



# TRANSPORT FOR A GLOBAL ECONOMY

*Challenges and Opportunities  
in the Downturn*

FORUM 2009 • 26-29 May • Leipzig

## WORKSHOP 4

*Ensuring a Secure Global  
Transport System*

*Towards Risk-Based Aviation Security Policy*

*Robert W. Poole Jr.*

*Reason Foundation*

## TOWARD RISK-BASED AVIATION SECURITY POLICY

Robert W. POOLE, Jr.  
Reason Foundation

### 1. Introduction

The well-coordinated terrorist attacks on Sept. 11, 2001 presented the world with a new aviation security threat: the capture of aircraft in flight to be used as human-guided missiles. The two previous threats—hijacking an aircraft for ransom and putting a bomb aboard an aircraft—had led to varying degrees of screening of baggage and passengers in developed countries, plus some use of on-board security personnel on selected flights in some countries.

In the wake of 9/11, governments in the United States, Canada, and Europe (at both national and EU levels) implemented a number of additional aviation security measures, among them strengthened (and locked) cockpit doors, 100% screening of checked baggage, more thorough screening of passengers and their carry-on baggage, increased use of on-board security officers, increased attention to air cargo, and greater attention to airport access control and perimeter control.

Although the rhetoric of risk-assessment and claims that security policies are risk-based are often heard, much of the actual policy change appears to have been driven by political imperatives to reassure frightened populations that air travel is still safe. In the United States, for example, although the initial legislation, enacted within two months of the 9/11 attack, was called the Aviation and Transportation Security Act (ATSA), and it created the Transportation Security Administration nominally to protect all of transportation, the vast majority of the TSA's budget has gone for legislatively mandated aviation security (with by far the largest share concentrated on passenger and baggage screening). No risk assessment preceded this statute's enactment, nor has this initial allocation of resources been changed significantly by the subsequent large-scale reorganization that created the multi-faceted Department of Homeland Security (DHS), into which the TSA and many other agencies were transferred.

Economics reminds us that resources are always limited, and that resources allocated to X are not available for Y. The challenge in dealing with terrorist threats—whether to a nation, a sector such as transportation, or a sub-sector such as aviation—is always one of deciding where to invest scarce resources to maximum benefit. This inevitably requires difficult choices to be made, and the premise of this paper is that risk assessment provides an essential framework for making such choices and should be applied more consistently to aviation security.

This paper is organized as follows. First, to provide context, it discusses macro-level considerations in countering terrorism. Next, it provides a provocative example of applying risk analysis to assess the cost-effectiveness of several post-9/11 aviation security measures. With that as background, the paper then compares and contrasts the post-9/11 aviation security

policies of the USA, Canada, and the EU countries, with costs and risks as a principal focus. Finally, it provides suggestions for making aviation security policy more consistently risk-based.

## **2. Context: The Problem of Defending Against Terrorism**

### **2.1. The Basic Problem**

The sector-specific approach that has been applied to aviation is an example of target-hardening. The problem with this approach is that we live and function in a target-rich world, and this is inherent in the nature of developed economies. Because resources are limited, all conceivable targets cannot be hardened. But terrorists can readily shift from hardened to non-hardened targets. Target-hardening is an example of what analysts have called “asymmetries” between terrorists and their target governments. As Sandler, Arce, and Enders (1) point out, there are a number of such asymmetries. Terrorists operating in loosely connected networks appear to cooperate more readily than governments. Terrorists also seem to operate with longer time horizons than the political process. Because terrorists hide among the general population, they present a target-poor environment to governments, compared with the terrorists’ target-rich environment. And the cost to terrorists of wreaking destruction and creating fear are modest, in comparison to the costs of governmental attempts to defend (everything) against terrorist attack.

### **2.2. Macro-Policy Alternatives to Counter Terrorism**

In 2008, the Copenhagen Consensus project commissioned a challenge paper on terrorism. In the paper, Todd Sandler and Daniel Arce of the University of Texas at Dallas and Walter Enders of the University of Alabama focus on transnational terrorism as a problem fundamentally different from other global crises.(1) Their basic message is that “there is no solution to transnational terrorism because it is a cost-effective tactic of the weak against a more formidable opponent.” Thus, they conclude, “terrorism can be put into remission but it cannot be eliminated.”

To illustrate the difficulties involved in cost-effectively countering terrorism, they outline five conceptual global strategies and estimate the benefit/cost ratio of each. Before doing so, they discuss why doing benefit/cost (B/C) analysis is so difficult in the case of counter-terrorism efforts. First, there is no permanent solution, so benefits from a counter-terrorist strategy are likely to last (they guess) only two to five years. Second, there is no reliable way to know what level of terrorist activity there would have been in the absence of the strategy. Third, the cost of such strategies is difficult to ascertain, since much information is classified.

The benefits of preventing terrorist actions consist primarily of the value of lives saved and injuries prevented, along with avoided reductions in gross domestic product (GDP). Because (at least thus far) terrorist incidents are infrequent and of relatively small impact, it turns out that homeland security expenditure, as a fraction of GDP, dwarfs the other variables in the B/C calculations, over a wide range of assumed values for the parameters.

The first of the five strategies, called “business as usual” is basically the current policies adopted by the developed world. The authors’ B/C ratio for this is .095 — *i.e.* benefits of less than 10 cents per dollar spent. A policy of increased proactive steps (taking the battle to terrorist havens) would have much higher costs and somewhat larger benefits, resulting in a B/C ratio of .077. Augmented defensive measures (more-aggressive target-hardening globally) has an estimated B/C ratio of 0.28—higher than the first two, but still far less than 1.0. A more sensitive foreign policy for western governments (instead of current measures), although the most difficult to evaluate, was judged to possibly have a B/C ratio exceeding 1.0. The only one of the five

strategies estimated as having benefits considerably in excess of costs was “greater international cooperation” (such as freezing assets and cutting off terrorist resources, along with increased police cooperation among countries), as opposed to the current combination of target-hardening and striking at terrorist havens. The B/C ratio for this approach was estimated at 5.3 — but it was also considered the most difficult strategy to implement.

Overall, Sandler, Arce, and Enders conclude that “security-based solutions display adverse B/C[ratios]” and that it would be better to shift to low-cost strategies based on greater international cooperation and changed foreign policy.

A very important caveat to this assessment, as discussed by Michael Intriligator in a companion paper, is that the authors do not factor in possible terrorist use of biological, chemical, radiological, or nuclear materials, since their estimates of lives lost, injuries sustained, and reductions in GDP are based on historical trans-national terrorist activity, none of which has involved these more serious threats(2). Had data been available to quantify such costs, the B/C ratios for several of the strategies would have been “much larger,” as Sandler, et al. concede. However, for our purposes, aviation does not appear to be a current target for such weapons.

### **2.3. The Dynamics of Counter-Terrorism**

The Maginot Line is a classic case of a static defense that failed. Target-hardening approaches risk making the same mistake, via the equivalent of building walls to prevent the previous kind of attack. As Intriligator points out, “[t]he most effective way to defeat transnational terrorism is not to try to protect vulnerable assets. That is the principal approach of the U.S. DHS, which concentrates on protecting airplanes and airports, ignoring other potential targets. Such an approach is like generals fighting the last war, in this case the 9/11 attacks.”(2)

Terrorists adapt to the creation of defenses. In *Breaching the Fortress Wall*, a nine-member RAND Corporation team sought to understand terrorist groups’ efforts to overcome defensive technologies.(3) Their 139-page assessment reviews four such groups, in Palestine, Southeast Asia, Sri Lanka, and Northern Ireland. Across the board, they found that terrorist groups responded to the use of defensive technologies by:

- Altering operational practices;
- Making technological changes or substitutions;
- Avoiding the defensive technology; or,
- Attacking the defensive technology.

In the case of technologies used to harden targets, terrorists’ most effective approach was “operational changes that allowed penetration of target defenses.” In an example with direct relevance to airport security, when security forces used terrorist profiling, “every group sought and used terrorists with characteristics that were inconsistent with the profile and could therefore avoid detection.” Most groups also shifted to different targets or different tactics altogether.

The RAND researchers concluded that “the historical record of terrorists’ efforts to counter defensive technologies is not encouraging.” They found that “for most technologies, the groups will adapt to circumvent them,” and the security forces will have to respond. Thus, technology cannot be “the” solution to terrorism. They recommend that new defensive technology systems

“must be designed with terrorist counter-technology behaviors and past successes in mind.” In particular, they suggest designing flexibility into defensive technologies, and frequently testing them against “red teams” trying to get past them.

