Chapter Title: Aviation Security After Four Decades, It's Time for a Fundamental Review
Chapter Author(s): Brian Michael Jenkins

Book Title: Aviation Security
Book Subtitle: After Four Decades, It's Time for a Fundamental Review
Book Author(s): Brian Michael Jenkins
Published by: RAND Corporation

Stable URL: https://www.jstor.org/stable/10.7249/j.ctt1q60kx.2

Aviation Security

After Four Decades, It's Time for a Fundamental Review

Brian Michael Jenkins

The recovery earlier this year of a new, improved bomb designed to avoid detection by airport security underscores terrorists' continuing determination to bring down commercial airliners. Like the bomb carried by Umar Abdulmutallab in his unsuccessful attempt to sabotage an airliner in 2009, the new device designed by al Qaeda's bomb-maker was intended to be concealed in the saboteur's underwear. The device was obtained by an intelligence operative who managed to persuade his al Qaeda handlers that he was ready to carry out that suicide mission. While it is necessary to investigate possible ways to counter this latest terrorist innovation, a more fundamental review of how we secure the airplanes that 2 million passengers board every day in the United States is imperative.

Evolving terrorist tactics and technology pose new threats, as growing passenger loads and added security procedures are already straining airport screeners. And terrorists are not the only problem faced by the Transportation Security Administration (TSA). Airline passengers have become increasingly hostile to the very measures deployed to protect them, while TSA is under continuous assault in Congress.

How Did We Get Where We Are?

In terms of the total volume of terrorist violence in the world and the casualties it causes, attacks on aviation do not loom large. Between 9/11 and the end of 2011, there were 75 terrorist attacks on airliners and airports worldwide, resulting in 157 deaths. Compare that with nearly 2,000 terrorist attacks on trains and buses, resulting in approximately 4,000 fatalities during the same period.[1]

In view of this, why is so much of our effort and our precious resources focused on protecting airplanes

Overview

Aviation security is costly, controversial, and contentious; no other security measures directly affect such a large portion of the country's population. Because of the nature of the threat, aviation security is the most intrusive form of security, pushing hard on the frontier of civil liberties. And the threat is real: terrorists remain obsessed with attacking airplanes.

At the same time, passenger loads are increasing, while security budgets are likely to decline. Performance suffers. Meanwhile, public tolerance and cooperation are beginning to fray. But the Transportation Security Administration is often blamed for things beyond its control. And post-catastrophe reviews can push us in the wrong direction, usually resulting in new security measures rather than a reexamination of strategy.

After 40 years of focus on tactical measures, it is time for a sweeping review of aviation security. Instead of forming the usual federal commission to undertake this task, several non-government research institutions could be selected to independently design an optimal aviation security system, beginning not with the four decades of accumulated security measures currently in place but with a clean slate. The competing models would be reviewed and the best ideas or combination of ideas would be put forward. Even if the results turn out to resemble what is already in place, at least the process offers some comfort that we are pretty close to getting it right.

---

[1] These statistics were obtained from the Mineta Transportation Institute's database of attacks on transportation targets.

www.rand.org

and airports? From the earliest days of contemporary international terrorism in the late 1960s, terrorists have made commercial aviation a theater of combat, mainly through hijackings. While governments were trying to build international consensus on outlawing airline hijacking and sabotage as acceptable modes of conflict, they were, at the same time, obliged to protect their own airlines. And they also had to protect themselves.

Aviation security was never viewed solely as a problem of passenger safety. Far more people die in ordinary traffic accidents. Hijackings and incidents of airline sabotage are spectacular events that put passengers' lives in the balance for hours, days, even weeks, or cause airplanes to explode in the air. They have created dangerous political crises. Hijackings have forced governments to negotiate for the lives of hostages, to stand by while hostages were murdered, or to attempt long-shot rescues—all bad options.

Sabotage of aircraft represented a significant escalation in terrorist violence, matching the most massive truck bombings. It led to popular demands for retribution, including sanctions, military retaliation, acts of war—decisions governments did not want to be forced to make.

Imagine the impact on the country if the shoe bomber had brought down a commercial airliner just three months after 9/11 or the consequences if the underwear bomber had succeeded in bringing down a plane in 2009. Nor is such a disaster a far-fetched possibility today.

Al Qaeda leader Anwar al-Awlaki's alleged involvement in terrorist operations, including the 2009 airline sabotage attempt, made him the target of an American drone strike in Yemen in 2011, in which he was killed. The bomb-maker responsible for the device used in the sabotage attempt and the improved model recovered in May 2012 also resides in Yemen, where al Qaeda in the Arabian Peninsula, currently considered al Qaeda's most dangerous branch, has expanded its base. With the United States reportedly already engaged in discreet military efforts in Yemen and calls being made to expand its role, an American airliner plunging to the ground, killing hundreds on board, could easily be the provocation that escalates American intervention.

