

THE Avascent REVIEW

No. 13

SEPTEMBER 2006

MIND THE GAP

Aviation Security Trends Since 9/11

This article was originally published in the Fall 2006 issue of *DFI Quarterly*, the predecessor publication to *THE Avascent REVIEW*



THE Avascent GROUP
analysis • vision • results

MIND THE GAP

Aviation Security Trends Since 9/11

BY DARYLE E. LADEMAN

Despite major changes to the nation's aviation security system since September 11, 2001, the United States remains vulnerable to large-scale terrorist attacks on civil aviation. These vulnerabilities are particularly disconcerting given continued terrorist fixation on civil aviation targets, as evidenced most recently by the foiled London-based plot to destroy commercial airliners en route over the Atlantic Ocean.

Even as the nation aspires to a robust, coherent, multi-tiered system, today's aviation security regime remains a hodgepodge of programmatic and technological responses to yesterday's threats. What is more, the default solution offered by the Transportation Security Administration (TSA) for addressing threats exposed since 9/11—including concerns about “shoe-bombs” and, now, the threat of liquid explosives—is to add yet more layers of universal passenger screening. At some point, the passenger screening system will become so burdensome that it will deter large numbers of travelers and cripple the airline industry, which is currently amid a tenuous return to profitability after a half-decade of financial turmoil.

Additional screens and searches cannot remain

the default response for fixing gaps in the aviation security system in the long term. Aviation security stakeholders—including the airlines, TSA, Congress, and industry—must work together to develop a rational, multi-tiered security system that addresses key gaps and anticipates evolving threats.

While a completely failsafe system is improbable for both practical and financial reasons, there is no doubt that the roughly \$24 billion spent on aviation security since 9/11 could be better deployed, providing more meaningful enhancements to aviation security.¹ In particular, invested dollars should favor solutions and systems that are cost-effective, reliable, and ultimately less intrusive to passengers, the vast majority of whom pose no threat to airline security. In some instances, this approach may portend a shift from relying on technology to using more practical, personnel-driven solutions. In other instances, it may require minimizing the role of personnel in favor of technology and automation.

The Four Tiers of Aviation Security

The ideal multi-tiered aviation security system can be visualized as a series of concentric circles, structured in such a way that point failures on an outer layer can



Daryle Lademan is a senior associate at The Avascent Group and leads the firm's commercial aviation-related activities

be addressed by subsequent inner layers of security (see figure 1).

In the four-tiered structure presented here, Tier 1 covers intelligence, perhaps the most critical element of the multi-layered system. The recent plot to bomb transatlantic flights was thwarted due to effectiveness in this outermost layer of security. However, intelligence is a diffuse function that sup-

ports the broad, multifaceted mission of national security and counter-terrorism. It is not a function unique to aviation security and cannot be relied upon to defend against all threats.

The probability of failed intelligence requires that other, robust layers of security be in place. Tier 2 emphasizes airport security and covers passenger screening, carry-on baggage screening, cargo and checked-baggage screening, along with access control by airline and other employees who work in the “sterile” areas of the airport, areas beyond the security screening checkpoint. Tier 2 encapsulates the more traditional concept of aviation security, aimed at keeping dangerous persons and materials off an aircraft.

Tier 3 covers some relatively new concepts in aviation security, all of which emphasize defending the actual aircraft from destruction or misuse in the event that Tier 2 security measures fail. This third layer of security also considers the threat from persons or objects that have not been subject to airport security screening, including threats from Man-

Portable Air-Defense Systems (MANPADS) or laser devices.

A fourth and final layer of security, a “last resort” option, anticipates a scenario in which all three previous layers have failed and a hijacked aircraft threatens ground-based targets. In this 9/11-style situation, combat air patrol aircraft or ground-based air defense assets would be forced to destroy the airliner in order to prevent additional, large-scale casualties.

Of the four layers, airport security (Tier 2) and, increasingly, aircraft defense (Tier 3) represent the most important areas for private-sector involvement.

Airport Security

A profound failure of intelligence and a breakdown of airport security allowed 19 terrorists armed with knives and box-cutters to make their way onto four aircraft on September 11, 2001. Just as 9/11 prompted a major retooling of the US intelligence community, significant attention has been devoted to shoring up Tier 2 of the aviation security system.

Many of these changes were mandated in the Aviation and Transportation Security Act (ATSA), signed into law in November 2001. Among other things, the act created TSA and gave the federal government direct responsibility for airport security, a function previously executed by airlines and private contractors.

Unfortunately, after five years and tens of billions of dollars spent, this crucial layer of security has seen only marginal improvement, as documented by numerous reports and congressional testimonies issued by the General Accountability Office (GAO) and the Inspector General of the Department of Homeland Security (DHS) over the last few years.²

TSA has also been criticized for spending too much money on personnel and not enough on devel-

oping and deploying new technologies to assist in both passenger and baggage screening. In fiscal year 2003, for example, Congress appropriated \$110 million for security technology, but TSA reprogrammed more than half of those funds for screener salaries.