### 3. An Example of Cost-Effectiveness Analysis in Aviation Security

The previous section discussed the difficulty of conducting overall benefit/cost analysis of anti-terrorist strategies. But there are other approaches to assessing the value of security measures. A recent paper from the University of Newcastle analyzes several components of the TSA’s aviation security program in the United States.<sup>(4)</sup> In this paper, there is no attempt to make absolute B/C ratio calculations, as in the Copenhagen Consensus paper discussed previously. Instead, Stewart and Mueller assess the *relative* cost-effectiveness of several measures, using as a metric the cost per life saved. This approach has been used extensively in studies of the relative cost-effectiveness of safety-related regulatory measures. A table in their report draws on regulatory analyses of measures enforced by six U.S. safety regulatory agencies (including the Federal Aviation Administration). The annual cost per life saved (in 1995 dollars) ranges from a low of \$0.1 million for FAA’s aircraft cabin fire protection standard to a high of \$6.78 trillion for EPA’s hazardous waste listing for wood-preserving chemicals. In reviewing possible safety regulations, the U.S. Department of Transportation uses a figure of \$3 million per life saved as a ceiling for acceptable regulatory costs.

Stewart and Mueller present a list of 20 TSA aviation security efforts, 14 of which apply in the airport environment (mostly concerning passenger and baggage screening, but also access control and other issues) and six that deal with in-flight security. They group the six in-flight measures into three: crew and passenger resistance, hardened cockpit doors, and Federal Air Marshals (FAMs). Consistent with much informal thinking within aviation security circles, they assume that in-flight efforts have made a considerable difference in reducing the probability that a plane will be hijacked and turned into a weapon. Hence, their starting assumption is that the in-flight measures account for 50% of the reduced risk of a 9/11 aircraft takeover, with the 14 pre-board security measures adding up to the other 50%. And as a starting assumption, they assume that the three in-flight measures are each equally effective—i.e., each accounts for 16.67% of the total reduced risk. They then factor in a generous 10% probability that Federal Air Marshals will be present on any particular plane. That reduces the risk reduction due to FAMs alone to 1.67%.

How likely would another 9/11 attack be were these 20 security measures not in place? Stewart and Mueller postulate that in the absence of those measures, there would be a 9/11 repeat (with approximately 3 000 deaths) once every 10 years. Hence, they assume this set of measures prevents 300 deaths per year in the United States.

From there on, it is a simple matter of doing the math, using the best available information on the annual costs of each measure. The results they present for the annual cost per life saved are as follows:

- Hardened cockpit doors: \$800 000
- Federal Air Marshals: \$180 000 000

Because several of their assumptions are somewhat arbitrary, they follow this with a sensitivity analysis that varies the probability of success of each measure, showing that the general results in terms of relative cost-effectiveness hold true over a wide range of assumed probabilities. They conclude that “even an order of magnitude reduction in the effectiveness of

hardened cockpit doors (resulting in a cost per life saved of \$8 million) would not change the conclusion” that the cockpit doors are a far more cost-effective measure than air marshals.

That is as far as Stewart and Mueller take their analysis, but the same kind of calculation can be applied to the set of pre-board security measures. Using their assumption that 50% of the reduced risk of a 9/11 attack is due to the pre-board measures, we use their basic equation:

$$C_{ls} = C_r / (\text{annual lives saved due to security measure})$$

where  $C_{ls}$  is the annual cost per life saved and  $C_r$  is the annual cost of regulation  $r$ .

According to Oster and Strong (5), about \$4.7 billion of TSA’s annual \$6.7 billion budget is spent on airport-related security (excluding cargo security). Using that figure for  $C_r$  yields an estimated cost of \$31.3 million per life saved thanks to pre-board airport security measures—more than 10 times the US DOT standard, and 39 times as great as hardened cockpit doors.

While this approach obviously has its limitations, depending critically on assumptions about annual lives saved, thanks to reasonably good cost data and sensitivity analysis it does make it possible to estimate the *relative* cost-effectiveness of various aviation security measures over a range of possible assumptions about security event frequencies.

A summary of the OECD/ITF Round Table on Security, Risk Perception, and Cost-Benefit Analysis drew an important distinction between safety analysis and security analysis. The former is concerned with risk, while the latter is concerned with uncertainty.(6) In analyzing safety risks, the events involved are unintentional and there is generally a reasonably large data set from which to estimate probabilities. By contrast, security events are intentional, and are far fewer in number, such that “no credible objective probability can be assigned to their occurrence.” After reviewing a number of possible sources of probability estimates, the summary concludes that while “no objective probabilities can be determined for the occurrence of attacks,” subjective probabilities “can be gleaned from intelligence, the insurance industry, and prediction markets” even though this is not currently being done systematically in security policy-making.

## **4. US, Canadian, and European Approaches to Aviation Security**

### **4.1. Introduction**

Aircraft hijackings in the late 1960s and early 1970s led the member states of the International Civil Aviation Organization (ICAO) to adopt Annex 17 to the Convention on International Civil Aviation, commonly known as the Chicago Convention. Annex 17 requires each member state to designate a single agency to develop national policy on aviation security—specifically, objectives, policies, and programs to prevent unlawful acts that threaten the safety of civil aviation. Annex 17 has been amended several times in subsequent decades, in response to the emergence of new threats and trends.

This section provides an overview of the development of aviation security policies since the adoption of Annex 17 in Europe, Canada, and the United States.

### **4.2. Europe**

In Europe, hijacking was primarily a terrorist activity from the start, in contrast to the lone-hijacker-for ransom pattern in the United States in the 1960s and 1970s. Groups such as the

Popular Front for the Liberation of Palestine and the Red Army Faction presented a larger and more-organized threat than lone hijackers interested in money or momentary fame.

Prior to 9/11, aviation security was handled on a national basis in Europe. In Germany, as described by Hainmuller and Lemnitzer (7), the federal government urged its states (Lander) to implement airport security measures in 1970, and the larger airports did so. In 1980, after additional hijackings led to years of debate, a national civil aviation act was enacted, mandating that airports screen baggage and passengers, funded out of state budgets. Screeners were state employees, mostly drawn from the ranks of Federal Border Guards. In 1990, however, state budget pressures led to federal enactment of an aviation security fee, added to airline tickets, to recover part of the cost of staff and equipment for passenger and baggage screening. Continued cost pressures led to federal permission for screening to be outsourced to private security companies, with the first such contracts beginning in 1995. By 2000, "most of the German airports employ private screening firms or conduct screening themselves [e.g., Frankfurt]," according to Hainmuller and Lemnitzer's 2003 paper.

The pattern has been similar in other European countries, with airport security measures (mostly passenger and baggage screening) introduced in the 1970s and 1980s in response to hijackings. As in Germany, most such screening began with screeners as state employees. But the combination of airport privatization (beginning with the initial public offering of all shares in the British Airport Authority in 1987) and cost pressures led to the outsourcing of screening functions at most major airports by 2000. According to data compiled in 2001 by the (U.S.) Aviation Security Association and reported in Poole (8), as of that year passenger and baggage screening was handled by either private security firms or a privatized airport company at 22 of the largest 25 European airports (ranked by international passengers). The exceptions were in Portugal, Spain, and Switzerland.

The destruction of Pam Am Flight 103 over Lockerbie, Scotland in December 1988, via a bomb in an unsuspecting passenger's checked bag, led to further changes in European aviation security. Positive matching of passengers and bags became mandatory in most European countries by 1989, and Germany had implemented 100% checked baggage screening at all 37 major airports by the end of 2002.(7) The United Kingdom and a number of other countries did likewise.

Payment of aviation security costs in Europe follows no clear pattern. In some countries, such security is considered a national defense expense and is funded primarily by the national government out of general tax revenues. In the U.K., by contrast, the privatized and commercialized airports are responsible for airport security costs, and recover those costs in their fees and charges to airlines. In Germany, as noted previously, a security tax on airline tickets covers a portion of security costs, with the balance shared between airports and the federal government.

No EU-wide aviation security policy existed until 2002, when the European Parliament and Council agreed upon Regulation No 2320/2002 establishing common rules for civil aviation security. Those regulations were revised substantially in 2008, with Regulation No 300/2008 repealing and replacing the 2002 regulation. Consistent with ICAO Annex 17, each member state of the EU must have a national civil aviation security program, with a single agency in charge. Member states may adopt more stringent measures (on the basis of risk assessment), but the objective of No 300/2008 is to provide a "common interpretation of Annex 17" within Europe.(9)

### 4.3. Canada

As in Europe, aviation security precautions began as a response to hijackings in the 1970s. The government designated Transport Canada as its aviation security agency under ICAO Annex 17, and developed an airport security policy and program based on ICAO recommended specifications and practices for international airports.<sup>(10)</sup> Hijacking, taking on board offensive weapons and/or explosives, and endangering the safety of an aircraft in flight were made federal criminal offenses in 1972, and security-related measures were added to the Aeronautics Act in 1973. Those changes made airlines responsible for aircraft security and Transport Canada for overall security standards for airlines and major airports (of which Transport Canada was then the owner). That agency provided and operated checkpoint metal detectors and X-ray machines to screen passengers and carry-on bags.

