efforts; (3) applying and strengthening a risk management approach for implementing missions and making resource allocation decisions; (4) sharing information with key stakeholders; and (5) coordinating and partnering with federal, state and local, and private sector agencies. We have made numerous recommendations to DHS to strengthen these efforts, and the department has made progress in implementing some of these recommendations.

DHS has faced a variety of difficulties in its efforts to transform into a fully functioning department. We designated DHS's implementation and transformation as high-risk in part because failure to effectively address this challenge could have serious consequences for our security and economy. DHS continues to face challenges in key areas, including acquisition, financial, human capital, and information technology management. This array of management and programmatic challenges continues to limit DHS's ability to effectively and efficiently carry out its mission. In addition, transparency plays an important role in helping to ensure effective and efficient transformation efforts. We have reported that DHS has not made its management or operational decisions

28. GAO-07-660.

transparent enough so that Congress can be sure it is effectively, efficiently, and economically using the billions of dollars in funding it receives annually. More specifically, in April 2007, we testified that we have encountered access issues during numerous engagements at DHS, including significant delays in obtaining requested documents that have affected our ability to do our work in a timely manner.[29] The Secretary of DHS and the Under Secretary for Management have stated their desire to work with us to resolve access issues and to provide greater transparency. It will be important for DHS and its components to become more transparent and minimize recurring delays in providing access to information on its programs and operations so that Congress, GAO, and others can independently assess its efforts.

In addition, DHS has not always implemented effective strategic planning efforts and has not yet fully developed performance measures or put into place structures to help ensure that the agency is managing for results. We have identified strategic planning as one of the critical success factors for new organizations, and reported that both DHS's and TSA's efforts in this area have been mixed. For example, with regards to TSA's efforts to secure air cargo, we reported that TSA completed an Air Cargo Strategic Plan in November 2003 that outlined a threat-based risk management approach to securing the nation's domestic air cargo system, and that this plan identified strategic objectives and priority actions for enhancing air cargo security based on risk, cost, and deadlines. However, we reported that TSA had not developed a similar strategy for addressing the security of inbound air cargo—cargo transported into the United States from foreign countries, including how best to partner with CBP and international air cargo stakeholders. In another example, we reported that TSA had not yet developed outcome-based performance measures for its foreign airport assessment and air carrier inspection programs, such as the percentage of security deficiencies that were addressed as a result of TSA's on-site assistance and recommendations, to identify any aspects of these programs that may need attention. We recommended that DHS direct TSA and CBP to develop a risk-based strategy, including specific goals and objectives, for securing air cargo;[30] and develop outcome-based performance measures for its foreign airport assessment and air carrier inspection programs.[31] DHS generally concurred with GAO's recommendations.

DHS has also not fully adopted and applied a risk management approach in implementing its mission and core management functions. Risk management has been widely supported by the President and Congress as an approach for

29. GAO, *Department of Homeland Security: Observations on GAO Access to Information on Programs and Activities*, GAO-07-700T (Washington, D.C.: April 2007).
30. GAO-07-660.
31. GAO, *Aviation Security: Foreign Airport Assessments and Air Carrier Inspections Help Enhance Security, but Oversight of These Efforts Can Be Strengthened*, GAO-07-729 (Washington, D.C.: May 11, 2007).

allocating resources to the highest priority homeland security investments, and the Secretary of Homeland Security and the Assistant Secretary for Transportation Security have made it a centerpiece of DHS and TSA policy. Several DHS component agencies and TSA have worked towards integrating risk-based decision making into their security efforts, but we reported that these efforts can be strengthened. For example, TSA has incorporated certain risk management principles into securing air cargo, but has not completed assessments of air cargo vulnerabilities or critical assets—two crucial elements of a risk-based approach without which TSA may not be able to appropriately focus its resources on the most critical security needs. TSA has also incorporated risk-based decision making when making modifications to airport checkpoint screening procedures, to include modifying procedures based on intelligence information and vulnerabilities identified through covert testing at airport checkpoints. However, in April 2007 we reported that TSA's analyses that supported screening procedural changes could be strengthened. For example, TSA officials decided to allow passengers to carry small scissors and tools onto aircraft based on their review of threat information—which indicated that these items do not pose a high risk to the aviation system—so that TSOs could concentrate on higher threat items.[32] However, TSA officials did not conduct the analysis necessary to help them determine whether this screening change would affect TSO's ability to focus on higher-risk threats.[33]