The development of new detection and screening technologies is crucial, as metal detectors and X-ray machines remain the predominant technologies used to screen passengers and carry-on luggage, respectively. Both technologies suffer from key limitations. For example, an entire class of readily available composite weapons, including razor-sharp carbon-fiber knives, is essentially undetectable using conventional screening technologies. Plastic and liquid explosives are equally elusive to metal detectors and X-rays, and may only have a chance of being picked up by secondary screening with a trace detection wand or other machines that screen for chemical signatures. The recent London bombing plot aimed to exploit these vulnerabilities in both passenger and baggage screening. Had intelligence failed to unearth the plot, it is

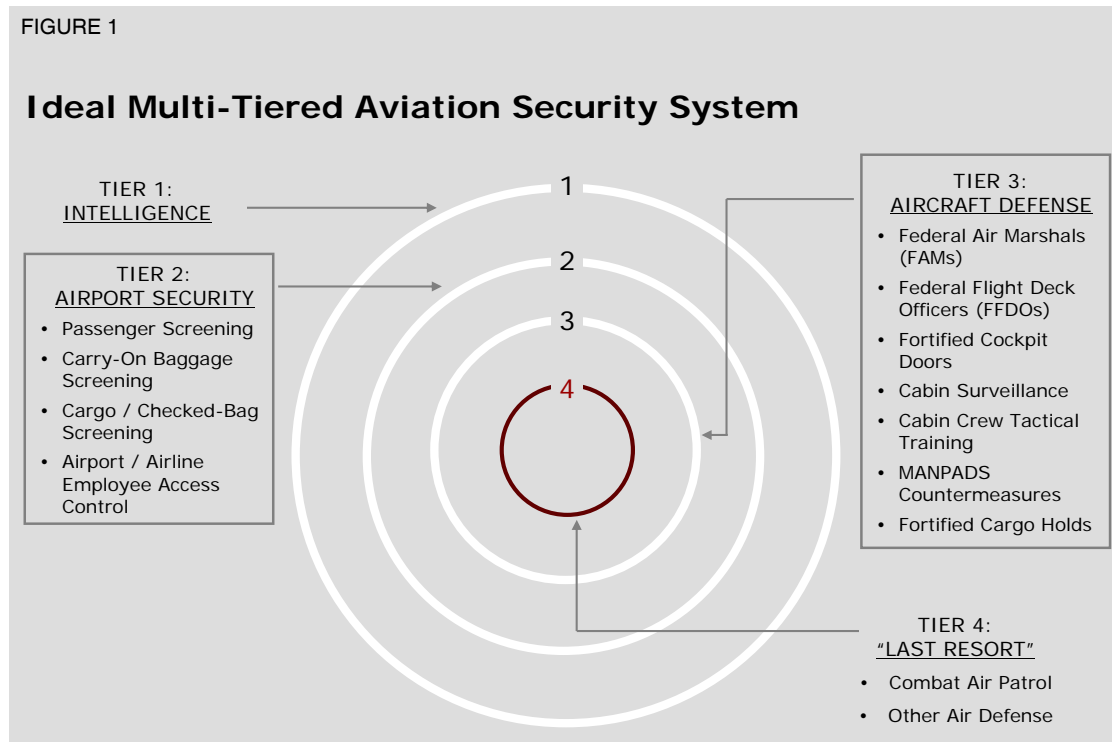
doubtful Tier 2 aviation security in either the United States or Europe would have sufficed to avert a disaster.

The London plot, coupled with the five-year anniversary of 9/11, has helped refocus attention on aviation security. Within days of the London plot being made public, the DHS Science and Technology Directorate turned to industry to ascertain what capabilities currently exist for detecting liquid explosives, such as bottle screening devices capable of detecting and distinguishing explosive and flammable liquids from benign compounds. In the meantime, industry continues to push forward with other technologies aimed at filling a number of other gaps in passenger and baggage screening.

Passenger Screening

Passenger screening has received the lion’s share of US aviation security funding since 9/11. However, the majority of that funding supports the roughly 45,000 TSA screeners that staff the nation’s 445 air-

ports. Indeed, the cost of personnel is substantially more than the cost of screening equipment—about 95 percent of the total transaction.³ For industry, TSA’s high employee costs argue in favor of developing machines that rely less on human interpretation. As noted, the traditional walk-through



metal detectors that remain the primary technology used in the physical screening of passengers are incapable of screening for non-metallic threats. What is more, they suffer from a high false positive rate, which reduces passenger throughput and increases the labor-intensive nature of this method of screening.

TSA has begun to supplement metal detectors with trace detection machines, or “puffers,” at security checkpoints at more than 30 major airports around the country. Passengers identified for additional screening enter the trace portal, where several strong puffs of air are released with the intent of dislodging and detecting tiny traces of explosive material.⁴ While well suited for secondary screening, the trace detectors—manufactured by General Electric and Smiths Detection and costing roughly \$160,000 a piece, according to TSA—are not a substitute for metal detectors, since they are unable to pick up metallic threats. Manufacturers of trace detectors boast their machines offer a low false positive rate, but “nuisance alarms” are still problematic. Nuisance alarms have been known to plague gun owners, soldiers, miners and construction workers, and even gardeners, who may have traces of gun powder, dynamite or fertilizer on their hands, clothing or shoes.