In June 1985, an Air India flight from Toronto to New Delhi was destroyed in flight by a bomb, and on the same day two baggage handlers in Tokyo were killed by a bomb that originated on a flight from Vancouver and was destined for another Air India flight. Those events led to stepped-up passenger checkpoint screening, and physical inspection or X-ray of all checked luggage on international flights, as well as the installation of 26 explosive detection system (EDS) units for checked baggage screening and the use of passenger bag matching on international flights, along with policy changes to strengthen airport security. After 1992, when airports were divested by the national government to newly created airport authorities, responsibility for passenger and baggage screening shifted to airports and their airline tenants.

In the wake of the 9/11 attack, new legislation was enacted in March 2002, the Canadian Air Transport Security Act. It created a new crown corporation, the Canadian Air Transport Security Authority (CATSA), which was given responsibility for several core functions, including provision of passenger and baggage screening at 89 airports, as well as developing a program for screening persons with access to secure areas of airports and assisting airports financially with the cost of increased policing at the 17 largest airports. CATSA has also been given responsibilities to develop and implement biometric identity cards for persons needing access to restricted areas at airports and to enter into financial agreements with the Royal Canadian Mounted Police to provide air marshals on selected flights.

Transport Canada's role was changed by the 2002 legislation. The creation of CATSA refocused Transport Canada on security policy and regulation, rather than the direct provision of security services, which became CATSA's responsibility.

In part because of the need to get into operation rapidly, and perhaps in part based on the success of outsourced screening functions in Europe in the 1990s, CATSA opted to contract with private service providers for those functions at all 89 airports. As of 2006, CATSA had more than 20 contracts with 12 different security companies to provide screening at these airports.<sup>(10)</sup>

Along with creating CATSA, the government enacted an Air Travelers Security Charge (ATSC), to be paid by passengers "at a level sufficient to fund the enhanced air travel security system." The charge is added to airline tickets and remitted to the government, and the funds are appropriated annually for CATSA's use. Since its inception, revenues from ATSC have exceeded CATSA expenditures, resulting in several decreases in the rates charged for various categories of air service.

#### **4.4. United States**

As in Europe and Canada, the evolution of the U.S. aviation security system was driven by the changing nature of the threat. The first U.S. hijacking took place in 1961, the first of many such hijackings that ended up in Cuba. The Federal Aviation Administration, which included security among its safety regulatory duties, persuaded airlines to install a limited number of walk-through metal detectors and X-ray machines for carry-on items at selected airports from which hijacked flights had originated. With the airlines resistant to mandates that would increase their costs, the FAA did not pursue legislation. A further rash of hijackings for ransom in 1971 led to legislative proposals that did not pass, and a 1972 emergency rule by FAA requiring airlines to screen all passengers and carry-on bags. That policy was given the force of law by the Anti-Hijacking Act of 1974 and the Air Transportation Security Act of 1974. Airports were made responsible for the security of their premises, while airlines were responsible for screening (including the purchase and maintenance of the equipment). Since the latter costs became new airline operating expenses, the airlines had an incentive to keep them as low as possible, especially once price competition became important, following the Airline Deregulation Act of 1978. Airlines opted to outsource screening to private security companies, at the lowest possible cost.

The next changes, as in Europe and Canada, came about in response to the new threat of bombs in checked luggage, with the Pan Am 103 bombing as the trigger. The Presidential Commission on Aviation Security and Terrorism issued its report in May 1990, criticizing both Pan Am and the FAA for not making use of passenger bag matching. In response, Congress that year passed the Aviation Security Improvement Act, which ordered the FAA to launch an accelerated research & development program to produce an effective explosive detection system for checked baggage, and introduced background checks for new employees and contract personnel with access to secure areas.

In response to two (non-terror-related) airline crashes in 1996, a White House Commission on Aviation Safety and Security was created. Its final report recommended government funding for aviation security, licensing and performance standards for screening companies, background checks for all screeners and persons with access to secure areas, expanded testing of airport security, and comprehensive passenger-baggage matching.<sup>(11)</sup> It also recommended that a passenger pre-screening system developed and used by Northwest Airlines called CAPPS (Computer Assisted Passenger Prescreening System) be used by all airlines, which took place starting in 1998. However, the FAA's 1999 rules on CAPPS limited its use to determining which passengers should have their checked baggage screened for explosives. The FAA barred its use for selecting passengers for extra screening and searching, on grounds that this might be interpreted as discrimination.<sup>(11)</sup>

The poor quality of passenger and baggage screening had been the subject of several reports by the government's General Accounting Office, starting in 1987. In that first report, GAO recommended that FAA set performance standards for passenger screening, but the FAA failed to act. In 1996, Congress included in legislation reauthorizing the FAA the requirement that it "certify companies providing security screening and improve the training and testing of security screeners through the development of uniform performance standards for providing security screening services." FAA finally issued a proposed rule in January 2000, but when it had not been finalized by November of that year, Congress directed the FAA to issue the final version by May 31, 2001. The FAA failed to meet that deadline, and as a result, no such standards were in place by Sept. 11, 2001.<sup>(12)</sup>

Thus, when the 9/11 attack occurred, the United States had a mediocre, low-performing passenger and baggage screening system. Fewer than 150 EDS machines were in use (at larger airports), background checks had been expanding but were far from universal, and passenger-bag matching was in use only for flights to and from Europe and the Middle East. However, none of these factors were implicated in the 9/11 attackers' success with a new mode of attack on aviation. The only measure that might have stopped them—the use of CAPPS to select higher-risk passengers for what we now term “secondary screening”—had been forbidden by the FAA.

Nevertheless, the well-documented poor performance of airline-hired screening companies became the main focus of attention as Congress debated legislation to beef up U.S. aviation security. The resulting Aviation and Transportation Security Act of 2001 (ATSA), enacted barely two months after 9/11, “federalized” airport screening by creating a new federal government agency, the Transportation Security Administration to carry out expanded passenger and baggage screening using a large new cadre of government employees. It set aggressive deadlines for TSA to staff up and take over screening from the security companies and appropriated funds to purchase several thousand EDS machines and many more electronic trace detection (ETD) machines to permit 100% screening of all checked bags for explosives by a date certain (which subsequently had to be extended by one year). CAPPS was allowed to be used to designate selectees for secondary screening, and a more-advanced successor version (CAPPS-2) was promised.(13)

ATSA also created two sources of funding for aviation security. The Sept. 11<sup>th</sup> Security Fee, like Canada's ATSC, is imposed on airline tickets. The Aviation Security Infrastructure Fee is a tax on airlines, intended to raise approximately the amount they had been spending on outsourced screening services each year. Together, these two sources covered 42% of TSA's aviation security budget in 2005, 43.6% in 2006, and 51.8% in 2007.(5)

The TSA was originally housed within the U.S. Department of Transportation, with its initial staff coming mostly from the FAA's former security operation. But in November 2002 Congress passed legislation creating the new Department of Homeland Security.(13) TSA was one of dozens of federal agencies shifted into the new department.

## **5. Comparison and Assessment of Current Aviation Security Policies**

### **5.1. Who Pays for Aviation Security?**

Our first point of comparison among Canada, Europe, and the United States will be to examine which parties are responsible for paying for the aviation security regimes enacted following the 9/11 attacks. The Canadian system represents the most transparent case. As noted in the previous section, the Air Travelers Security Charge is applied to all airline tickets (with different rates for domestic, trans-border to/from the USA, and other international flights). Its proceeds fund 100% of the budget for CATSA, which handles airport security and the funding of air marshals; it also paid for strengthening the cockpit doors of Canadian airliners and pays the costs of additional Transport Canada security inspectors.

Thus, Canadian policy on transportation security appears to be mode-specific, i.e., the costs of protecting a mode of transportation are borne by the users of that mode. (Whether Canada is applying that policy consistently to other modes is beyond the scope of this paper.) Canadian airport and airline trade associations argue that “aviation security is a ‘national defence’ issue and as such should be funded from general revenues.”(14) But after making this point, their

recommendations (during a five-year review of CATSA in 2006) all focus on making the present funding mechanism more transparent and responsive to changing needs.