We have further reported that opportunities exist to enhance the effectiveness of information sharing among federal agencies, state and local governments, and private sector entities. In August 2003, we reported that efforts to improve intelligence and information sharing need to be strengthened, and in 2005, we designated information sharing for homeland security as high-risk.[34] In January 2005, we reported that the nation still lacked an implemented set of government-wide policies and processes for sharing terrorism-information, but DHS has issued a strategy on how it will put in place the overall framework, policies, and architecture for sharing information with all critical partners—actions that we and others have recommended.[35] DHS has taken some steps to implement its information sharing responsibilities. States and localities are also creating their own information "fusion" centers, some with DHS support. With respect to aviation security, the importance of information sharing was recently highlighted in the 9/11 Commission Act, which requires DHS to establish a plan to promote the sharing of transportation security

32. GAO, *Aviation Security: Risk, Experience, and Customer Concerns*, GAO-07-634 (Washington, D.C.: May 2007).

33. GAO, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved*, GAO-07-634 (Washington, D.C.: April 16, 2007).

34. GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: August 2003) and GAO, *HIGH-RISK SERIES: An Update* GAO-05-207 (Washington, D.C.: January 2005).

35. GAO-07-454.

information among DHS and federal, state and local agencies, tribal governments, and appropriate private entities.[36] The Act also requires that DHS provide timely threat information to carriers and operators that are preparing and submitting a vulnerability assessment and security plan, including an assessment of the most likely methods that could be used by terrorists to exploit weaknesses in their security.[37]

In addition to providing federal leadership with respect to homeland security, DHS also plays a large role in coordinating the activities of key stakeholders, but has faced challenges in this regard. To secure the nation, DHS must form effective and sustained partnerships between legacy component agencies and a range of other entities, including other federal agencies, state and local governments, the private and nonprofit sectors, and international partners. We have reported that successful partnering and coordination involves collaborating and consulting with stakeholders to develop and agree on goals, strategies, and roles to achieve a common purpose; identify resource needs; establish a means to operate across agency boundaries, such as compatible procedures, measures, data, and systems; and agree upon and document mechanisms to monitor, evaluate, and report to the public on the results of joint efforts.[38] We have found that the appropriate homeland security roles and responsibilities within and between the levels of government, and with the private sector, are evolving and need to be clarified. For example, we reported that opportunities exists for TSA to work with foreign governments and industry to identify best practices for securing air cargo, and recommended that TSA systematically compile and analyze information on practices used abroad to identify those that may strengthen the department's overall security efforts.[39] Further, regarding efforts to respond to in-flight security threats, which—depending on the nature of the threat—could involve 15 federal agencies and agency components, we recommended that DHS and other departments document and share their respective coordination and communication strategies and response procedures.[40]

## CONCLUDING OBSERVATIONS

The magnitude of DHS's and more specifically TSA's responsibilities in securing the nation's commercial aviation system is significant, and we commend the department on the work it has done and is currently doing to secure this network. Nevertheless, given the dominant role that TSA plays in securing the

36. See Pub. L. No. 110-53, § 1203, 121 Stat. at 383-86.
37. See Pub. L. No. 110-53, §§ 1512(d)(2), 1531(d)(2), 121 Stat. at 430, 455.
38. GAO, *Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security*, GAO-07-833T (Washington, D.C.: May 2007).
39. GAO-07-660.
40. GAO, Aviation Security: Federal Coordination for Responding to In-flight Security Threats Has Matured, but Procedures Can Be Strengthened (Washington, D.C.: July 31, 2007). GAO-07-891R

homeland, it is critical that its programs and initiatives operate as efficiently and effectively as possible. In the almost 6 years since its creation, TSA has had to undertake its critical mission while also establishing and forming a new agency. At the same time, a variety of factors, including threats to and attacks on aviation systems around the world, as well as new legislative requirements, has led the agency to reassess its priorities and reallocate resources to address key events, and to respond to emerging threats. Although TSA has made considerable progress in addressing key aspects of commercial aviation security, more work remains in the areas of checkpoint and air cargo technology, airport security, and passenger prescreening. As DHS and TSA and other components move forward, it will be important for the department to work to address the challenges that have affected its operations thus far, including developing results-oriented goals and measures to assess performance; developing and implementing a risk-based approach to guide resource decisions; and establishing effective frameworks and mechanisms for sharing information and coordinating with homeland security partners. A well-managed, high-performing TSA is essential to meeting the significant challenge of securing the transportation network. As TSA continues to evolve, implement its programs, and integrate its functions, we will continue to review its progress and performance and provide information to Congress and the public on its efforts.