Unlike trace detection technology, which can screen only for explosives, backscatter and millimeter wave technology may be able to replace metal detectors and also protect against a range of explosive and other non-metallic threats like ceramic knives. Backscatter technology involves low-level X-rays capable of penetrating clothing but not skin, affording a whole body image that visualizes both explosives and hidden weapons. Millimeter wave technology involves transmitting ultra-high frequency, low-powered radio-frequency waves to achieve a similar

result.

While effective for detecting a fairly broad range of threats, deployment of whole-body imagers has been controversial due to the explicit images they generate. Privacy concerns notwithstanding, DHS Secretary Michael Chertoff has expressed interest in the devices, testifying before Congress in April 2005 about their promise of recognizing threats routinely missed by metal detectors and traditional X-ray technologies.⁵ TSA has issued contracts to American Science & Engineering, Inc. and Rapiscan Systems, a division of OSI Systems, Inc., to upgrade the software in their respective backscatter systems to address privacy concerns by developing proxy images that mask private parts. TSA also recently decided to broaden competition for whole body imagers, issuing a pre-solicitation notice in July 2006 seeking sources that use non-backscatter technology, including millimeter wave systems offered by SafeView, an L-3 Communications company, and Sago Systems, a division of Trex Enterprises. Pilot studies on these machines, as well as versions from Brijot Imaging Systems and Britain’s ThruVision Ltd., are underway now, with results expected later this year.

Multi-threat portals are destined to replace traditional metal detectors for passenger screening. However, today’s portals are, in truth, only dual-threat devices that screen for weapons and explosives. The “holy grail” for the security industry is the development of a true multi-threat system that can screen for explosives, narcotics, and weapons—even weapons of mass destruction, including chemical, nuclear, and biological threats. Some argue such a system should ultimately integrate biometric technology for identification authentication and be linked to relevant databases to ensure suspected terrorists are flagged.

A truly integrated, multi-threat system would

also be able to scan passengers and carry-on luggage simultaneously, abolishing the need for passengers to take off coats or shoes, or remove their laptops from their carrying cases. GE Security is testing one such advanced security checkpoint concept at San Francisco International Airport dubbed “Checkpoint of the Future.” GE, which has invested in excess of \$100 million since 9/11 in next-generation aviation security technologies and products, continues to test a variety of solutions at this simulated checkpoint with the hope of refining the technology and ultimately offering it to TSA for widespread deployment.

Technology is not the only solution to improving overall passenger screening. TSA is considering more widespread use of behavioral profiling in the wake of the London bombing plot. While not without controversy, behavioral profiling (quite distinct from racial profiling, according to TSA) has reportedly been successful when used on a trial basis at Boston’s Logan International. Profiling techniques, which are modeled on those used by Israel, are designed to zero in on passengers who demonstrate specific and discreet autonomic signs of anxiety, stress, or deceptiveness.

Carry-On Screening

Technology for screening carry-on bags has not changed much since 9/11. Hand luggage screening still relies heavily on human interpretation of X-ray images to identify weapons and explosives. Even the most diligent screeners routinely miss banned items. Hand-held trace detectors are randomly used as a backup to X-ray conveyor systems, but this is a time-consuming process. TSA continues to contemplate the use of computed tomography (CT) technology—the same currently used for checked-baggage screening, and a well-known spin-off from the medical in-

dustry—for the screening of carry-on luggage. While more expensive than current X-ray systems, CT-based systems do not rely on human interpretation (although they require human intervention for threat resolution).

As previously noted, in the wake of the London bombing plot, TSA is seeking vendors that can provide off-the-shelf systems capable of identifying liquid explosive threats. Future carry-on screening systems will likely favor technologies that pair the ability to detect trace and bulk explosives, including liquids, with identification of metallic and non-metallic weapons.

Checked-Baggage Screening

Two months after 9/11, ATSA mandated 100-percent screening of checked baggage at all US commercial airports by the end of 2002 using explosive detection systems (EDS) based on CT technology—a long-overdue decision to close a gaping hole in aviation security that had been exploited by terrorists more than a decade earlier. Indeed, prior to 1988, screening of checked baggage received little attention. In December of that year, Pan Am 103 went down over Lockerbie, Scotland, killing all aboard when 350 grams of Semtex plastic explosives hidden in checked luggage in the cargo hold detonated.

In the wake of Lockerbie, additional security measures went into effect for US carriers at European and Middle Eastern airports, including both X-ray or hand searches of all checked baggage and the matching of passengers to their baggage. These measures were largely symbolic, however, as bag matching did not protect against suicide bombers, and the best available screening technology at the time (thermal neutron analysis, or TNA) would likely have missed the plastic explosives used in the Pan Am 103 inci-

dent.

A 1990 presidential commission on aviation security recommended the Federal Aviation Administration (FAA) aggressively research other detection systems, including CT technology. In December 1994, the FAA awarded its first explosive detection certification to the CTX 5000 manufactured by InVision Systems.

