Risk Analysis, Vol. 33, No. 5, 2013 DOI: 10.1111/j.1539-6924.2012.01905.x

Terrorism Risks and Cost-Benefit Analysis of Aviation Security

Mark G. Stewart[1,*] and John Mueller[2]

We evaluate, for the U.S. case, the costs and benefits of three security measures designed to reduce the likelihood of a direct replication of the 9/11 terrorist attacks. To do so, we assess risk reduction, losses, and security costs in the context of the full set of security layers. The three measures evaluated are installed physical secondary barriers (IPSB) to restrict access to the hardened cockpit door during door transitions, the Federal Air Marshal Service (FAMS), and the Federal Flight Deck Officer (FFDO) Program. In the process, we examine an alternate policy measure: doubling the budget of the FFDO program to $44 million per year, installing IPSBs in all U.S. aircraft at a cost of $13.5 million per year, and reducing funding for FAMS by 75% to $300 million per year. A break-even cost-benefit analysis then finds the minimum probability of an otherwise successful attack required for the benefit of each security measures to equal its cost. We find that the IPSB is costeffective if the annual attack probability of an otherwise successful attack exceeds 0.5% or one attack every 200 years. The FFDO program is costeffective if the annual attack probability exceeds 2%. On the other hand, more than two otherwise successful attacks per year are required for FAMS to be costeffective. A policy that includes IPSBs, an increased budget for FFDOs, and a reduced budget for FAMS may be a viable policy alternative, potentially saving hundreds of millions of dollars per year with consequences for security that are, at most, negligible.

KEY WORDS: Air marshals; aviation security; cost-benefit analysis; risk analysis; terrorism

1. INTRODUCTION

We seek to evaluate the costs and benefits of those security measures that are designed to prevent commercial passenger airliners from being commandeered by small bands of terrorists, kept under control for some time, and then crashed into specific targets. We will incorporate a general consideration of all airline security measures into our analysis, but we focus in particular on the detection rates, risk reduction, and costeffectiveness of three from the in-flight security list: (1) the Federal Air Marshal Service (FAMS), (2) the Federal Flight Deck Officer (FFDO) Program, which allows pilots and crew members to carry firearms to defend the flight deck, and (3) installed physical secondary barriers (IPSBs), which restrict access to the hardened cockpit door during door transitions. Because the FAMS costs $1.2 billion per year and because its effectiveness is in doubt,[1,2] we consider an alternate policy measure in which the budget of the FFDO Program is doubled to $44 million per year, IPSBs are installed in all U.S. aircraft at a cost of $13.5 million per year, and funding for FAMS is reduced by 75% to $300 million per year.

[1]Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales, 2308, Australia.
[2]Mershon Center for International Security Studies, Ohio State University, Columbus, OH, and Cato Institute, Washington, DC, USA.
*Address correspondence to Mark G. Stewart, Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales, 2308, Australia; mark.stewart@newcastle.edu.au.

The need for risk and cost-benefit assessment for homeland security programs, and those supported by the Department of Homeland Security in particular, has been well made by many in government, industry, and academe.[3,4,5] To do so requires the quantification of threat probabilities, risk reductions, losses, and costs of the security measures. This task is challenging, but it is necessary for any risk assessment, and the quantification of security risks and cost-benefit assessment is increasingly being addressed,[6–17] as are life-cycle and cost-benefit analyses for infrastructure protective measures.[18–23] Much of this work can be categorized as "probabilistic terrorism risk assessment."[24,25]

Stewart and Mueller[1] found that U.S. FAMS fails to be costeffective, but that hardening cockpit doors is very costeffective. However, this study considered cost per life saved as the decision-support criterion and did not include other costs of terrorist attacks such as damage to infrastructure, loss of business, tourism and GDP, and other indirect losses that increase the total cost of the 9/11 attacks to up to $200 billion.[26,27] More recently, Stewart and Mueller[28] conducted a systems reliability analysis and more detailed cost-benefit assessment of advanced imaging technologies (AIT)—full-body scanners to inspect a passenger's body for concealed weapons, explosives, and other prohibited items. Because there is uncertainty and variability of parameters, three alternate probability models were used to characterize risk reduction and losses. MonteCarlo simulation methods were used to propagate these uncertainties in the calculation of benefits, and the minimum attack probability necessary for AITs to be costeffective was calculated. It was found that the attack probability needs to exceed 1.6 to 3.3 attacks per year to be 90% certain that AITs are costeffective.