That is the fundamental difference between the response to the bombing of Pan Am 103 and the likely response today. The United States did not consider itself at war in 1988, even though it had bombed Libya in 1986 in retaliation for Libya's sponsorship of a terrorist bombing in Berlin in which American soldiers were killed. In 1988, a military strike was an unlikely course of action. Today,

although the term is no longer used, America still considers itself "at war" with terrorism, with overt and covert military operations ongoing in a number of countries. Military action in response to terrorism is today a well-carved path.

Aviation security remains one of the most important components of our overall defense against terrorism. It is costly, controversial, and contentious. It dramatically demonstrates the basic tenet of terrorism—that small groups with a limited capacity for power can achieve disproportionate effects by using terrorist tactics. The threat of one terrorist bomber obliges the nation to divert vast sums to airport security. Terrorists need to recruit only one bomber; the United States has to protect 450 commercial airports, with tens of thousands of flights daily. Millions of passengers are inconvenienced, some possibly humiliated.

That raises strategic, even philosophical questions. If security is such a bad exchange, should the United States instead track down and kill terrorist leaders and bomb-makers—itself a controversial mission? Must the United States go further and attempt large-scale military missions to destroy terrorist organizations and stabilize the failing states in which they reside? In the wake of 9/11, the United States invaded Afghanistan. Al Qaeda's bomb-maker currently resides in Yemen. Must American troops now follow?

Aviation security is also important because it is there, as nowhere else, that security measures directly affect such a large portion of the country's population. Moreover, because of the nature of the threat, aviation security is the most intrusive form of security, pushing hard on the frontier of civil liberties. We cannot afford to keep missing opportunities to conduct a thorough, objective, and dispassionate national review of how we—not just TSA, but we as a country—address this critically important activity.

An Adaptive and Imaginative Adversary

For 40 years, terrorists have tried to develop new tactics and devices that would defeat airline security. Sometimes they have succeeded, as they did in 1988, bringing down Pan Am 103 with a small, sophisticated explosive device probably concealed in a tape cassette player; or on 9/11, when they managed to take over four airliners, using knives and pepper spray. Over the long run, however, increasing security has made their operations more difficult. The effectiveness of security is measured not in the number of weapons or explosive devices discovered at airport checkpoints but in the steadily declining number of attempted terrorist hijackings and sabotage attempts.

> **Aviation security remains one of the most important components of our overall defense against terrorism.**

In the 1970s, terrorist hijacking or bombing attempts worldwide were occurring, on average, at the rate of one a month—and people still flew. Since then, the number of attempts has steadily declined.

The decline in the number of terrorist hijacking and bombing attempts worldwide reflects in part the fact that there are fewer terrorist groups focused on aviation. In the 1970s and early 1980s, terrorist hijacking or sabotage attempts were being carried out by a number of Palestinian groups, Shi'ite and Sikh fanatics, Croatian separatists, Ethiopian extremists, Cubans waging war on Castro's Cuba, and members of the Japanese Red Army and Germany's Red Army Faction, as well as Libyan and North Korean agents. Today, the threat comes primarily from al Qaeda, and in Russia, from Chechen bombers, who brought down two Russian airliners in 2004 and bombed a Moscow airport terminal in 2011.

Another reason for the decline in terrorist attempts is better security. While some critics may think airline security is a joke, terrorists take it seriously. They cannot simply march a hundred martyrs toward security checkpoints, hoping some might get through. The risks of betrayal and failure are too great. Instead, they carefully study security measures to identify vulnerabilities they can exploit and ways to allay suspicion. Over the long run, increasing security has made their task more difficult.

Locked, armored cockpit doors and passengers willing to pounce on anyone threatening an airplane have greatly reduced the hijacking threat. Of course, it is necessary to keep guns off airplanes. Terrorist bombs, however, are still getting through security. Terrorists have succeeded in all eight attempts that have been made to get bombs on board commercial aircraft since 9/11, although only two of the devices (both in Russia) worked, and no attempts were made in the United States.

The fact that terrorists are forced to build smaller, easier-to-hide devices with exotic ingredients and no metal parts to make them less detectable represents a kind of progress for security—the new terrorist devices are less reliable and, even if detonated, may not bring down a plane. But the security dilemma remains: Terrorists can make bombs and conceal them in ways that make them undetectable by all but the most intrusive searches.