In the years following Pan Am 103, commitment to widespread deployment of CT-based scanners for checked baggage waned at the FAA, although the TWA 800 accident in July 1996—first thought to be the result of a bomb but later determined to be caused by mechanical failure—temporarily reinvigorated interest in the systems. With time, the sense of urgency in the wake of TWA 800 gave way to funding shortfalls.

Consequently, on the morning of September 11, 2001, EDS machines were thinly deployed (only 47 airports had systems in place) and significantly underutilized. Though the FAA had a stated goal of screening 100 percent of all checked luggage for explosives, its timeline for reaching that goal was somewhere between 2009 and 2017. Although the 9/11 terrorists did not exploit the checked baggage screening gap, the momentum generated by the attacks was sufficient for Congress to mandate 100-percent screening of all checked baggage by the end of 2002.

That TSA met this aggressive timeline is one of the few successes in aviation security since 9/11. Unfortunately, EDS deployment has not been without problems. Most of the currently deployed EDS technology was developed in the early to mid-1990s. The machines are both large and heavy, roughly the size of a minivan and weighing up to 17,000 pounds. False positive rates and throughput capabilities also remain problematic. For example, roughly 15-20 per-

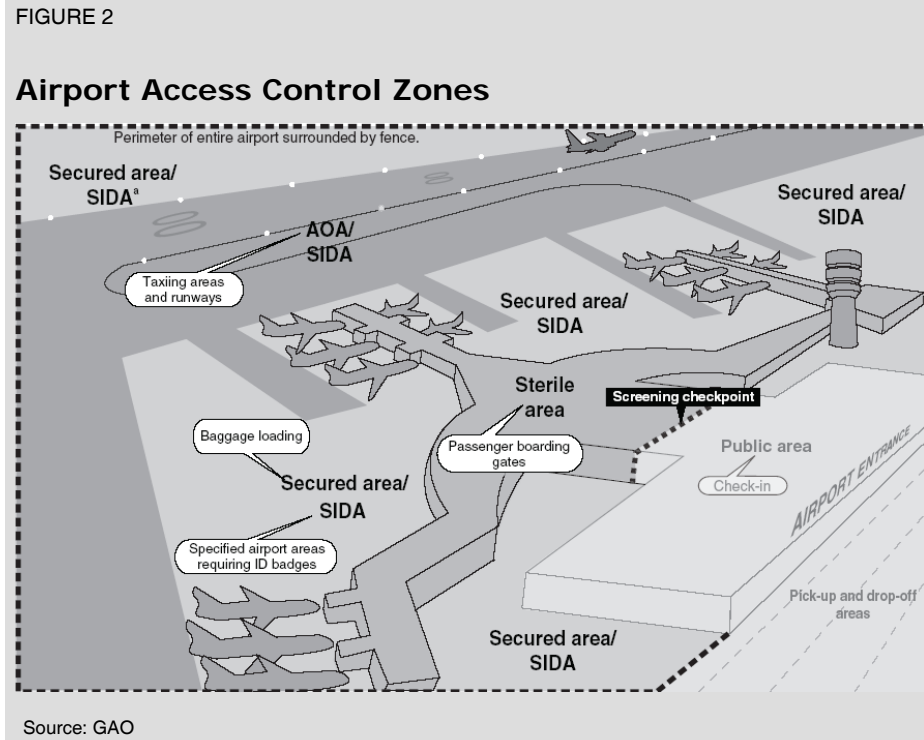
cent of all bags must be opened and manually searched because a CT machine triggers a false alarm, and the maximum number of bags an EDS machine can screen per hour is around 500. These rates assume that the machines are integrated with the airport baggage conveyor system, which is not always the case given the forethought and investment required for in-line baggage screening systems installation.

Industry is developing new EDS equipment to address some of the key deficiencies of existing technology. Rapiscan Systems, for example, is testing a machine that would be capable of scanning in excess of 1,500 bags per hour. Such improvements in throughput, as well as in deployability and accuracy, will continue to be of interest to TSA, though replacing the installed base of current EDS systems will likely be a secondary priority after deploying new passenger and carry-on baggage solutions.

Cargo Screening

Among the largest gaps in the Tier 2 aviation security system is the failure to screen a significant portion of the mail and cargo carried aboard commercial passenger flights. While ATSA required the screening of cargo on passenger jets, TSA has largely relied on a “known shipper” program that allows businesses with a history of working with air carriers or freight forwarders to ship cargo in the belly of passenger jets, leaving verification of the contents of the package to the shipper.

Several members of Congress have expressed frustration over the irony of spending billions of dollars each year to screen 100 percent of checked luggage while commercial cargo goes unscanned. No one has been as vocal as Representative Edward J. Markey (D-MA), a senior Democrat serving on the



House Homeland Security Committee, who has repeatedly called for passage of legislation requiring that all cargo to be screened using the same protocols as for passenger baggage. The adoption of such measures would likely create a major spike in demand for advanced CT-based systems with significantly higher throughput and lower false positive rates.