For many engineering systems, the hazard (or threat) rate is known or predicted "*a priori*," but for terrorism the threat may arise from an intelligent adversary who will adapt to changing circumstances to maximize likelihood of success. Some have thus argued that probabilistic terrorism risk assessment is not well suited to this type of threat.[29,30] Yet many terrorists are neither as intelligent nor as adaptive as one might expect. For example, Kenney[31] interviewed dozens of officials and intelligence agents and analyzed court documents in the Spain and the United Kingdom. He finds that Islamist militants there are operationally unsophisticated, short on know-how, prone to make mistakes, poor at planning, and limited in their capacity to learn. Other studies document the difficulties of network coordination that continually threaten operational unity, trust, cohesion, and the ability to act collectively.[32,33] It is true, of course, that some terrorist attacks are carefully planned. However, many, quite possibly most, terrorist target selection effectively becomes something like a random process.[26] In most cases, target selection may not have been random in their minds but would essentially be so in the minds of people trying specifically to anticipate their next move. Some statistical approaches exist for terrorist threat prediction,[10,11,34] however these rely heavily on expert judgments from security experts, game theory, etc. so the inherent uncertainties can still be high.

A practical approach is a "break-even" cost-benefit analysis that finds the minimum probability of a successful attack required for the benefit of security measures to equal their cost. The threat probability, then, is the output of the cost-benefit analysis, and it is the prerogative of the decisionmaker, based on expert advice about the anticipated threat probability, to decide whether or not a security measure is costeffective. If the threat probability is known with confidence, then the "break-even" approach can be recast another way by calculating the minimum risk reduction required for a security measure to be costeffective. Although this approach is not without challenges,[35] break-even cost-benefit analyses are increasingly being used for homeland security applications.[19,20] Hence, we will undertake a break-even cost-benefit analysis in this article. Although the framework for cost-benefit applications to homeland security has been well described,[35,36,37] there are few quantitative studies of risk reductions for security measures currently in place in the United States and elsewhere. The novel aspect of this article is its attempt to quantify the risk reduction of each of the TSA layers of aviation security, and then to assess whether FAMS, FFDOs, and IPSBs reduce risk enough to justify their costs.

This article focuses on aviation security in the United States. However, Australia, the United Kingdom, Canada, and many other countries have similar cost and effectiveness issues. Hence, the article may have wider application.

2. RISK AND COST-BENEFIT METHODOLOGY

An appropriate decision analysis compares the marginal costs of security measures with the marginal

benefits in terms of fatalities and damages averted. The decision problem is to maximize the net benefit (benefits minus the costs), or the net present value:

$$\textit{Net Benefit} = p_{\text{attack}} \times C_{\text{loss}} \times \Delta R - C_{\text{security}} \quad (1)$$

where

(1) p_{attack}: The *probability of a successful attack* is the likelihood that a successful terrorist attack will take place if the security measure were not in place.
(2) C_{loss}: The *losses sustained in the successful attack* include the fatalities and other damage—both direct and indirect—that will accrue as a result of a successful terrorist attack.
(3) ΔR: The *reduction in risk* is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack.
(4) C_{security}: The *costs* are those of providing the risk-reducing security measure required to attain the benefit.

A security measure is viewed as costeffective or efficient if the net benefit exceeds zero.[38] There are many risk acceptance criteria and these depend on the type of risk being quantified (life safety, economic, environmental, social), the preferences of the interested parties and the decisionmaker, and the quality of the information available. Risk acceptance criteria based on annual fatality risk or failure probability may also be used.[22,23]

Terrorism is a frightening threat that affects our willingness to accept risk, a willingness that is influenced by psychological, social, cultural, and institutional processes. Moreover, events involving high consequences can cause losses to an individual that they cannot bear, such as bankruptcy or the loss of life. On the other hand, governments, large corporations, and other self-insured institutions can absorb such losses more readily and so governments and their regulatory agencies normally apply a risk-neutral approach in their decision making.[39,40] Thus the U.S. Office of Management and Budget requires cost-benefit analyses to use expected values (an unbiased estimate) and, where possible, probability distributions of benefits, costs, and net benefits.[41] However, Equation (1) can be generalized for expected utility incorporating risk aversion,[42] as well as for differing time periods and discounting of future costs. The issue of risk aversion is an important one as this seems to dominate counterterrorism and other decisions,[43] but it also arises from uncertainties about the effectiveness of counterterrorism measures as well those about threats.