Today's adversaries remain adaptive and imaginative. After reviewing whether current security measures could have prevented al Qaeda's latest underwear bomb from getting through airport screening undetected, TSA Administrator John Pistole reported that the advanced imaging body scanners deployed at U.S. airports after the first underwear bomber's failed attempt in 2009 have "the best chance" of detecting such bombs, but he added, realistically, "This is not 100 percent guaranteed" (Richardson, 2012).

Al Qaeda's master bomb-maker in Yemen, Ibrahim al-Asiri, who is believed to have designed the explosive device that Umar Abdulmutallab attempted to detonate aboard a Delta Airlines flight from Amsterdam to Detroit in 2009, also designed the bombs concealed in printer cartridges intended to be carried on two Chicago-bound cargo flights in 2010 and the latest device intercepted by intelligence. He once sent his brother on a suicide mission with a bomb reportedly concealed in his buttocks (some reports say in his rectum) to assassinate Saudi Prince bin Nayef. The bomb exploded, but the bomber's own body absorbed much of the blast and Prince bin Nayef survived.

A recent article in one of al Qaeda's online magazines now claims the bomber got through security despite the fact that he was strip-searched and his underwear was inspected, because the bomb was implanted in his abdomen (Al Qaeda in the Arabian Peninsula, 2012). That may be disinformation designed to rattle the rest of the world, although recent intelligence reports indicate that terrorists are exploring the possibility of concealing bombs inside household pets or even surgically implanting them in human suicide bombers.

Whether this is feasible or is simply terrorist propaganda calculated to create terror is hard to say. The security countermeasures such weapons would necessitate beyond body scanners and pat-downs are not pleasant to contemplate. The Israelis, whom Americans credit with taking airline security very seriously, reportedly have concluded that indicators of an underwear bomb cannot be resolved without undressing the passenger, something TSA may not be ready to do, nor would passengers be willing to accept.

Despite their past successes in getting bombs through airport security abroad, jihadists may have given up on getting through security at U.S. airports. Jihadist terrorists in the United States have plotted to attack a broad variety of targets, including subways, synagogues, shopping malls, pipelines, public officials, National Guard armories, army recruiting offices, training centers, courthouses, and commercial buildings. Although one of the uncovered terrorist plots involved attacking the fuel depot at an airport, and homegrown terrorists were ready to take delivery of surface-to-air missiles offered them by FBI undercover agents in sting operations, none of the plots contemplated smuggling weapons or explosives through airport screening. Every recent terrorist

While some critics may think airline security is a joke, terrorists take it seriously.

attempt on U.S. aviation has come from abroad. U.S. law makes TSA responsible for the security of all U.S.-bound flights, enabling it to mandate additional security measures, but primary passenger screening remains in the hands of local authorities.

Richard Reid, the shoe bomber, boarded his flight in Paris. Terrorists planning to bring down multiple planes on transatlantic flights intended to board them in London. Abdulmutallab boarded his flight in Amsterdam. The two bombs intended for U.S. cargo flights in 2010 were smuggled aboard in the Middle East. And the most recently discovered device was to be carried aboard a U.S.-bound flight from Europe. This was also the pattern of terrorist sabotage attempts and all but one terrorist hijacking before 9/11—bombs and weapons were smuggled aboard U.S. carriers abroad, not in the United States.

Terrorist use of shoulder-fired, precision-guided surface-to-air missiles represents another threat to airliners. In 2002, al Qaeda operatives tried to bring down an Israeli jetliner in Kenya—they fired two missiles, and both missed. In 2003, surface-to-air missiles fired by insurgents in Iraq struck two U.S. Air Force transports and a DHL cargo airliner. The severely damaged DHL plane was landed safely owing to the pilots' superb airmanship. Analysts have worried about the terrorist missile threat for decades, especially after the United States lost control over hundreds of Stinger missiles given to Afghans fighting Soviet invaders in the 1980s. Concern has been revived recently by the disappearance of a large portion of Libya's arsenal of missiles. According to official reports, Moammar Gaddafi's regime acquired 20,000 of these weapons from Russia, but only 5,000 of them have thus far been recovered. Jihadist groups in Africa are believed to have acquired at least some of them.

At an international conference on aviation security in 1989, I offered the nightmare scenario that "suicidal terrorists will hijack a commercial airliner and, by killing or replacing the crew, crash into a city or vital facility" (Jenkins, 1989). My observation was not meant to be a prediction, but rather an extrapolation inferred from what I believed terrorists might be thinking.