Access Control

Passengers, luggage, and cargo are not the only threats to consider in the airport security environment. Literally thousands of workers—from aircraft cleaning crews and baggage handlers to in-flight catering services, janitors and airport vendors—have unescorted access to the secure side of the airport and, in some cases, to the actual aircraft (see figure 2). A typical major airport encompasses a perimeter of more than ten miles—larger than the downtown areas of most major cities—and may employ as many

as 20,000 workers. Preventing unauthorized access to sensitive areas of the airport and ensuring the trustworthiness of personnel with unimpeded access is a long-standing problem.

In the wake of 9/11, ATSA called for TSA to establish pilot programs to test and evaluate new technologies, including biometrics and advanced surveillance techniques, to address deficiencies in access control. Unfortunately, progress has been slow. A former FAA “red team” leader, testifying before the 9/11 Commission, stated that his team was successful in breaching the multi-

million-dollar computer-controlled access system up to 90 percent of the time, and a 2004 GAO report found TSA to be deficient in vetting new technologies to improve access control.⁶

Secured-area access at airports is still generally granted by electronic ID cards issued to employees who must pass a basic criminal background check, view a security awareness video, and, in some cases, undergo a fingerprint check. Once vetted, an authorized employee’s ID card opens an electronic lock. A guard may be present to inspect the worker’s ID or to prevent the worker from allowing unauthorized persons to “piggyback” access to the secured area.

However, employees are not physically screened. Moreover, airport workers routinely carry backpacks, purses and other articles into and out of secure areas when they report for work. Their possessions are rarely inspected. TSA argues it is impractical to screen physically the nearly one million airport workers around the country every time they enter the

secure area, not only due to cost and resource diversion, but because many airport workers require banned items such as box cutters and knives to do their jobs at the airport.

Misuse of credentials by authorized employees remains a major concern. DHS has tasked multiple full-time agents at major airports to investigate widespread internal theft and contraband transit among authorized employees. Over the last several years, officials have arrested dozens of baggage handlers, TSA screeners, and other ground employees for theft and drug trafficking—some even operating in organized rings. There have been several incidents of employees taking bribes to allow contraband, including guns, through checkpoints. In every case, the employee had passed the required criminal background check.

More thorough background investigations are an obvious, if impractical, solution to the problem of airport employees misusing credentials. The fingerprint check alone is estimated to cost \$60-80 for each employee, or over \$80 million annually. Given the large number of employees and their relatively high turnover rates, in-depth background checks are simply not feasible. Instead, solutions that rely on more robust technology to monitor airport perimeters, doors, and secure locations may help deter or detect criminal activity by both authorized and unauthorized individuals.

The latest cutting-edge access control and monitoring technology is currently being exploited not in the aviation security community, but in Las Vegas casinos where efforts to identify very subtle suspicious acts and immediately respond to crimes in a crowded, chaotic environment with limited customer intrusion offer promise to the airline industry. GE's VisioWave Intelligent Video Platform, for example,

offers intelligent video analysis software, which acts as a computer sentry programmed to seek out suspicious behavior in images through changes in light, facial recognition, and other attributes. Once the intelligent video system flags a suspicious act, it sends an alarm to a human operator for review. In this way, human resources are freed from the constant monitoring of video surveillance equipment. In one study, human operators missed 95 percent of suspicious activity after only 22 minutes monitoring for it.⁷

The ability of these types of technologies to positively identify an individual or a discreet suspicious act with little intrusion, potentially screening hundreds of passengers or employees per minute, offers great promise in improving access control. Advanced monitoring technologies allow multiple areas to be policed with less manpower, potentially offering the best “bang for the buck” in tracking suspicious behavior going forward.

Aircraft Defense

Largely nonexistent on 9/11, Tier 3 of aviation security—which seeks to address the consequences of a breach of airport security, where terrorists and/or their weapons have made their way onboard commercial aircraft—is destined to become an increasingly important element of the overall system.

By most accounts, the recently foiled London plot was prevented ultimately because an informant led authorities to those planning the attack—the result of good intelligence but also, arguably, a considerable amount of good luck. Good luck also played a key role in foiling the “Bojinka Plot,” a similar plan to blow up commercial airliners over the Pacific Ocean in 1994. In either case, had intelligence failed, it is likely airport security would have failed as well, leaving nothing but the defensive capability aboard

the targeted aircraft to prevent a catastrophe.

Prior to 9/11, commercial aircraft were completely dependent on intelligence and airport security and almost entirely defenseless in the event that both layers of security failed. Cockpit doors were not secure, flight crews were trained to cooperate with hijackers, and only 33 federal air marshals (FAMs) were employed globally. Pilots were prohibited from carrying defensive weapons of any sort and had to pass through the same airport screening as airline passengers.

In the post-9/11 world, aircraft defense has concentrated on fortifying cockpit doors and dramatically expanding the FAM program. While progress has been made in standing up this critical third tier of aviation security, additional cost-effective measures could be taken to make aircraft defense far more robust.

Fortified Cockpit Doors

Fortified, bulletproof cockpit doors have now been installed on all US commercial aircraft, and crews are trained to prohibit passengers from loitering near them in flight. While fortified cockpit doors are helpful, they are not failsafe. Cockpit doors are routinely opened during flight to allow flight crew to receive a meal, use the lavatory, accept relief pilots on international flights, and move around enough to prevent medical stress on long-haul flights. The necessary breaks create opportunities for security breaches and terrorism.