In Europe, the pattern varies by country. In the United Kingdom, the major airports (all of which are commercialized, with most now in the private sector) are responsible for all airport security, at their own expense. These costs get factored into the cost base on which they charge airlines for airside and landside services. Germany has a federal aviation security tax which is added to airline tickets, but that tax covers only a portion of the capital and operating costs of airport security, the balance of which are paid for out of airport budgets. Some German airports (e.g., Frankfurt, Hamburg, Dusseldorf) have been privatized, while others remain owned by some combination of state (Land) and municipal governments. Thus, ultimate responsibility for aviation security costs in Europe seems to be a mix of passenger taxes and airport costs, with the latter being absorbed by airline charges. Article 5 of 2008 EC Regulation No 300/2008 allows for each member state to decide the mix of funding, from the state, airports, airlines, other agencies, and users (presumably passengers and shippers). Thus, Europe is not as mode-specific in its approach to security funding as is Canada.

However, the E.U. countries seem to be moving in the direction of the “user-pays” approach. A recent survey by the European Commission found that 11 member countries rely almost exclusively on aviation fees to support the costs of aviation security, while six sometimes make significant general tax support for such costs and four did not provide such information.<sup>(15)</sup> The Commission recommended increased transparency to ensure that aviation users can ascertain that such fees are used only for security costs and do not discriminate among airlines or airports. As a step toward that end, it also recommended “one-stop” security for intra-EU passengers—i.e., the elimination of re-screening of such passengers when they change planes at an airport within the EU, “provided the infrastructure separates passengers screened under EU requirements from other passengers.”

The United States presents the most complex assortment of funding sources. As noted in the previous section, by 2007 the fraction of TSA’s aviation budget that was provided by security taxes on airlines and passenger tickets slightly exceeded 50%. The balance of TSA’s funding comes from the federal government’s general fund. In addition, airports themselves are responsible for access control and airside security, costs which become part of their cost base and are passed along to airlines via airport rates and charges. Cost estimates for those portions of aviation security expense are not readily available. But because of significant federal general-fund support of TSA’s aviation security budget, the United States departs significantly from the fully mode-specific funding approach of Canada and the increasingly mode-specific funding approach of EU countries. (Incidentally, U.S. airlines make the same argument as their counterparts in Canada and Europe: that aviation security is basically a national defense function and should be covered entirely from the federal government’s general fund.)

There is some merit to the argument that transnational terrorism is a threat to entire societies and therefore that measures taken against it could be considered one component of national defense and hence paid for out of general government revenues. However, if some components of a society present larger targets to terrorists, there is some justification for deciding that those who make use of that component should bear the costs. In this sense, security expenses can be seen as analogous to insurance. In general, in free societies, we allow people to engage in activities with various levels of risk (such as building homes in flood plains or on earthquake faults, or building and operating oil refineries). Those activities that are inherently higher-risk generally carry higher insurance costs, reflecting those risks. The existence of high insurance costs generally provides incentives for those incurring those costs to take protective measures to

minimize risks. In hindsight after 9/11, U.S. airlines learned that their low-performance contracts for passenger screening were inadequate to the task of coping with suicide-bomb threats. If the federal government had not taken over that function shortly thereafter, it is likely that airlines would have insisted on higher-quality screening thereafter.

As noted previously, airlines and airports object to the mode-specific approach, making the national-defense argument in Canada, the EU, and the United States. Despite this rhetoric, in fact they function as advocates for greater cost-effectiveness in aviation security policy, since they and their customers must bear the costs. Thus, their behavior supports the hypothesis that mode-specific funding serves as a check on unwise spending.

However, the case for mode-specific funding being applied to aviation is only fair (in the sense of not creating distortions in mode-choice for customers) if the same principle is applied to the security costs of other transport modes. While an examination of the extent to which this is being done is beyond the scope of this paper, one indication is provided by a recent U.S. report, from the DHS's Office of Inspector General.<sup>(16)</sup> Only in 2005 did the TSA begin to devote resources to surface transportation modes, creating a small workforce of 100 Transportation Security Inspectors (expanded to 175 in 2008). Their initial focus is on mass transit and freight and passenger railroads. The TSA also operates three surface transportation security grant programs—for mass transit, trucking, and intercity bus transportation. In FY 2008, funding for these three programs totaled \$415 million. While that sum is less than 10% of the TSA budget for aviation, all such funding for surface transportation security comes from federal general funds, rather than from security fees or taxes on the modes in question.

If those involved with a particular type of transportation must bear the costs of securing that mode against terrorism, they presumably will be more concerned than otherwise about the cost-effectiveness of those protective measures. As the EC report states, "It may be reasonable that security measures are financed, at least in part, by passengers, cargo shippers, and [carriers], as they are best placed to scrutinize the cost implications of security measures."<sup>(15)</sup> Given the tendency of elected officials to enact grandiose target-hardening plans without benefit of analysis, a countervailing force directly concerned with the costs of those plans seems wise.

On this score, then, Canada appears to be the most consistent adherent of the user-pays (or mode-specific) approach to paying for at least aviation security, with the United States departing the most from this approach.

## **5.2. Who Provides Aviation Security?**

As is the case with funding, the provision of aviation security varies considerably among countries. All OECD members have designated a single national agency to be responsible for aviation security—Transport Canada in the case of Canada, the Transportation Security Administration in the United States, and usually a transport ministry in European countries. Those agencies are responsible for making policy decisions about security (within the constraints of legislative direction), and for regulating the various entities involved in aviation—airports, airlines, pilots, etc. But which party actually delivers various security functions differs considerably.

Canada is unique in having created a crown corporation to carry out most aviation security functions: passenger and baggage screening, access control, biometric identity cards, etc. In Europe, these functions are usually the responsibility of each airport. The United States is unique on having a decidedly mixed system, thanks to the way Congress defined the TSA in its 2001

legislation. By law, TSA must carry out passenger and checked-baggage screening at nearly 450 commercial airports, despite TSA also being the national aviation policy-maker and regulator. Yet nearly all the remaining airport security functions—access control, perimeter protection, terminal-area policing, etc.—are the responsibility of the airport, under TSA’s regulatory oversight. Thus, the TSA combines regulation and service provision within a single entity—a troubling conflict of interest, which violates the principle of arm’s-length regulation. And TSA’s responsibility for providing some but not all airport security functions means divided airport security, when unified security and single-point responsibility would be wiser.

One of the largest contrasts in the provision of security functions is the use of private security firms for passenger and baggage screening. Where this function has been devolved from the national policy-maker to either the airport level (Europe) or to a crown corporation (Canada), the inherent advantages of outsourcing have led to its universal adoption in Canada and to its widespread use in Europe. But in an over-reaction to the low-performing airline security contractors in place at U.S. airports prior to 9/11, Congress mandated that a federal government workforce carry out passenger and baggage screening nationwide. Only after a bitter battle in Congress was a small pilot program included in the legislation, under which five airports (one in each size category) would be permitted to use private security companies for screening, and after two years of TSA provision at all other airports, those airports would be permitted to ask TSA to leave and replace their people with a TSA-approved security company, selected by TSA and assigned to that airport. Despite better performance by security companies at the five pilot-program airports, no airport has asked TSA to leave (perhaps because TSA is also its security regulator).

An important advantage of outsourcing passenger and baggage screening is flexibility. An increasingly deregulated airline industry is dynamic, with new airlines being created, older ones merging or failing, and services being increased or decreased both seasonally and in response to airline initiatives and the ups and downs of the economy. Numbers of emplaned passengers at U.S. airports fluctuate up and down from one month to the next from 10 to 20% for most airports, with some smaller airports experiencing much larger monthly changes.<sup>(17)</sup> Yet the TSA’s allocation of screeners to airports is done on an *annual* basis, making it difficult to match staffing to workload. That is the kind of short-term flexibility that outsourcing facilitates. Another problem that has manifested itself in both Canada and the United States is uniform national compensation levels for airport screeners. In both countries, the cost of living (and hence pay scales) varies considerably from one region to another, with CATSA having particular difficulties attracting and retaining screeners in the booming oil province of Alberta.

But the larger, long-term advantage of outsourcing was noted in the RAND Corporation paper on how terrorists adapt to defensive technologies. Over time, terrorists may avoid the technology or alter their operational practices. Five years from now, a 43,000-person civil-service work force of TSA airport screeners may no longer be appropriate, due either to changes in terrorist methods of operation or to improved technologies. In that eventuality, it would be far easier to down-size outsourced screening workforces—and redirect the resources to higher-priority uses--than to reduce the number of civil servants expecting something akin to lifetime tenure.

Thus, on the question of how airport security functions are provided, the European approach of devolving the responsibility for provision to each airport and permitting outsourcing by airports, under regulatory supervision, seems wisest. It allows for tailoring service levels to local conditions and it provides flexibility to upsize or downsize in response to changing threat levels and priorities. The least flexible approach is that of the United States, with a highly centralized

approach and the blurring of regulation and service provision. Canada's somewhat decentralized approach, with outsourcing, is somewhere in between.