What are today's nightmare scenarios? Given America's current public and political fragility, a single successful sabotage of a commercial airliner might suffice to provoke paroxysms of panic and rage—at least, al Qaeda's bomb designers think so. In the wake of 9/11, airline travel in the United States plummeted from 734 million passenger boardings in 2000 to 683 million in 2001 to 671 million in 2002 before rising again in 2003—hardly panic,

but a substantial economic blow, especially to the travel industry. Restructuring in the aviation industry and the bankruptcy of several airline companies also contributed to the decline in passenger boardings, but undoubtedly, post-9/11 apprehension was a major factor that affected the entire travel industry (Borenstein and Rose, 2003).

Nevertheless, the public might rediscover some of the stoicism it showed in the 1970s. Meanwhile, terrorists have exhibited loftier ambitions, including the coordinated sabotage of several large airliners at once. This was the scenario in the 1995 Bojinka plot uncovered in the Philippines, which envisioned the near-simultaneous destruction of 12 airliners flying across the Pacific. The plotters in the 2006 Heathrow bomb plot intended to bring down a number of airliners on transatlantic flights. Either plan, had it succeeded, could have caused thousands of casualties.

Analysts, if not terrorists, have thought about the effects of a continuing campaign of airline sabotage instead of a single barrage of airline bombings. Such a campaign poses a much greater operational challenge to the terrorists, but even if only partially successful—a couple of actual explosions on flights, several failed attempts (perhaps diversions), intelligence reports indicating more bombs and bombers still at large (perhaps the product of a terrorist disinformation campaign)—its effects would be nerve-wracking. The increase in risk to individual passengers would be statistically negligible, but it would put enormous strains on airport security.

Bilious Anger

Airport screeners are under increasing stress. Each terrorist innovation has added another security procedure. Because of the shoe bomber, passengers must take off their shoes. In response to the 2006 terrorist plot involving liquid explosives, restrictions were placed on liquids. The underwear bomb led to the deployment of body scanners. Each added procedure complicates the search, slows down the screening process, and further stretches human resources. At the same time, passenger loads are increasing, while security budgets are likely to decline. If the same number of screeners are expected to perform more procedures on more passengers without letting the lines back up at checkpoints, performance can be expected to suffer. Meanwhile, public tolerance and cooperation are beginning to fray.

Americans are a cantankerous bunch. They have come to hold unreasonable expectations that government should provide 100-percent security, and they quail when there is any failure. At the same time, they have little tolerance for inconvenience and react

Each added procedure complicates the search, slows down the screening process, and further stretches human resources. At the same time, passenger loads are increasing, while security budgets are likely to decline.

with outrage to intrusions into their privacy. Successful terrorist attacks underscore the threat and consequent need for stringent security. Fortunately, there have been no successful terrorist attacks against American airliners since 9/11. But the safer people feel, the less their tolerance for what they see as increasingly intrusive security.

Part of the problem derives from lack of understanding. There is a reason behind every security measure. Why, for example, do screeners search children and elderly women? The fact is, the oldest person arrested in the United States for plotting a terrorist attack was 76, while terrorists have employed children as young as six as suicide bombers. The terrorists apprehended by British authorities in 2006 for plotting to blow up airlines flying across the Atlantic contemplated allaying suspicion by boarding the aircraft with their own children, including a nine-month-old baby, who would have been killed in the planned suicide attack. Security procedures must be based on suspicion. If terrorists could be certain that children would not be searched, they would not hesitate to have them carry explosives.

Terrorists watch what security does—and what it cannot do. The public's reaction to the more intrusive pat-downs after the underwear bomber's failed attempt kept this line of attack open. Terrorists could believe that they were on the right path but only needed to make a better underwear bomb.

An element of randomness—changes that the public may find confusing and arbitrary—is essential to prevent security from being too predictable. Moreover, changes in security may be dictated by current intelligence, which TSA cannot always reveal.

The latest security measures have increased public resentment. Public attitudes turned a sharp corner with the deployment of full-body scanners and the introduction of more thorough pat-downs in response to the underwear bomber and subsequent demands for something to be done. Seen as a more intrusive regime, the procedures provoked resistance, which in turn was stoked by the news media and joined by individuals and organizations with other agendas.

Most people in the United States have limited direct contact with government authority. At the local level, think of encounters with parking enforcement officers, traffic cops, and the Department of Motor Vehicles. At the federal level, think of IRS audits or security screening at an airport. None of these institutions are beloved. TSA has the greatest frequency of encounters. About 800 million times a year, Americans pass through a TSA checkpoint. For many, it is a hands-on experience. Everyone has a story to tell about his own (or his aunt's) experience with airport security—usually illustrating a failure or causing outrage. Some of these tales have the quality of urban legends. Some are patently false.