Several successful cockpit breaches have occurred since 9/11, even when a fortified door was locked. In one case, after-hours aircraft cleaners broke a fortified door off its hinges by running a heavy snack cart into it on a bet; in another, a drunk passenger kicked a hole in a cockpit door panel; in yet a third, a pas-

senger simply entered the same electronic access code she had seen the flight attendants use throughout the flight, releasing the lock.⁸

Counterterrorism experts warn no man-made door is impenetrable, especially when some international flights are more than six hours from the nearest point of landing. If passengers were incapacitated by an agent such as pepper spray (which was allegedly used on 9/11), or, worse, a nerve agent like that deployed in the Tokyo subway attacks, terrorists would have ample time to breach the door.

Pilots also remain concerned by the fact that while new cockpit doors are bulletproof, the panels to the sides of the door that form the rear wall of the cockpit are not. They are made of light aluminum, offering only token resistance to a motivated attack from the cabin.

Federal Air Marshal Program

The once-robust Federal Air Marshal Service established in the 1970s to address a rash of conventional hijackings employed just 33 officers on the morning of September 11, 2001, and virtually all were dedicated to covering international flights. The domestic long-haul flights targeted on 9/11 were rarely, if ever, covered by FAMs.

The ASTA called for significantly increasing the FAM program in the wake of 9/11, a move meant to restore confidence in aviation security among the flying public as much as to counter the newly identified threat of unconventional suicide hijackers. While the exact number of air marshals in the system today is classified, numerous public sources indicate the current force provides coverage to roughly five percent of the 28,000 daily commercial flights, at a cost of just under \$700 million a year. The Airline Pilots Security Alliance indicates the cost to protect

nearly all commercial flights in US airspace with a team of marshals would require an annual budget of \$14 billion, and a force of tens of thousands of marshals, roughly the size of the United States Coast Guard.

Clearly, it is economically unfeasible to offer anything close to full coverage of all flights, which is precisely why the value of the FAMs is predicated on their ability to identify and cover high-risk flights, blend in with passengers, and raise questions in the minds of would-be terrorists concerning their presence on any particular flight.

Although TSA deserves credit for rapidly standing up the air marshal force in the wake of 9/11, some of the policies and procedures it has imposed upon officers have been counterproductive at best. For example, until recently, FAMs were required to adhere to a strict dress code of business attire, making it difficult to protect their anonymity on some flights. Some air marshals report the generally mundane but travel-intensive nature of the work also led to an attrition rate as high as 40 percent among officers, particularly those who came from other law enforcement agencies with higher operational tempo. While FAM supervisors deny this, they admit there are marked morale problems in the agency. Thus, TSA faces a continuing challenge of maintaining its FAM workforce.

Federal Flight Deck Officer Program

While federal air marshals and reinforced cockpit doors are valuable additions to the aviation security system, statistics and physics say they may fail to protect an airliner from being commandeered by terrorists. For this reason, many aviation security stakeholders favor a robust armed pilot program as inexpensive insurance against future 9/11-style terrorist

attacks.

Against opposition by TSA, Congress passed the Arming Pilots Against Terrorism Act in 2002, mandating that professional pilots be cross-trained as Federal Flight Deck Officers (FFDOs) on a voluntary basis. The rationale for a volunteer armed pilot program is compelling. Two professional pilots are on every commercial flight and more than 80 percent of them have military or firearms experience. If just more than half of the 85 percent of commercial airline pilots who supported the creation of the FFDO program came forward as volunteers, virtually all commercial flights would be guaranteed to have an armed pilot in the cockpit for a ten-year annualized cost of less than \$30 million.⁹

Unfortunately, only about 10 percent of an estimated 90,000 eligible commercial airline pilots have been trained and deputized as FFDOs—a surprisingly low figure, given the strong support of the program's stated objectives by airline pilots. The low volunteer rates are attributable to a variety of issues, virtually all of which relate to how TSA has chosen to implement the program.

Pilots complain of a lengthy, cumbersome screening and application process that is largely redundant with the screening they undergo to receive and maintain their commercial flying jobs. In the early days of the program, TSA disqualified volunteers with solid credentials, including former agents from the Federal Bureau of Investigation and the Drug Enforcement Administration, police officers, and firearms instructors, leading many potential volunteers to rethink their plans.

Would-be volunteers and deputized FFDOs alike also continue to voice concerns over the non-standard weapons carriage and operational protocols imposed by TSA. FFDOs are the only federal law en-

forcement officers prohibited from carrying firearms on their persons. Instead, they are required to transport their weapon in a heavy steel lockbox and maintain it in the lockbox at all times except when on the flight deck as a working pilot. They must also box and unbox their weapon after every landing. The burdensome, non-standard practice of off-person weapons carriage exposes FFDOs to increased risk of accident, loss, or theft of the weapon. What is more, agreements allowing FFDOs to carry weapons into other countries have not been negotiated, so they cannot protect international flights.