### **5.3. How Risk-Based Are Current Security Policies?**

#### **5.3.1. ICAO Sets the Context**

ICAO's Annex 17 sets forth the minimum aviation security standards expected of all member states.<sup>(18)</sup> As noted previously, it requires each state to have a civil aviation security organization and a written aviation security program, as well as requiring each airport and airline to have a written security program. Supplementing Annex 17 is the *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference*, commonly referred to as ICAO DOC 8973. It provides detailed procedures and guidelines on how states may go about implementing the provisions in Annex 17, but is guidance, not a standard.

Standard 3.1.3 of Annex 17 states that each contracting state "shall keep under constant review the level of threat to civil aviation within its territory, and establish and implement policies and procedures to adjust relevant elements of its national civil aviation security program, *based on a security risk assessment* carried out by the relevant national authorities."(emphasis added) As interpreted by the review panel on CATSA in 2006, this establishes two basic principles for aviation security policy:

- "[I]t must be intelligence-led, based upon up-to-date threat assessments and resilient enough to adapt to new threats as they emerge."
- "Risk analysis and assessment are the basis for effective use of security resources."<sup>(18)</sup>

While this might sound like a grant of considerable freedom, the document goes on to provide standards for pre-board screening of passengers and baggage, the quality of screeners and periodic testing of them, passenger-bag reconciliation, cargo security controls, access control via secure identification and random screening, and airport perimeter control. Other Annexes provide for secured cockpit doors, procedures for dealing with disruptive passengers, and air marshals.

Thus, while the ICAO Annexes seek to ensure that at least minimum attention is given to all of these areas, there is potential tension between the implication that various inputs and methods *must be used* and the directive that decisions should derive from risk analysis based on up-to-date intelligence.

#### **5.3.2. Canada's Aspirations for Risk-Based Policy**

The 2006 Advisory Panel review of the Canadian Air Transport Security Authority Act includes a section called "Risks and Layers: Envisioning Aviation Security." It cites the ICAO rhetoric and notes that "[Security] resources, financial and human, are not unlimited and should be allocated according to assessed risk."<sup>(10)</sup> It notes that Canada's Auditor General the previous year had insisted that a risk-based approach is desired and expressed disappointment that Transport Canada "has not fully implemented formal risk management."<sup>(19)</sup> The Advisory Panel report goes on to say that in its presentations to the Panel, "CATSA referred to its concept of security screening as risk-based," and that "Priorities must be established, and these should be based on assessments of the relative level of risk."

But industry stakeholders, such as airports and airlines, told the Panel that CATSA should follow a more seriously risk-based approach. For example, in passenger screening, the agency should “focus on higher-risk passengers, rather than on the objects carried by all passengers.” They also called for better background vetting, so as to streamline the screening that takes place at the airport, “such as [via] a Registered Traveler Program.” The submission by the Canadian Airports Council (CAC) used stronger language, saying that the current “one size fits all approach wastes precious resources.”(14) CAC urged that CATSA move to “a standard that allows different levels of screening at sites and between sites based on risk assessment criteria,” and also recommended that a Registered Traveler program be implemented.

According to an interview with the chief executive of CAC, as of late 2008 none of the changes the organization recommended have been implemented, but he believes that risk-based changes are coming, with ICAO encouragement.(20)

### 5.3.3. *Europe’s Steps Toward Risk Assessment*

The fourth section of Article 4 of EC No. 300/2008 permits member states to “adopt alternative security measures that provide an adequate level of protection on the basis of a local risk assessment.” By being presented in the context of criteria that would allow states to “derogate from the common basic standards,” this wording implies that less-stringent protection may be provided if justified by lower levels of risk or certain locations, aircraft sizes, or infrequency of operation.

According to European airport and airline groups, efforts to implement a truly risk-based system are at an early stage within the EU. In October 2006 the Airports Council International-Europe and the Association of European Airlines created a joint effort “to address shortcomings of the current system.”(21) In its news release announcing the launch of the European Strategic Partnership for Aviation Security (ESPAS), the Director General of ACI Europe said that “Any new security rule should focus specifically on the threat or risk that needs to be eliminated, taking account of the impact on passenger mobility and convenience, operations, and cost.” Industry sources portray the replacement of EC No. 2320/2002 with No. 300/2008 as a step toward a more flexible and better-harmonized aviation security system within Europe. The online publication *HomelandSecurityEU.com* commented, “From an industry standpoint, the inclusion of risk assessment is the key element of the new regime. By ensuring that the new security measures deriving from the framework are risk-based, each party will fully accept its responsibilities and its role in the security chain.”(22)

However, as of early November 2008, the Policy Manager for ACI Europe stated that “We are still in the early process of a truly risk-assessment-based system in aviation security in the EU.”(23)

### 5.3.4. *The USA – Mostly Rhetoric on Risk-Based Policy*

The Transportation Security Administration is one of many agencies that are part of the Department of Homeland Security. In 2005, the relatively new DHS Secretary Michael Chertoff announced a sweeping reorganization of the agency, shifting to what appeared to be a more risk-based approach to security. The well-respected former Inspector General of DHS, Clark Kent Ervin, praised the new approach as “a threat-based, risk-based, consequence-based approach.” And then-new TSA Administrator Kip Hawley said that “The federal government must focus resources on the basis of consequences, threat and vulnerability assessments, and the prioritization of risks.”(17)

The three years since 2005, very little evidence of risk-based policy change has emerged from the TSA. In an August 2007 report on DHS's progress in implementing its mission, the Government Accountability Office assessed the department's progress in aviation security as "moderate" and said that "Th[e] lack of a comprehensive strategy and integrated management systems and functions limits DHS's ability to carry out its homeland security responsibilities in an effective, risk-based way. DHS has also not yet fully adopted and applied a risk management approach," although the TSA had taken some steps in that direction.(24) In June 2008 GAO published a summary of a forum in which 25 experts discussed the issue of applying risk management to homeland security.(25) They considered the Coast Guard (but not TSA) to be one of the few federal government agencies that had effectively incorporated risk management principles into its decision-making; they also suggested that responsibility for risk management has been so distributed as to inhibit coordination on overall security priorities.

An example of TSA's unwillingness to embrace a risk-based approach is the evolution of the U.S. Registered Traveler (RT) program. When the idea was first introduced to the aviation security community shortly after 9/11, it was presented as a risk-based program that would lead to better allocation of airport screening resources, by permitting those who had been "pre-screened" to receive a lower level of scrutiny at the checkpoint.

Unfortunately, once TSA permitted the RT program to be launched by private provider companies, the agency was unwilling to do more of a check than simply to verify that an applicant was not on the TSA watch list. Since TSA Administrator Kip Hawley believes that carefully-selected "sleeper" terrorists could pass that test, he concluded of RT that "It's not a security program but an ID [identification] program."(26) Screening of RT members is therefore exactly the same as for non-members.

Despite this rather dismal record, U.S. aviation stakeholders and TSA have been conferring about a methodology for risk-based assessment of aviation security policies. A group of stakeholders, including airlines, airports, law enforcement, and Boeing Company have been working with TSA and DHS starting in 2007 and continuing in 2008 to develop a Risk Management Assessment Plan (RMAP). Reportedly, the group has developed a risk assessment model, as a tool for better decision-making. One application would be for a TSA Federal Security Director for a particular airport to be able to use RMAP to put in place various changed policies that would not likely be anticipated by terrorists.(27)

## **6. Toward a More Risk-Based Approach**

### **6.1. Introduction**

As we have seen, aviation security officials in Canada, Europe, and the United States have all professed the importance of risk assessment as an important tool for allocating limited resources to protect civil aviation from terrorist attacks. But thus far, there is little evident use of such assessment to make judgments about which current policies are worth their costs. In section 3.0 we saw an example that suggested poor cost-effectiveness for air marshals, in terms of likely lives saved per million dollars spent. That example concerned in-flight security, where all the countries under consideration in this paper have adopted the cost-effective measures of strengthening cockpit doors and changing the protocols by which flight and cabin crew deal with attempts to commandeer an aircraft in flight. In this section we will consider what similar risk assessment might imply, for screening of passengers and baggage and for air cargo.

## 6.2. Risk-Based Passenger and Baggage Screening

Current screening practices are very similar in Canada, Europe, and the United States—and indeed, given the extensive travel among these jurisdictions, reasonably common and consistent policies make good sense. The major change entailed by the proposed risk-based approach would be to alter the present de-facto policy of treating all passengers and bags as needing equal scrutiny. Instead, the system would be based on applying somewhat different procedures to different passengers and their bags, based on an assessment of their relative riskiness.