Madam Chair, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

## GAO CONTACT AND STAFF ACKNOWLEDGMENTS

For further information on this testimony, please contact Cathleen Berrick at (202) 512-3404 or at berrickc@gao.gov. Individuals making key contributions to this testimony include Steve D. Morris, Assistant Director, Gary Malavenda, Susan Langley, and Linda Miller.

October 16, 2007.

# Index

*This page intentionally left blank*

# About the Editor and Contributors

ANDREW R. THOMAS is assistant professor of marketing and international business and associate director of the Taylor Institute for Direct Marketing at the University of Akron. He is founding editor-in-chief of the *Journal of Transportation Security*, the first peer-reviewed journal dedicated to the study and practice of this critical business component. A *New York Times* best-selling writer, Dr. Thomas is author, coauthor, or editor of:

- *Supply Chain Security and Innovation*
- *The Distribution Trap!*
- *Global Manifest Destiny: Growing Your Business in a Borderless Economy*
- *Direct Marketing in Action: Proven Strategies for Finding and Keeping Your Best Customers*
- *The New World Marketing*
- *Growing Your Business in Emerging Markets: Promise & Perils*
- *The Rise of Women Entrepreneurs: People, Processes, and Global Trends*
- *Defining the Really Great Boss*
- *Managing by Accountability: What Every Leader Needs to Know About Responsibility, Integrity—and Results*
- *Change or Die! How to Transform Your Organization from the Inside Out*
- *Aviation Security Management*
- *Aviation Insecurity: The New Challenges of Air Travel*
- *Air Rage: Crisis in the Skies*

Dr. Thomas has published articles in leading management journals such as *MIT Sloan Management Review*, *Business Horizons*, and *Marketing Management*.

He is a regularly featured analyst for BBC, UNIVISION, FOX NEWS, and CNBC. He has been interviewed by more than 800 television and radio stations around the world. A successful global entrepreneur, Professor Thomas has traveled to and done business in more than 120 countries on all seven continents.

GARY E. ELPHINSTONE, adviser to the editor, is currently managing director of AVSEC AusAsia Pty Ltd., an international aviation security consultancy. Elphinstone's distinguished career in aviation began with the Royal Australian Air Force, where he specialized in signals intelligence and communications. During his service, he was promoted to serve at the British GCHQ, Hong Kong, for two and half years and, later, served as a fully rated flight services officer with the then Australian Department of Civil Aviation (DCA), working out of Sydney International Airport, Airways Operations. This was followed with an engagement to NASA at the deep space tracking station DSS 42, participating as electronics communications technician in a support role for the Apollo missions 8–13 and other NASA Deep Space Network programs. He rejoined the Federal Department of Aviation's Security Branch in 1978 and subsequently was chosen for an assignment with ICAO (the International Civil Aviation Organization) as aviation security adviser team leader with the aviation security project team, based in Thailand. The ICAO project (RAS 087/003) provided assistance to some 23 countries with a purpose of enhancing the capabilities of the governments in the region to minimize acts of unlawful interference against civil aviation. This was the forerunner to the current ICAO USAP (Universal Security Audit Programme). Elphinstone retired from government service in 1997 as superintendent AVSEC Western Region, after 19 years. He resides with his family in Perth, Australia.

RUWANTISSA I. R. ABEYRATNE, FRAeS, DCL, PhD, LLM, LLB,. is coordinator, Air Transport Programmes, at the International Civil Aviation Organization in Montreal.

ANTON BOLFING is a doctoral student at Max Planck Institute for Biological Cybernetics, Tübingen, Germany, and the University of Zurich, Switzerland. His main research topics are human factors in aviation security, applied vision research, psychophysics, digital image processing, and statistical modeling.