Of all the layers of security, the FFDO program is perhaps the easiest, least expensive, and quickest means of reducing the chance that future airline hijackings will succeed. Commercial pilots indicate many more would volunteer were the program run consistent with standard protocol, similar to the FAM program. Senators Jim Bunning (R-KY) and Barbara Boxer (D-CA) introduced legislation in 2004 aimed at forcing TSA to reform the FFDO program, but the effort stalled in committee and has not yet been reintroduced.

TSA recently established working groups to explore options for changing the program to address pilots' concerns. If changes are made and tens of thousands of additional volunteers come forward, the FFDO program will encompass the largest single group of law enforcement officers in the country, providing opportunities for deployment support from gun and tactical equipment manufacturers and firearms training facilities.

Fortified Cargo Holds

Given the continued porosity in the system for screening passenger luggage and, more significantly, cargo and mail carried on commercial aircraft, some

aviation security stakeholders have argued in favor of taking measures to fortify cargo containers or the cargo hold itself. Though not a new concept—research into hardening passenger aircraft to protect against improvised explosive devices has been a focus since the Pan Am 103 disaster in 1988—interest in the issue has grown recently, particularly in the wake of the London bombing plot.

Advances in detection technology imply structural hardening may need only to protect against smaller blasts—a far more realistic mission. Next-generation commercial aircraft could ostensibly have survivability features built in, just as military aircraft are designed to withstand a certain degree of damage. TSA is researching blast resistant liners for both aircraft cabins and cargo hold areas that could be manufactured into the aircraft at the time of production.

In the meantime, the hardening of aircraft cargo containers may be a practical way to balance structural hardening with significantly improved, but not failsafe, detection technology. At least two firms, including Telair International and Titan, have developed hardened unit load devices (HULDs) that can withstand explosions and contain post-blast fires. TSA is continuing to work with industry to develop lighter, less costly HULD designs that could be embraced by the airlines, as well as solutions to protect narrow-body aircraft that do not use containers for baggage and cargo loading.

MANPADS Countermeasures

There is considerable disagreement within the aviation security stakeholder community as to the true threat posed to commercial aircraft by MANPADS. Those who believe the threat is high point to the fact that at least 42 civilian aircraft have been fired on by

MANPADS around the world since the 1970s. The airline industry tends to downplay the risk, arguing that the cost of protecting the existing commercial aircraft fleet is disproportionately high relative to the risk posed by these systems and relative to other aviation security concerns.

DHS seems to be straddling both perspectives at present. While it has not yet committed substantial financial resources to a counter-MANPADS pro-

In the long term, the aviation stakeholder community must strive for security solutions that are cost-effective, inconspicuous, and non-intrusive to the vast majority of passengers

gram, it has created a special program office to investigate the feasibility of applying existing military protection technology to commercial aircraft. FAA certification, reliability, system

and maintenance costs, and airport operational procedures are among the many issues the DHS Counter-MANPADS System Program Office is exploring.

Working with the Department of Defense and key industry players, DHS is currently exploring a number of existing and emerging counter-MANPADS technologies, including systems offered by Northrop Grumman and Raytheon. The most promising technologies typically utilize an aircraft-mounted laser to detect and confuse an incoming missile.

Other Technologies

The balance of high-tech tools for aircraft defense is not yet beyond the conceptual phase and, in most cases, such instruments would be logistically or financially difficult to implement. These range from

remote control technologies allowing ground controllers to supersede cockpit autopilot control and guide a hijacked aircraft to landing, to cabin surveillance technology providing a visual image of a hijacking, to the deployment of a system that would shock would-be cockpit intruders with miniature lightning bolts.

New security solutions integrated into aircraft designs may also be forthcoming. Last month, Airbus, in partnership with BAE Systems, began testing a suite of technologies in Bristol and Hamburg to guard against hijackings onboard a specially modified aircraft. The technology reportedly allows the aircraft to intercede autonomously and steer away from tall buildings, monitors cabin conversations with cameras and microphones, and uses biometrics to preclude anyone but the pilot from flying an aircraft. Initial system components are planned as options on aircraft orders in 2008, with the full suite deliverable in 2009.

While innovative, the Airbus concept does not cover core improvements like MANPADS defense or hardened cargo compartments, suggesting aircraft manufacturers have yet to consider seriously taking the larger step of fundamental redesign to address the spectrum of new threats.

Conclusions

While markedly better in a few key areas, the US aviation security system remains significantly vulnerable across the spectrum of attack scenarios five years after 9/11. Apart from the general shift in awareness on the part of all members of the aviation security stakeholder community—from intelligence agencies, to front-line employees, to the flying public—the most promising security changes since 9/11 have been the installation of fortified cockpit doors, the

creation of the FFDO program, and the screening of all checked baggage. Unfortunately, the cockpit door is not failsafe, the FFDO program has not been properly administered, and the failure to screen all cargo and mail that accompanies luggage in the belly of passenger aircraft largely negates the accomplishment of 100-percent baggage screening.