Not surprisingly, many people revile TSA as the embodiment of what they see as an increasingly tyrannical federal government. Every error of judgment, every apocryphal accusation arouses a growing chorus of TSA-haters. The antipathy goes over the top on the public blogs where screeners are routinely described as "Nazis" and "thugs" who push people around, violate their privacy, and touch their "junk." This kind of bilious anger suggests resentment against more than what happens at an airport.

Nevertheless, just as they can demand better security, Americans should be able to indicate their dissatisfaction with existing airline security measures, rejecting those measures they regard as inappropriate as long as they also understand and collectively accept the increased risks this will entail. The problem is that terrorist risks are difficult to quantify, and the opinions of those estimating the risk and those flying the airplanes are likely to be divided. A market approach would be to directly charge passengers for aviation security, but the costs of aviation security cannot be justified by the threat terrorists pose to individual passengers. The risks are minuscule, which is why a strict application of cost-benefit analysis does not work here.

The risks to the nation of a successful terrorist attack go far beyond the safety of individual travelers. Bringing down a passenger airliner could have significant economic and psychological consequences for the nation and could propel the country toward military action. That makes aviation security a matter of national security, not simply passenger safety. There is no easy way to reconcile these perspectives.

Hostility in Congress

There are legitimate questions about TSA's performance. Is it taking the right approach to meet new threats? Does it have a strategy? Can it effectively manage the development and deployment of new technology? Can it operate the information systems necessary to support the no-fly and secondary inspection lists, improved passenger pre-screening, and trusted-traveler programs? Is it overly bureaucratic? Is it top-heavy? Is there too much turnover of its front-line personnel? Has the performance of screening demonstrably improved?

Critics describe TSA as dysfunctional. Some of that perception derives from a dysfunctional political situation. Like the American public, Congress seeks guarantees of absolute security and is ready to point fingers and call for heads to roll when failures occur.

Many people revile TSA as the embodiment of what they see as an increasingly tyrannical federal government.

From the very beginning, some in Congress have been hostile to TSA on ideological grounds, seeing it as another federal bureaucracy employing more government workers. Performance problems are portrayed as proof of TSA's organizational failure. Some call for TSA to be abolished altogether, although what would replace it is unclear.

TSA's congressional critics raise valid issues, but they then pile on tendentious accusations, which prompt questions of motive, undermine credibility, and turn thoughtful inquiry into political theater. Congressional critics have pointed to 25,000 "security breaches" at U.S. airports in the last decade as evidence that TSA is failing to effectively carry out its mission. At first glance, it seems an alarming figure. A "security breach" is when someone enters the secure area without having been fully screened. Usually, the person is quickly located and returned to the checkpoint, but sometimes he or she disappears from sight and the terminal has to be shut down. A ten-year total of 25,000 security breaches at 450 commercial airports in the United States averages out to five or six per airport per year. Looking at it another way, more than 7.6 billion passengers boarded planes at U.S. airports—at 25,000 breaches, screening is operating at 99.999-percent efficiency, which doesn't seem too bad. Actually, we have no way of counting how many prohibited items screeners have missed—stories of the overlooked army knife or the sterling serving fork missed by screeners are retold with great relish. Even if security is 99.99 percent effective in finding potentially dangerous items, with an average of 700 million passenger boardings a year, thousands of objects theoretically could get through.

Terrorists, however, calculate not how many items per million might be successfully smuggled aboard a plane. They have to calculate their odds of being on a no-fly list or a meriting-a-closer-look list; they have to worry that nervous behavior might betray them; they have to assess the odds of their weapon or bomb being discovered by screeners. They get only one try.

And in spite of the fact that some "potentially dangerous items" have eluded detection by airport screening since 9/11, these have not resulted in a single successful attack, suggesting that aviation security might be more effective if it focused on people rather than objects.

TSA is often blamed for things beyond its control—terrorists boarding flights in Europe or smuggling bombs onto flights in the Middle East, for example. It is true that the increasing difficulty of finding small, sophisticated bombs puts greater pressure on intelligence. Congressional critics (and the President) were outraged by the intelligence failure

> **The real problem is not that aviation security is unavoidably reactive; rather, over time, it has produced an accumulation of narrowly focused measures that are both inefficient and impervious to fundamental change.**

that allowed Abdulmutallab to board a U.S.-bound flight, but TSA is a consumer of intelligence, not a producer. And there have been a number of intelligence successes, including the discovery by British authorities of the Heathrow bomb plot; the intelligence warning that bombs had been placed aboard two U.S.-bound cargo flights; and the recent recovery of the latest al Qaeda bomb. To be sure, these successes were owed largely to foreign intelligence services, but the unprecedented cooperation among the world's intelligence services and law enforcement organizations is itself a remarkable success story.