CHARLES M. BUMSTEAD has been involved in aviation affairs for 60 years, having spent a career as a fighter pilot in the U.S. military (USAF) and 27 years with the FAA, and a short seven-year career with ICAO (Bangkok) and IATA(Bangkok). He has specialized in international relations and international terrorism. His most publicized work was a paper on terrorism, "Selective Assassination: An Instrument of National Policy." An additional major publication was a treatise titled *Air Traffic Control in the 1990s*, produced in 1972. He is currently retired but is still deeply involved with international affairs. Educated at the University of Alabama, Troy University

(summa cum laude), and Inter-American University, he is a charter member of the Alpha Phi Chapter of Alpha Sigma Lambda (NHS) and is a distinguished graduate of the USAF Air War College.

ANTHONY T. H. CHIN. Prior to his return to the Department of Economics at the National University of Singapore in July 2004, Professor Chin was appointed as lead economist in the Economist Service at the Ministry of Trade and Industry. An NUS overseas merit scholar, he completed his PhD at Macquarie University, Australia, in discrete continuous choice methods. He is currently a member of the Public Transport Council and the Government Parliamentary Committee on Transport in Singapore and a fellow of AirNeth of the Netherlands. He is editor-in-chief of the *Journal of Logistics and Sustainable Transport* of the European Society of Logistics and Sustainable Transport and serves on the editorial boards of the *Journal of Air Transport Management*, *Asian Economy and Social Environment*, and the *Singapore Economic Review*. Among his areas of research specialization are consumer choice behavior (travel and crime); aviation economics; demand management and strategic planning of air hubs; and the economics of deviant behavior and personnel security. He has contributed articles to academic journals and presented papers at academic conferences and is a member of several international committees.

DAVID E. FORBES is a security analyst, having worked as an industry-based student of and advisor on aviation security since 1983. He has published a number of articles and white papers including the January 2004 paper, "Missing in Action—Aviation Security in America." His business and research work is conducted from bases in Denver, Colorado, and Perth, Western Australia. He is the cofounder and a director of Jagwa Forbes Group Pty. Ltd., an Australian consulting and training company specializing in emergency preparedness, safety training, and security risk management, with a major focus on aviation.

SASKIA M. KOLLER is a PhD student with the Visual Cognition Research Group of Prof. Dr. Adrian Schwaninger at the University of Zurich. In 2006, she finished her studies in psychology, business management, and criminology at the University of Zurich and is now writing her doctoral thesis in the field of airport security.

CHIEN-TSUNG LU teaches aviation system safety and risk management at the University of Central Missouri, Warrensburg, Missouri. He earned his PhD from the University of Nebraska and his MS from the University of Central Missouri. He is an FAA-certified aviation maintenance technician (A&P) and Federal Communication Commission licensee. Dr. Lu has numerous publications in aviation-related journals. His research and teaching interests are in the areas of aviation safety analysis, management models, and performance measurement.

CLINTON V. OSTER, JR., is professor and associate dean of the School of Public and Environmental Affairs, Indiana University. Professor Oster's

current research centers on air traffic management and aviation infrastructure, aviation safety, and airline economics and competition policy. His most recent book is *Managing the Skies: Public Policy, Organization, and Financing of Air Navigation*, with John S. Strong (Ashgate Press, 2008). He has also coauthored four books and numerous articles on aviation safety and various aspects of the U.S. airline industry. Professor Oster has served on multiple special study committees and expert panels for the National Academy of Sciences. He has been a consultant on aviation and other transportation issues to national governments, multilateral institutions, state and local governments, and private sector companies in the United States, Canada, the United Kingdom, Russia, and Australia. Professor Oster received a BSE from Princeton University, an MS from Carnegie-Mellon University, and a PhD from Harvard University.

JEFFREY IAN ROSS, PhD, is an associate professor in the Division of Criminology, Criminal Justice, and Social Policy, and a fellow of the Center for International and Comparative Law at the University of Baltimore. He has researched, written, and lectured on national security, political violence, political crime, violent crime, corrections, and policing for over two decades. Ross's work has appeared in many academic journals and books, as well as popular outlets. He is the author, coauthor, editor and coeditor of 12 books including most recently *Special Problems in Corrections* (Prentice Hall, 2008). Ross is a respected and frequent source of scholarly and scientific information for local, regional, national, and international news media, including interviews with newspapers and magazines and radio and television stations. Ross has also been featured on CNN and on the Fox News Network. Additionally Ross has written op-eds for the *Baltimore Sun*, the *Maryland Daily Record*, the *Baltimore Examiner*, and the *Tampa Tribune*. From 1995 to 1998, Ross was a social science analyst with the National Institute of Justice, a division of the U.S. Department of Justice. In 2003, he was awarded the University of Baltimore's Distinguished Chair in Research Award.