As new threats have emerged in the post-9/11 environment, TSA has turned to stop-gap measures that often involve adding extra layers of universal screening on passengers. While committed to fixing the holes in security, airlines correctly point out that burdening passengers cannot be the default solution to every security threat. The surge in interest in private air travel options following the London bombing plot, including charter operators and fractional ownership programs, is evidence that passengers—particularly the lucrative business traveler—will seek alternatives to flying commercially when the system becomes too onerous.

In the long term, the aviation stakeholder community must strive for security solutions that are cost-effective, inconspicuous, and non-intrusive to the vast majority of passengers. This argues in favor of bolstering intelligent airport access control measures, modifying the FFDO program to attract the maximum possible number of volunteers, improving the air marshal program, and using fewer universal screening methods in favor of better, more targeted behavioral profiling.

While TSA and industry alike should continue pursuing new technologies aimed at bolstering airport security—with a particular emphasis on integrated, multi-threat portals for passenger and baggage screening that feature significantly improved passenger throughput and low false positives—the aviation security community and the flying public

must acknowledge the limits of additional airport security investments. No matter how many TSA screeners and next-generation multi-threat portals are deployed, and no matter how many billions of additional dollars are spent, airport security will never be impervious to terrorists.

The persistence of the terrorist threat emphasizes the need for enhanced aircraft defense. In addition to making changes to strengthen both the FAM and FFDO programs, aircraft manufacturers should begin thinking about aircraft security just as they do about aircraft safety—that is, looking for ways to design in features that protect the aircraft from a range of threats. Fortified cargo holds, blast-protected passenger cabin floors, cabin surveillance technology, and MANPADS countermeasures are only a few ideas for improving aircraft security. More imaginative approaches will no doubt emerge as focus continues to shift to Tier 3. Likewise, there may be opportunities to leverage cost effectively some military technologies to further protect commercial aircraft. 🦋

¹ According to TSA spokesman Darrin Kayser, as quoted in Gregory Richards, “Chertoff Commends Local Port for Its Security,” *The Virginian-Pilot*, September 1, 2006.

² GAO, *TSA Oversight of Checked Baggage Screening Could Be Strengthened*, GAO-06-869, July 2006; *Federal Action Needed to Strengthen Domestic Air Cargo Security*, GAO-06-76, October 2005; *Screening Training and Performance Measurement Strengthened, but More Work Remains*, GAO-05-457, May 2005; *Private Screening Contractors Have Little Flexibility to Implement Innovative Approaches*, GAO-04-505T, April 2005; *Systematic Planning Needed to Optimize the Deployment of Checked Bagging Screening Systems*, GAO-05-365, March 2005; *Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls*, GAO-04-728, June 2004; Department of Homeland Security, Office of Inspector General, *Major Management Challenges Facing the Department of Homeland Security (Excerpts from the FY 2005 DHS Performance and Accountability Report)*, OIG-06-14, December 2005.

³ Homeland Security Research Corporation, *2003-2010 - People Screening: Weapon & Explosive Detection*, July 1, 2003.

⁴ The TSA is presently using puffers, in addition to metal detectors, on passengers on flight-screening lists generated by the airlines, passengers exhibiting odd behavior, and random passenger “selectees.”

⁵ DHS Secretary Michael Chertoff, Testimony Before the Homeland Security Subcommittee of the Senate Appropriations Committee, April 20, 2005.

⁶ Bogdan Dzakovic, Statement to the National Commission on Terrorist Attacks Upon the United States, May 22, 2003; GAO, *Aviation Security: Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations*, GAO-04-440T, February 12, 2004.

⁷ The study was apparently conducted by the military, and reported in Australia’s *Security Solutions* magazine, October/November 2002.

⁸ Personal interviews with members of the Airline Pilots Security Alliance.

⁹ Airline Pilots Security Alliance; available at www.secure-skies.org.

The Avascent Group

1717 Pennsylvania Avenue, NW
Suite 1300
Washington, DC 20006-4614

Phone: 202.452.6990

Fax: 202.452.6910

www.avascent.com

For more information on this
publication, please contact:

Christina Balis

cbalis@avascent.com

For more information on The
Avascent Group, please contact:

Jay Korman

jkorman@avascent.com

This is a publication of The
Avascent Group © 2007

The Avascent Group provides management consulting services to global leaders operating at the intersection of technology, business and public policy. Working with senior level management, The Avascent Group assists clients to become more competitive by making better, more informed strategic and tactical decisions on issues of strategy, marketing, operations and innovation in pursuit of their near- and long-term business objectives.

We offer our clients insightful analyses of today's changing business climate and how it affects their strategic outlook and market position. The Avascent Group specializes in:

Strategy Development

Market and Competitive Analysis

Industrial and Government Marketing
& Business Development Support

Merger, Acquisition, and Strategic Alliance Support

By combining our analytic talents with a deep understanding of the industries we serve and the broader political and policy context, we have earned a reputation for offering business leaders actionable recommendations and solutions to the challenges they face. We are set apart by our dedication to quality, timeliness, and pragmatism.

The Avascent Group's clients include leading and emerging companies in defense, aerospace, biotechnology, logistics, homeland security, and information technology.