TSA also takes heat for keeping persons on the no-fly list off airplanes, but here again, it does not generate the names on the list. They are produced by the intelligence agencies and coordinated by the Terrorist Screening Center, which operates under the auspices of the FBI. The no-fly list has grown rapidly since 9/11, when it contained only a few hundred names. Today, it contains somewhere between 10,000 and 20,000 names, of whom only a small fraction are U.S. citizens or residents. It has been reported that the no-fly list was significantly expanded after the underwear-bomber incident. With so many names, errors will inevitably occur, causing problems for some innocent people.

We have no way of knowing how many actual terrorists may have been kept off airplanes. Possibly some. At the very least, the existence of a no-fly list obliges terrorist groups to seek new recruits with clean backgrounds for sabotage missions rather than using trusted existing members, and that makes them vulnerable to infiltration by intelligence operatives, as demonstrated in the recent recovery of the al Qaeda explosive device.

Pre-security screening offers promise. Computer-Assisted Passenger Pre-Screening (CAPPS), which was in effect before 9/11, identified nine of the 19 9/11 hijackers as requiring greater scrutiny, although it is not clear that any of them were subjected to secondary searches. The passenger screening protocol used by the airline identified Richard Reid, the shoe bomber, as someone who should not be allowed to board the plane. French authorities interrogated him twice and let him through.

In the past, TSA attempted to introduce an improved version of CAPPS, but because of software problems and resistance from civil-liberties groups, it gave up on the idea. The old CAPPS system used criteria based on analysis of the passenger's individual flight booking, whereas TSA now relies on Secure-Flight to identify elevated-risk passengers (selectees) solely on the basis of national intelligence indicating a suspected connection with terrorists. Passengers'

experience indicates that very few are identified as selectees. Since only selectees receive screening stringent enough to find the kinds of explosive devices terrorists are now using, security depends on remarkably complete and precise intelligence.

TSA is initiating a new trusted-traveler program, called PreCheck, in which frequent travelers can volunteer information about themselves in return for access to expedited security screening. This may provoke less resistance from civil libertarians, but critics say that the security gains are marginal. Does improving efficiency also improve effectiveness, or is there an inherent tension between the two?

Congressional critics say that airline security is reactive. Indeed, most security is reactive. Terrorists and intelligence analysts can imagine more scenarios than security can protect against. It is hard to mobilize finite resources and gain public acceptance of measures to prevent something that has not yet occurred. We knew that terrorists were exploring the use of liquid explosives long before the 2006 plot, but restricting liquids would have been unacceptable before revelation of the plot. Officials have known for a long time that some terrorists probably have missiles, but they have decided not to spend $40 billion over the next ten years to equip the commercial airliner fleet with anti-missile technology (figure from Chow et al., 2005). Once an attack occurs, however, it is almost impossible to resist taking measures to prevent its repetition. The public demands it. Congress must be seen to be doing something.

The real problem is not that aviation security is unavoidably reactive; rather, over time, it has produced an accumulation of narrowly focused measures that are both inefficient and impervious to fundamental change.

While its members complain about TSA's inefficiencies, Congress itself has at times been an obstacle to change. When former TSA head Kip Hawley wanted to dispense with the tedious search for small sharp objects once cockpit doors were locked and armored, Congress said no. Simply put, no politician wants to publicly agree to lifting any security measure. (Hawley's successor, John Pistole, later quietly ordered the change.) As long as the same procedures remain in place, the illusion of absolute prevention survives, and failures can be attributed to poor performance. Change brings ownership. It entails risk. It is easier to blame than it is to accept the burden of responsibility if something goes wrong.

Time for a Thorough Review

It is now more than a decade since TSA was established and eight years since the 9/11 Commission published its report on aviation security. A national review is in order and should not be put off until another catastrophe compels it to be done.

In fact, post-catastrophe reviews tend to push us in the wrong direction. Hastily done, narrowly focused on the latest failure, they often end up merely adding new security measures rather than reexamining strategy.

Procedural tweaks and technological advances (plus a lot of luck) may keep airline security one step ahead of aviation-obsessed terrorists while gradually improving efficiency. But more-radical approaches may be needed. They should at least be explored without waiting for a terrorist-created tragedy to drive a new inquiry.

Kip Hawley offers a number of suggestions in his new book *Permanent Emergency*. He argues that TSA needs to break out of its strict rule-based security regime to develop more-flexible approaches, revamping what screeners look for and reducing time wasted looking for objects that are no longer capable of bringing down a flight. He writes that TSA already has the machines to detect liquid explosives and therefore can do away with the restrictions on liquids, although software problems remain. Actually, while the technology can detect the presence of liquids and the composition of some, the false-alarm rates are extremely high, and resolving them is difficult. Restrictions on liquids may be reduced, but not without risks.