MARK B. SALTER is associate professor at the School of Political Studies, University of Ottawa. He received a master's degree from the London School of Economics and a doctorate from the University of British Columbia. He is currently associate editor of the *Journal of Transportation Security*, and has edited two books on airports, borders, and security: *Politics at the Airport* and *Global Policing and Surveillance* (with Elia Zureik). He is the author of *Rights of Passage: The Passport in International Relations* and has also published articles in *International Political Sociology*, *Alternatives*, *Security Dialogue*, and the *Journal of Air Transport Management*. Salter has acted as a consultant for the Canadian Air Transport Security Authority, Transport Canada, and the Canadian Human Rights Commission, and has presented papers at numerous conferences, including AVSEC World and the Canadian Aviation Security Conference. In 2007, he was the recipient of the National Capital Educator's Award and the Excellence in Education Prize at the University of Ottawa.

Prof. Dr. ADRIAN SCHWANINGER has lectured at the University of Zurich and at the Federal Institute of Technology (ETH) in Zurich since 1999 and at the University of Applied Sciences Northwestern Switzerland since 2008. He is a member of the Training and Technical Task Forces of the European Civil Aviation Conference (ECAC), the moderator of the ECAC Technical Task Force TIP Study Group, and the chairman of the InterTAG ad hoc Working Group on Competency Assessment. In 1999, he received the Young Researcher Award in Psychology. In 2003 he received the ASI International Award of Excellence in Aviation Security: Enhancement of Human Factors. Together with his Visual Cognition Research Group (VICOREG) he is in charge of several aviation security projects in Belgium, Bulgaria, Canada, France, Germany, Greece, Norway, Romania, Sweden, Switzerland, the Netherlands, and the United States of America.

TERRY A. SHERIDAN, MA, AFAIM, MRCSA, is managing director and founder of Guardian Angel, an employment service with offices in Australia and Singapore, which uses a unique emotional energy based methodology to assist employers and employees in the workplace. Originally, the business was set up in 2002 to assist the mature aged unemployed, specializing in managers and executives. Other services have been added that are more preventative in approach, for example, counseling, employee-retention programs, and executive screening services. More recently, her methodology has been applied in a number of different areas, including aviation security and financial fraud detection. Her clients are from North America, Europe, Asia, and Australia. Ms. Sheridan has a background in human services and business management; her past roles include those of CEO of an employment service for people with disabilities, financial and management services director of a large superannuation fund, and director of a university commercial arm. She has presented over 30 papers at national and international academic conferences and forums on a variety of topics. In 2005, she undertook a national investigation of unemployed women managers for the Australian Commonwealth Government. Her professional affiliations include the following: she is an associate fellow of the Australian Institute of Management, and holds professional memberships of the United Kingdom Institute of Career Guidance and the Australian Association of Career Counsellors. Ms. Sheridan is currently completing her PhD, on the impression management techniques of executive fraudsters, at the Graduate School of Business, Curtin University of Technology, Western Australia.

JOHN S. STRONG is the CSX Professor of Finance and Economics at the Mason School of Business, College of William and Mary. Strong's research interests are in aviation policy and transport finance. He has coauthored five books and many articles on air transport finance, operations, safety, and infrastructure. His most recent book is *Managing the Skies: Public Policy, Organization, and Financing of Air Navigation*, with Clinton V. Oster, Jr. (Ashgate Press, 2008). He has served as a consultant on aviation issues to multilateral

institutions and governments in the United States, Southeast Asia, China, Russia, India, Latin America, Africa, and Europe. Professor Strong received a BA from Washington and Lee University, and an MPP and PhD from Harvard University.

MICHAEL TUNNECLIFFE is an adjunct senior lecturer in counseling at the University of Notre Dame, Australia. In his professional practice, Michael is a clinical psychologist, specializing in crisis intervention and human behavioral issues, especially in relation to people in high-demand occupations with significant stress potential. As well as working with international and domestic airlines, he provides psychological support and educational services to law enforcement officers, emergency workers, and security personnel throughout Australia and New Zealand. Tunnecliffe is the author of *How to Understand and Manage Stress*, *How to Manage the Stress of Traumatic Incidents*, and *A Life in Crisis*. He is also the coauthor of *Emergency Support* and *Risky Practices*.