### 6.2.1. Three-Tiered Approach for Air Travelers

The basic approach was outlined in this author's 2006 paper on risk-based airport security.<sup>(17)</sup> Its premise is that the task of airport screening should be to identify and isolate dangerous persons, not dangerous objects *per se*. The challenge is to keep those persons from causing harm, either in the terminal area or to the planes themselves. There are many ways in which terrorists can cause great harm in connection with airports: getting on board with the aim of hijacking, getting on board as a suicide bomber, putting explosives into checked luggage but not getting on board, or targeting large concentrations of passengers in terminals. Current policies devote the major share of airport security resources to just one of these threats: preventing would-be hijackers from boarding with weapons. Yet strengthened and locked cockpit doors (along with changed protocols for how crews deal with hijack threats), have greatly reduced the hijack threat. Far less money and effort is spent on securing airport terminal lobby areas and the ramp area where planes park. Thus, current policy, in effect, downplays the threat of suicide bombers targeting crowds at checkpoints and lobby-based EDS installations, and the threat of bombs being smuggled onto planes from the ramp (as opposed to the terminal).

The proposed risk-based approach would shift the focus to identifying dangerous people. This could include greater security guard presence in terminal lobby areas and outside the terminal, in ramp areas and around the airport perimeter. And within the terminal, at the checkpoint it requires separating passengers into at least three defined groups, based on the quantity and quality of information about each:

- Low-risk passengers, about whom a great deal is known.
- High-risk passengers, based either on no knowledge or on specific, negative information.
- “Ordinary” passengers, mostly infrequent flyers and leisure travelers.

A different approach to both passenger screening and bag screening would be applied to each group.

Low-risk passengers are defined as those who possess a current government security clearance or who have been accepted into a Registered Traveler program by passing a background check and being issued a biometric identity card. Passengers in this group would go through express lanes at checkpoints, with something like pre-9/11 protocols (e.g., no shoe or jacket removal, not having to remove laptops or video cameras, etc.). Their checked bags would not routinely be EDS-screened. The point is to not waste the system's resources or those passengers' time on procedures that add very little value to airport security. As a safeguard against the small probability that a dangerous person might slip into this category, a certain

percentage of these people and their bags would be randomly selected for “ordinary passenger” screening, and this policy would be well-publicized.

High-risk passengers include those with no paper trail, about whom so little is known that the safest thing to do is to assume the worst and do a thorough screening of both person and bags (both checked and carry-on). Everyone in this group, in other words, would receive a more rigorous version of today’s “secondary” screening, to include both explosive-detection screening of their carry-ons and either see-through scanning to detect non-metallic objects or a thorough pat-down search. The same protocol would apply to those whose names appear on government-maintained watch lists. Some of those in the latter category—those on a No-Fly list—would be detained rather than being put through a screening process.

Ordinary travelers are those in between the other two risk categories. These people would receive something like today’s level of passenger screening (but with a better-justified list of banned objects). A fraction of this group would be randomly selected for secondary screening, as described above.

#### 6.2.2. *Identifying Low-Risk Passengers (Registered Traveler)*

Michael Levine and Richard Golaszewski suggested the idea of separating out low-risk travelers and expediting their processing at airports in an article published two months after 9/11.(28) Frequent flyers would be able to apply to national aviation security authorities for membership by submitting to a background check, equivalent to a low-level security clearance. Those who passed this one-time screening would obtain a biometric identity card, and when they used the card at the airport to prove they were the person who had been cleared, they could bypass the more-stringent post-9/11 screening.

The concept was first subject to detailed analytical scrutiny by a team of graduate students in operations research at Carnegie Mellon University in 2003.(29) They first created a model of passenger checkpoint processing, based on data from Pittsburgh International Airport (PIT). Next they created a design for a Registered Traveler program called SWIFT and simulated its operations using the model. Based on data from two surveys of airline passengers, they estimated that 40% of originating passengers would sign up for and be accepted into the system. Based on their simulation, first-class and elite frequent flyers (who already had a priority line at PIT) would see their average throughput time cut nearly in half, from 2.5 minutes down to 1.35. Coach passengers joining the program would have their average time slashed from 19.5 to 1.35 minutes. But those still using the regular lanes would benefit also. Since 40% fewer people would be using the regular lanes, their average processing time would drop from 19.5 to 12.1 minutes. The paper estimated that first-year benefits would exceed first-year costs by \$2 million at PIT.

The RAND Corporation subsequently estimated that a protocol that would exempt Registered Travelers from the mandate for 100% screening of their checked baggage via explosive detection systems (EDS) would reduce the number of these costly machines required nationwide by approximately one-half.(30)

As noted in the previous section, when TSA allowed RT to be introduced, the only background check it carried out was to check applicants against its watch list—the same procedure applied to every air traveler prior to issuance of their boarding pass. Understandably, this was inadequate for allowing RT members to get less screening at the checkpoint than other air travelers. TSA has implied that the cost of a “real” background check would be prohibitive. Yet several million U.S. aviation workers have been subjected to criminal history background checks

since 9/11, as a condition of being allowed access to secure areas of the airport on a regular basis. This program is operated by the American Association of Airport Executives (AAAE), in cooperation with the Federal Bureau of Investigation, at a cost of \$27 per person.(31) At nearly all U.S. airports, such airport workers do not have to pass through metal detectors or have their tools X-rayed when entering secure areas. In fact, from the inception of the RT program, the certified RT companies sent the fingerprints of all applicants to the AAAE clearinghouse, but TSA never gave permission for these 200,000 sets of prints to be sent to the FBI for the expected criminal history background check.(32) Thus, a background check that TSA deems sufficient to allow unescorted and unscreened airport workers access to planes is deemed insufficient to allow RT members to pass through a streamlined version of checkpoint screening, as envisioned in the original RT concept.

As of this writing, the only Registered Traveler program in operation is the non-risk-based one in the United States. (A few countries' border control agencies have begun International Registered Traveler programs, but these merely permit expedited entry of frequent air travelers to the country in question; they are not part of an airport security program.)

### 6.2.3. *Separating Ordinary and High-Risk Passengers*

Once low-risk passengers have been self-selected out of the mix, the remaining task is to use all feasible information to separate high-risk passengers from all the rest. One tool for doing this is a government-maintained watch list, continuously updated, against which all airline passenger reservations would be checked by the national aviation security agency in real time. In the United States, such a program is scheduled for implementation in 2009, under the name Secure Flight.

A second approach is to assess what is known about each passenger, based on information provided at the time of ticket purchase. In the United States until 2009 this has been carried out by the Computer Assisted Passenger Prescreening System (CAPPS), which dates from pre-9/11 days. The idea of such risk-screening systems is to use various algorithms to (1) verify the passenger's identity, and (2) look for patterns that might suggest high risk. CAPPS, and presumably Secure Flight, uses algorithms to flag some passengers for secondary screening.

To supplement the above tools, and to deal with lobby-area persons not holding tickets (and therefore not passing through the screening checkpoints), a technique called "behavioral profiling" is being used at Israeli airports (33), Boston's Logan Airport, and Las Vegas casinos. The general idea is to unobtrusively monitor people's behavior, looking for suspicious activities, to be followed up by questioning by security personnel. Many other airports maintain either covert or highly visible law enforcement patrols within airport premises, including lobby areas and airside areas.

### 6.2.4. *Redesigning Passenger Checkpoints*

Security checkpoints for a risk-based system would be different from those at today's airports. First, there would be two different sets of lanes, one set for Registered Travelers and the other set for all others. The proportion of each would have to be varied over time, depending on the fraction of daily originating passengers who were RT program members. Space would be required on the approach to the RT lanes for kiosks at which members would insert their biometric identity cards to gain admission to the line for these lanes. These kiosks might be combined with common-use boarding-pass kiosks, saving RT members without checked baggage from having to stop at two different kiosks.

On the sterile side of the checkpoint, additional space would be required for secondary screening portals to check the bodies and carry-on bags of selectees for explosives and potential weapons. All high-risk passengers (except those on the No Fly list, who would be detained) would automatically go through secondary screening. Boarding passes would be coded electronically, not visibly, so that a selectee would not know whether he/she had been selected by an algorithm or at random.

Meeting this set of requirements may require somewhat more square footage than is now allocated for checkpoints, though this will vary from airport to airport. On one hand, added space would be needed for RT kiosks and for expanded secondary screening equipment for selectees. On the other hand, significant RT enrollment should reduce the length of waiting lines (and hence reduce the area needed for that purpose). And a smaller total number of selectees (thanks to more precise identification of people leading to fewer false positives in checks against watch lists) would lead to a smaller secondary screening area than if current percentages of passengers continued to be selected.