Others, including me, have proposed expending less effort looking for objects and focusing more on the passengers themselves, not all of whom pose the same risk. Based on personal information they volunteer, trusted travelers, whose identities would be confirmed at each flight, could go through a "pre-9/11 lite" inspection, while more-effective use of prior flight histories and other information already readily available to airlines might indicate the need for greater scrutiny for others. This would allow finite resources to be reallocated according to risk. TSA's PreCheck program is a step in this direction.

PreCheck depends on the reliability of the prescreening system and confirmation of passengers' identity. Stringent requirements for enrolling passengers in PreCheck—for example, limiting it to frequent flyers with long flying histories that can be confirmed—would reduce the risks of infiltration by terrorists. These passengers account for a disproportionate number of boardings. Enrolling them in PreCheck would enable TSA to shift resources to assist ordinary occasional travelers and, more importantly, expand the organization's capacity to focus on those posing greater risk (Poole, 2012). Mathematical mod-

A national review is in order and should not be put off until another catastrophe compels it to be done.

eling, supplemented by continuous realistic testing (not an easy task), could help TSA arrive at the right proportion of passengers and array of security measures for each category. The system, however, would maintain some element of randomness to reduce predictability.

Unfortunately, Americans prefer their security to be egalitarian—the same treatment for all. There already are complaints about the special lanes that allow frequent flyers, first-class, and business-class passengers to bypass the long queues waiting to pass through TSA screening. Claiming that this is unfair, Senator Ben Nelson has introduced legislation that would ban the "elite" flyer lanes. His Air Passenger Fairness Act does not affect trusted-traveler programs, but as PreCheck is introduced, TSA can expect travelers to complain about privilege or profiling, while terrorists might try to infiltrate the trusted-travelers group with "clean skins."

Senator Rand Paul suggests an extreme solution—scrap TSA altogether, presumably replacing it with private security personnel. It is hard to see how this will improve security. Private contractors currently do a good job at some airports, but allowing each airline and each airport to do its own thing risks a return to the bad old days before 9/11, when airport screening was determined more by profit motives than by national security, training was poor or lacking, and turnover rates among low-paid screeners at times reached 400 percent a year. And whether being "pawed" by private contract guards instead of federal employees strikes a blow for liberty seems at best arguable.

Agents of Change

There may be a better way to improve aviation security, but in order to know, we have to break out of the bureaucratic and ideological boxes that currently drive discussion. TSA itself conducts reviews of its own performance and supports research aimed at improving its own effectiveness and efficiency—PreCheck is one result. But TSA is preoccupied with current operations and equipment installation. It has little spare time to conduct the needed review or the perceived independence to support its conclusions. Congress clearly has the authority to conduct a thorough review of requirements and the means of meeting them, but the oversight committees have limited research capabilities and come up short on objectivity. One way of getting a credible, clean-slate review would be to create an independent commission to take a hard look at what must be done and how best to do it.

Having served as a member of one aviation security commission and having advised several others, I am acutely aware of the advantages and limitations of independent commissions. Having a finite lifespan, they can shake things up (much as the 9/11 Commission did), give credibility to novel ideas, and provide cover to nervous politicians. Commissions can also help educate the public. But they have limited clout, and although we would hope that they comprise intelligent people who are knowledgeable about aviation and savvy about politics, commissions are not able to perform the detailed conceptual analysis required to evaluate the current security architecture and design alternatives.

An approach employed at times by the Pentagon to examine complicated and contentious issues might provide an answer. Two or three non-government research institutions could be selected to independently design an optimal aviation security system, beginning not with the four decades of accumulated security measures currently in place but with a clean slate. When complete, the competing models would be reviewed—an appropriate role for an independent commission—and the best idea or combination of ideas would be put forward. Even if the resulting alternatives turn out to resemble what is already in place, the investigative process would at least offer some comfort that we are pretty close to getting it right.

The most difficult part of this approach is determining how to select the participating institutions. The big consulting firms that currently dominate government contracting would rush in. Each one has its own supporters in Congress, and some have patent ideological leanings. In today's partisan environment, the selection process would be likely to get very political. The Department of Homeland Security might seek political cover by cobbling together multi-institute consortiums, but these tend to be unwieldy.

Yet another approach would be to conduct an open challenge, as the Defense Department also has done in the past, with multi-million-dollar cash prizes divided among the winners. An independent commission could act as the judge. This process could be repeated every five years or so to ensure the continuing injection of new ideas and novel approaches.

What airline passengers seem to want and politicians appear to demand is fast, friendly, and flawless passenger screening that is 100-percent effective against the latest terrorist devices and concealment methods, while anticipating and thwarting new threats. The system must effectively screen every passenger—and every piece of checked and hand-carried luggage—without error and without irksome body

> Two or three non-government research institutions could be selected to independently design an optimal aviation security system, beginning not with the four decades of accumulated security measures currently in place but with a clean slate.

scanners and pat-downs. Performance must be perfect. And screeners must do this nearly 800 million times a year. At the same time, passenger screening should be discerning but democratic. Intelligence must keep terrorist suspects off flights but without errors that affect innocent travelers, and it must accomplish this without government-held databases, the existence of which is seen by some to threaten civil liberties. And all of this is to be achieved with significantly fewer government personnel, including fewer supervisors at airports where private security has taken over passenger screening but for which TSA remains responsible for failures. Cost reductions are mandatory. Failure in any dimension is evidence of government incompetence.

The problem is that satisfying these contradictory demands and wishes is utterly unrealistic.

As is often the case, terrorists are only one part of the problem. Contradictory public attitudes, bureaucratic inertia, competing agendas that trump national interest, ideologically driven analysis, uncompromising partisanship, and political timidity pose equal challenges. These impediments are momentarily swept aside only by catastrophe, allowing us—briefly—to focus on villains with bombs. We should not have to wait for that.

Unfortunately, aviation security will continue to be a national necessity. It merits a serious national review.

References

Al Qaeda in the Arabian Peninsula, "The Secrets of the Innovative Bomb," Sada al-Malahim (Echo of Battle), No. 12, February 15, 2012.

Borenstein, Severin, and Nancy L. Rose, "Do Airline Bankruptcies Reduce Air Service?" Cambridge, Mass.: The National Bureau of Economic Research, NBER Working Paper No. w9636, April 2003. As of July 30, 2012:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=398540

Chow, James S., James Chiesa, Paul Dreyer, Mel Eisman, Theodore W. Karasik, Joel Kvitky, Sherrill Lingel, David Ochmanek, and Chad Shirley, *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat*, Santa Monica, Calif.: RAND Corporation, OP-106-RC, 2005. As of August 9, 2012:
http://www.rand.org/pubs/occasional_papers/OP106.html

Hawley, Kip, and Nathan Means, *Permanent Emergency: Inside the TSA and the Fight for the Future of American Security*, New York: Palgrave Macmillan, 2012.

Jenkins, Brian Michael, *The Terrorist Threat to Commercial Aviation*, Santa Monica, Calif.: RAND Corporation, P-7540, 1989. As of July 23, 2012:
http://www.rand.org/pubs/papers/P7540.html

Poole, Robert W., Jr., "Should 75% of Flyers Be in PreCheck?" Airport Policy News, No. 80, June 2012.

Richardson, Whit, "Pistole: TSA Might Not Have Detected New Underwear Bomb," Security Director News, May 22, 2012. As of July 23, 2012:
http://www.securitydirectornews.com/public-matters/pistole-tsa-might-not-have-detected-new-underwear-bomb

About this Paper

This paper results from the RAND Corporation's Investment in People and Ideas program. Support for this program is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research. This research was conducted in the RAND Homeland Security and Defense Center, which conducts analysis to prepare and protect communities and critical infrastructure from natural disasters and terrorism. Center projects examine a wide range of risk management problems, including coastal and border security, emergency preparedness and response, defense support to civil authorities, transportation security, domestic intelligence, technology acquisition, and related topics. Center clients include the Department of Homeland Security, the Department of Defense, the Department of Justice, and other organizations charged with security and disaster preparedness, response, and recovery. The Homeland Security and Defense Center is a joint center of the RAND National Security Research Division and RAND Infrastructure, Safety, and Environment.

Information about the Homeland Security and Defense Center is available online (http://www.rand.org/multi/homeland-security-and-defense/). Inquiries about homeland security research projects should be sent to:

Andrew Morral, Director
Homeland Security and Defense Center
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5119
Andrew_Morral@rand.org

RAND

HEADQUARTERS CAMPUS
1776 MAIN STREET, P.O. BOX 2138
SANTA MONICA, CA 90407-2138

OFFICES
SANTA MONICA, CA
WASHINGTON, DC
PITTSBURGH, PA
NEW ORLEANS, LA/JACKSON, MS
BOSTON, MA

DOHA, QA
ABU DHABI, AE

CAMBRIDGE, UK
BRUSSELS, BE

REPRESENTATIVE OFFICE
MEXICO CITY, MX

www.rand.org

RAND publications are available at www.rand.org

OP-390-RC (2012)