#### 6.2.5. *Redesigning Checked Baggage Screening*

Neither Canada nor most European countries requires 100 percent of all checked baggage to be scanned by costly EDS machines. But where that mandate applies (as in the United States), the risk-based model would reduce the size and cost of checked baggage screening. The bags of RT members could be screened via two-dimensional X-ray machines, and would only move on to the more costly screening if a possible problem was detected by the initial X-ray. RAND Corporation has done a number of studies of the impact that an RT program (which RAND refers to as “positive profiling”) could have on the size and cost of EDS installations at large and medium airports. In a 2004 report, one simulation modeling exercise used the following parameters: size the system to ensure that bags get to the intended flight 99% of the time, assume 90% reliability (up-time) of the EDS machines, and assume that 50% of all bags are exempted from EDS screening.(30)

For this particular set of assumptions, the RAND team estimated the total cost to the flying public of various levels of EDS deployment, where cost includes both the capital and operating costs (screener payroll) of the EDS machines and the extra time currently wasted by passengers getting to the airport early enough to ensure that their flight is not delayed due to slow bag processing. In the absence of an RT program, the optimal number of EDS machines under these assumptions (nationwide) was found to be 6,000. But with an RT program that exempts 50% of all bags from screening (defined as screening all bags of non-RT members plus one-sixth of the bags of the 60% of daily passengers who are RT members), the optimal number of EDS machines declines to about 2,500. That’s a very large difference in both the space required at airports and also in capital and operating costs. In round numbers, under a reasonable set of assumptions, an RT program could cut costly EDS deployment by up to 50%.

Some of the capital cost savings could be used for expanding passenger checkpoints and/or for improving terminal access control and airport perimeter control. The latter two uses aim at protecting planes on the ramp from unauthorized persons. And some of the payroll cost savings (from fewer EDS machines) could be used to add security personnel in lobby areas and to add staff for access control and perimeter control, as necessary.

The risk-based approach should produce significant savings in passenger time, by speeding up baggage screening and passenger screening alike. While the modeling necessary to quantify such savings is beyond the scope of this paper, the ultimate impact would be that people would

not have to arrive at airports as early as they have learned to do in the post-9/11 era, reclaiming that time for personal or business purposes.

### **6.3. Air Cargo Security**

This discussion is limited to “belly cargo,” i.e., cargo that is carried in the baggage compartment of passenger planes. In sharp contrast to the non-risk-based approach to airport screening followed in Canada, Europe, and the United States, a generally risk-based approach to air cargo has been used since 9/11 in all of these jurisdictions. It parallels the way cargo is dealt with in the maritime system and in cross-border trucking and railroads. That general approach is to rely on a combination of intelligence information, “known shippers,” and random screening.

The enormous volumes of cargo in all of these modes, and the very high costs in both time delays and equipment that would be required if all cargo had to be physically screened seems to underlie the acceptance of risk-based approaches as a practical reality. Yet when it comes to belly cargo on passenger planes, the inconsistency between the U.S. policy of requiring 100% of all checked baggage to be screened by the most costly form of equipment (EDS) while belly cargo that sits next to those bags in the cargo hold is largely unscreened has led to repeated calls to close the belly cargo “loophole.”

In Canada, as of the 2006 review, CATSA had no mandate to screen cargo, but in its Budget 2006 document, the government allocated \$26 million over two years to design and test an air cargo security initiative, while Transport Canada was developing an Air Cargo Security Strategy in consultation with aviation stakeholders. Canada’s Border Security Agency in December 2005 required all air carriers and freight forwarders to electronically transmit air cargo data to it before loading the cargo at foreign airports. The CATSA Advisory Panel recommended that a similar program be implemented for air cargo originating in Canada.

In Europe, the new EC No 300/2008 calls rather vaguely for member states to determine “conditions under which cargo and mail shall be screened or subjected to other security controls, as well as the process for the approval or designation of regulated agents, known consigners, and account consigners.” The CATSA Advisory Panel singled out the U.K. approvingly for its existing air cargo screening system “with its process for certification and verification of the security practices of known shippers, including periodic inspection of their facilities.”

The struggle between risk-based and 100% physical screening approaches was highlighted in the United States when Congress included a measure based on the latter approach as part of the 9/11 Commission Act of 2007. The air cargo provisions called for TSA to physically screen all belly cargo, with 50% of this to be accomplished by February 2009 and 100% by August 2010. Airlines and airports objected that enforcing such a requirement at airports would be very difficult. There would be space problems, since belly cargo for wide-body planes often arrives on pallets, which are far too large to screen using the equipment in place for baggage screening; hence, large new facilities would be required to house costly new equipment. Moreover, the time required to physically screen all such cargo would disrupt schedules, undercutting the rationale for shipment of high-value, time-sensitive cargo by air.(34)

In response, TSA has developed the Certified Cargo Screening Program (CCSP), which would distribute most of the screening function to various points in the supply chain. Shippers and freight forwarders may opt to become Certified Cargo Screening Facilities, which would screen and seal shipping crates, pallets and/or containers. The sealed boxes would be delivered by them to the airport by certified personnel, to be turned over to the airlines for loading. In effect,

this represents an elaboration of the previous “known shipper” program. Under that program, shippers and freight forwarders who met certain TSA requirements (mostly about supply-chain integrity and control) were deemed to be safe originators of air cargo, whose packages required no more than occasional random screening at the airport, supplemented by periodic vetting of the shippers by TSA inspectors.

The new CCSP carries a high cost. An initial 2007 estimate from the Congressional Research Service was a cost to shippers and forwarders of \$3.7 billion over its first 10 years.(35) In 2008, the Government Accountability Office provided information enabling a more current estimate to be made (36). For an estimated 12,000 forwarders and shippers who may participate in CCSP, using screening equipment costing an average of \$375,000 each, the total cost of just the equipment would be \$4.5 billion. To that must be added the ongoing costs of staff doing the screening, paperwork, and transportation plus the cost of expanded TSA staff to inspect these 12,000 sites. For context, U.S. belly cargo consists of about 250 million individual packages per year, providing \$4.4 billion in airline revenue.(34)

In October 2008, the United States and the European Union announced an agreement under which the EU agreed to comply with the U.S. deadlines for belly cargo screening on flights from EU countries to the United States (i.e., 50% screened by February 2009 and 100% by August 2010). It provides that the EU “will use the same screening equipment, provide the same training to screeners, and impose the same security requirements on facilities where cargo is screened.”(37)

Thus, recent developments appear to be moving air cargo (at least belly cargo) away from the former risk-based approach and toward the more prescriptive 100 percent approach applied to passenger and baggage screening. In other words, the discrepancy in policy regarding belly cargo and checked bags seems to be resolved by moving away from a truly risk-based approach. This may increase pressure from some quarters to apply similarly costly and non-risk-based approaches to all-cargo planes and later to other modes of shipping.

## **7. Summary and Conclusions**

Defending target-rich free societies against terrorism is inherently difficult. On a macro level, it seems unlikely that terrorism can be eliminated in a permanent sense; the inherent asymmetries will likely make free societies attractive targets for one or another terrorist group indefinitely. We also know that terrorists learn from experience, and can change tactics and targets in response to defensive measures. Therefore, defensive measures must be dynamic and flexible, rather than static and predictable.

Most of the current aviation security policies and programs in Canada, the EU, and the USA are responses to previous terrorist attacks, rather than more broadly based protections against a range of possible future threats. It seems likely that a number of such programs (e.g., air marshals and 100% EDS screening of checked baggage and belly cargo) would not pass a test of relative cost-effectiveness, such as the annual cost per life saved. Yet risk assessment, though much talked about as providing a sound basis for setting security priorities and allocating resources, seems to be very difficult to put into practice, despite its potential for getting significantly more value from whatever amount of resources is available in a country for aviation security.

In the United States, the largest resource allocation decisions have been made not by the designated security agency, the TSA, but by the U.S. Congress, and enacted as legislation.

These include the mandates for 100% EDS screening of checked baggage and 100% physical screening of belly cargo, the creation of TSA with the dual roles of aviation security regulator and airport screening provider, and a static, “fortress wall” approach to airport screening. These decisions were not based on analysis by security experts, but rather by elected officials seeking to reassure the public that aviation is well-protected, regardless of cost or secondary effects.

One possible incentive for a more risk-based policy is mode-specific security funding—e.g., that the costs of aviation security be paid for by aviation system users. This gives that user group an incentive to monitor the costs and cost-effectiveness of security programs that affect it, serving to some extent as a counter-weight to politicians’ tendencies to impose costly but ineffective programs. In this regard, Canada most closely adheres to this principle, with the United States departing the most from it and Europe in between.

In terms of flexibility, the EU countries have devolved airport security functions most completely to the airport level (under national government regulatory supervision), permitting resources to be tailored to need and, thanks to outsourcing, permitting changes in workforce levels in response to changing threat and demand levels. Canada makes wide use of outsourcing, but in a centralized model that does not take account of regional cost differences. The United States is least flexible, with all passenger and baggage screeners (except for a handful employed by highly regulated contract firms) working directly for the federal government. In addition, the U.S. model results in fragmented security responsibility at the airport level, with the TSA providing screening services and the airport providing all other security functions.

Rhetoric in all the countries examined here supports risk-based security, and indeed, that is largely the practice in all forms of goods movement, including air cargo. Perhaps that is because cargo is much less visible to the public, and because the consequences for supply chains would be so great if passenger-type security measures were applied to all goods movement. The GAO’s expert panel on strengthening the use of risk management principles was asked to identify the “key challenges” to doing so.<sup>(25)</sup> The number one challenge (35% of panelists) was to “Educate the public about risks and engage in public discourse to reach consensus on an acceptable level of risk.” Number two (19%) was to “Educate policymakers and establish a common lexicon for discussing risk,” to counteract political obstacles to risk-based resource allocation.

The goal of such efforts should be to wean legislators away from enacting mandates not based on risk analysis. Legislators should be encouraged to direct the national aviation security policymaker/regulator to address various problems within some kinds of quantitative parameters (e.g. the U.S. DOT’s \$3 million per life saved measure). Details of making actual policy and resource-allocation decisions should be left to the aviation security agency. That agency, in turn, should be flexible in tailoring policies to changing threats and different situations at individual airports, which vary enormously in type, size, configuration, etc.

No security policy should be pursued “at all costs,” since resources are always limited. Likewise, all possible targets cannot be hardened to any appreciable degree, without bankrupting a country. While it seems likely that commercial aviation will remain a high-profile potential target, spending billions every year on static defenses at airports is almost certainly a poor use of resources. Whether any kind of effort can succeed in educating elected legislators and opinion leaders to these realities is the most difficult challenge.

## REFERENCES

- (1) Todd Sandler, Daniel G. Arce and Walter Enders, *Terrorism: Copenhagen Consensus 2008 Challenge Paper*, Copenhagen, Copenhagen Consensus Center, 2008.
- (2) Michael D. Intriligator, "On 'Transnational Terrorism'" – Perspective Paper on the Todd Sandler, Daniel G. Arce, and Walter Enders Paper for the 2008 Copenhagen Consensus, December 2007, Copenhagen, Copenhagen Consensus Center, 2008.
- (3) Brian A. Jackson, *et al.*, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, RAND Corporation, 2007. ([www.rand.org/pubs/monographs/2007/RAND-MG481.pdf](http://www.rand.org/pubs/monographs/2007/RAND-MG481.pdf))
- (4) M. G. Stewart and J. Mueller, "Assessing the Risks, Costs, and Benefits of United States Aviation Security Measures," Research Report No. 267.04.08, University of Newcastle (Australia), 2008 (<http://hdl.handle.net/1959.13/28097>).
- (5) Clinton V. Oster and John H. Strong, "A Review of Transportation Security Administration Funding, 2001-2007," *Journal of Transportation Security*, Volume 1, pp. 37-43, 2008.
- (6) "Round Table on 'Security, Risk Perception, and Cost-Benefit Analysis,' Paris, 11-12 December 2008: Summary and Conclusions," Paris, OECD/International Transport Forum, January 2008.
- (7) Jens Hainmuller and Jan Martin Lemnitzer, "Why Do Europeans Fly Safer? The Politics of Airport Security in Europe and the U.S.," *Terrorism and Political Violence*, Vol. 15, No. 4, Winter 2003, pp. 1-36.
- (8) Robert W. Poole, Jr., "A Risk-Based Airport Security Policy," Policy Study No. 308, Reason Foundation, May 2003. ([www.reason.org/ps308.pdf](http://www.reason.org/ps308.pdf))
- (9) Regulation (EC) No 300/2008 of the European Parliament and of the Council, of 11 March 2008 on Common rules in the Field of Civil Aviation Security (and repealing Regulation (EC) No 2320/2002).
- (10) "Flight Plan: Managing the Risks in Aviation Security," Review of the Canadian Air Transport Security Authority Act, Report of the Advisory Panel, 2006. ([www.tc.gc.ca/tcss/CATSA/toc\\_e.htm](http://www.tc.gc.ca/tcss/CATSA/toc_e.htm))
- (11) David Armstrong and Joseph Pereira, "Nation's Airlines Adopt Aggressive Measures for Passenger Profiling," *Wall Street Journal*, Oct. 23, 2001.
- (12) Robert W. Poole, Jr., "Improving Airport Passenger Screening," Policy Study No. 298, Appendix B, Reason Foundation, September 2002. ([www.reason.org/ps298.pdf](http://www.reason.org/ps298.pdf))
- (13) Steven Brill, *After: How America Confronted the September 12 Era*, Simon & Schuster, 2003.
- (14) "CATSA Act 5-Year Review: CAC Position Paper," Canadian Airports Council, May 2, 2006.
- (15) "Report from the Commission on Financing Aviation Security," European Commission, COM (2009) 30, Feb. 2, 2009.
- (16) "Effectiveness of TSA's Surface Transportation Security Inspector," Department of Homeland Security, Office of Inspector General, OIG-09-24, February 2009.

- (17) Robert W. Poole, Jr., "Airport Security: Time for a New Model," Policy Study No. 340, Policy Study No. 340, Reason Foundation, January 2006. ([www.reason.org/ps340.pdf](http://www.reason.org/ps340.pdf))
- (18) "Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference," Annex 17, Convention on International Civil Aviation, Eighth Edition, April 2006.
- (19) "National Security in Canada: The 2001 Anti-Terrorism Initiative: Air Transportation Security, Maritime Security, and Emergency Preparedness," Auditor General of Canada, April 2005.
- (20) Robert Poole telephone interview with Jim Facette, Canadian Airports Council, October 8, 2008.
- (21) "Airports and Airlines Launch Joint Action to Tackle Aviation Security," Airports Council International Europe and Association of European Airlines, news release, October 10, 2006.
- (22) Homeland Security, Issue 6, August 2007, ([www.homelandsecurityeu.com/currentissue/article.asp?art=271260&issue+219](http://www.homelandsecurityeu.com/currentissue/article.asp?art=271260&issue+219))
- (23) Email to Robert Poole from Vlad Olteanu of ACI Europe, October 28, 2008.
- (24) "Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions," GAO-07-454, Government Accountability Office, August 2007.
- (25) "Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security," GAO-08-904T, Government Accountability Office, June 25, 2008.
- (26) "One-on-One:TSA Administrator Kip Hawley Preps His Final Initiatives," Business Travel News, October 20, 2008.
- (27) Robert Poole telephone interview with former ACI-NA official Charles Chambers, November 6, 2008.
- (28) Michael E. Levine and Richard Golaszewski, "E-ZPass for Aviation," Airport Magazine, November/December 2001.
- (29) Catharine Foster, et al., "Enhancing Aviation Security with the SWIFT System," H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, May 18, 2003.
- (30) Russell Shaver and Michael Kennedy, "The Benefits of Positive Passenger Profiling on Baggage Screening Requirements," DB-411-RC, Rand Corporation, September 2004. ([www.rand.org/pubs/documented\\_briefings/2004/RAND\\_DB411.pdf](http://www.rand.org/pubs/documented_briefings/2004/RAND_DB411.pdf))
- (31) "AAAE and the Transportation Security Clearinghouse," [www.aaae.org/government/150\\_Transportation\\_Security\\_Policy/FactSheet\\_AAAE](http://www.aaae.org/government/150_Transportation_Security_Policy/FactSheet_AAAE), accessed November 10, 2008.
- (32) Robert Poole telephone interview with Carter Morris of the American Association of Airport Executives, November 10, 2008.
- (33) Ann Davis, Joseph Pereira, and William M. Bulkeley, "Security Concerns Bring Focus on Translating Body Language," Wall Street Journal, August 15, 2002.
- (34) Robert W. Poole, Jr., "Can the Air Cargo Security Mandate Be Met?" Airport Policy News, No. 37, July/August 2008.
- (35) Bart Elias, "CRS Report to Congress: Air Cargo Security," Congressional Research Service, updated July 30, 2007.

- (36) Cathleen A. Berrick, "Aviation Security: Transportation Security Administration May Face Resource and Other Challenges in Developing a System to Screen All Cargo Transported on Passenger Aircraft," GAO-08-959T, July 15, 2008.
- (37) Eileen Sullivan, "Officials: EU, US Agree on Air Cargo Screening, Associated Press, October 31, 2008.