3. THE "LAYERS OF SECURITY" APPROACH

To "strengthen security through a layered approach," the TSA has arrayed "21 Layers of Security" designed to provide defense-in-depth protection of the traveling public and of the U.S. transportation system.[44]

Of these 21 layers, 15 concern preboarding security—deterrence and apprehension of terrorists before boarding aircraft:

(1) Intelligence
(2) International partnerships
(3) Customs and border protection
(4) Joint terrorism task force
(5) No-fly list and passenger prescreening
(6) Crew vetting
(7) Visible Intermodal Protection Response Teams
(8) Canines
(9) Behavioral detection officers
(10) Travel document checker
(11) Checkpoint/transportation security officers (TSOs)
(12) Checked baggage
(13) Transportation security inspectors
(14) Random employee screening
(15) Bomb appraisal officers

The remaining six layers of security provide in-flight security:

(16) Passenger resistance
(17) Trained flight crew
(18) Hardened cockpit doors
(19) FAMS
(20) Law enforcement officers
(21) FFDOs

We are concerned with the costs and benefits of measures that seek to prevent duplications of 9/11 in which commercial passenger airlines are commandeered, kept under control for some time, and then crashed into specific targets. We do not include all "layers" of TSA security, such as checked baggage or canines, only those likely to stop a 9/11 type attack, and focus on those aviation security measures designed to foil, deter, or disrupt such a terrorist attempt in three steps:

(1) Success in boarding the aircraft undetected—11 of the 15 preboarding layers of security apply: intelligence, international partnerships, customs and border protection, joint terrorism task force, no-fly list and passenger prescreening, crew vetting, behavioral detection officers, travel document checker, checkpoint/TSOs, transportation security inspectors, and random employee screening.
(2) Success in hijacking the aircraft—passenger resistance, trained flight crew, air marshals, and onboard law enforcement officers.
(3) Success in entering the cockpit, commandeering the aircraft, and crashing it into a designated target—hardened cockpit door and armed flight crew (FFDO) as well as one additional layer that is not currently on TSA's list: IPSBs.

Of particular consideration is an examination of the possibility that a team of hijackers could seize control of the flight deck by forcing its way in during those brief and fleeting moments when the door is opened during flight. An important study by RTCA finds that such an undertaking could conceivably be accomplished in a matter of seconds.[45]

It should be noted that there are other potential "layers of security" that might be added to this consideration. One concerns the poor tradecraft of terrorists, particularly in complicated plots.[31–33] Since 9/11 no terrorist in the United States has been able successfully to detonate even a simple bomb and, except for the London bombings of 2005, neither has any in the United Kingdom.[46] Moreover, enhanced awareness by police and intelligence services constrains the opportunities for terrorists to acquire weapons or practice their tradecraft, and this contributes to many failures. In addition, a number of antiaircraft defensive measures have been put into place since 9/11. If a pilot were able to transmit to air controllers that the plane was under a violent hijacking attempt (or passengers used their cell phones to warn authorities), antiaircraft measures might immediately be scrambled to shoot down or ground the captured airliner before it could reach an intended target.

We begin assessing risk reduction by developing a simple systems model of existing aviation security measures. Fig. 1 shows a reliability block diagram used to represent the system of foiling, deterring, or disrupting a terrorist hijacking on a commercial airplane. If a terrorist attack is foiled by any one of these layers of security, then this is viewed as a series system in which each event probability is statistically independent such that the probability that a terrorist hijacking plot will be foiled, disrupted, or deterred is:

$$\Pr(\text{hijackingfoiled}) = 1 - \left\{ \begin{array}{l} \prod_{i=1}^{N} 1 - \Pr(\text{foiled by preboarding security measure i}) \\ \times [1 - \Pr(\text{foiled by passenger resistance})] \\ \times [1 - \Pr(\text{foiled by flight crew})] \\ \times [1 - \Pr(\text{foiled by hardened cockpit door})] \\ \times [1 - \Pr(\text{foiled by IPSB})] \\ \times [1 - \Pr(\text{foiled by FAMS})] \\ \times [1 - \Pr(\text{foiled by law enforcement officer})] \\ \times [1 - \Pr(\text{foiled by FFDO})] \end{array} \right\}, \quad (2)$$

where N is the number of preboarding security measures ($N = 11$).

The assumption of statistical independence may not always hold for Equations (1) and (2). For example, the enhanced ability of new screening technology might reduce the opportunity for terrorists to bring firearms onto an aircraft, increasing the chances that FAMS can apprehend the terrorists. Moreover, security measures may not be perfectly substitutional. For example, removing one layer of security may alter the systems model and/or detection rates of other layers of security. However, our systems model provides a starting point for this type of risk analysis and helps to begin to flesh out some other concerns, including the data requirements that become more challenging as the systems model increases in detail and complexity. It should also be noted that Equation (2) is based on a single threat scenario, whereas in reality security measures are often designed to deal with a range of threat scenarios where each layer complements the other by providing redundancy, filling known gaps, or providing flexibility for dealing with evolving threats. There are also multiple "risks" to be assessed. In addition to an aircraft crashing into a target, it might be important to assess risk reductions for an aircraft missing the target, being intercepted and shot down by fighter aircraft, or brought down by ground-based antiaircraft measures. A more detailed and comprehensive study is required to fully model the complex interactions and interdependencies in aviation security.

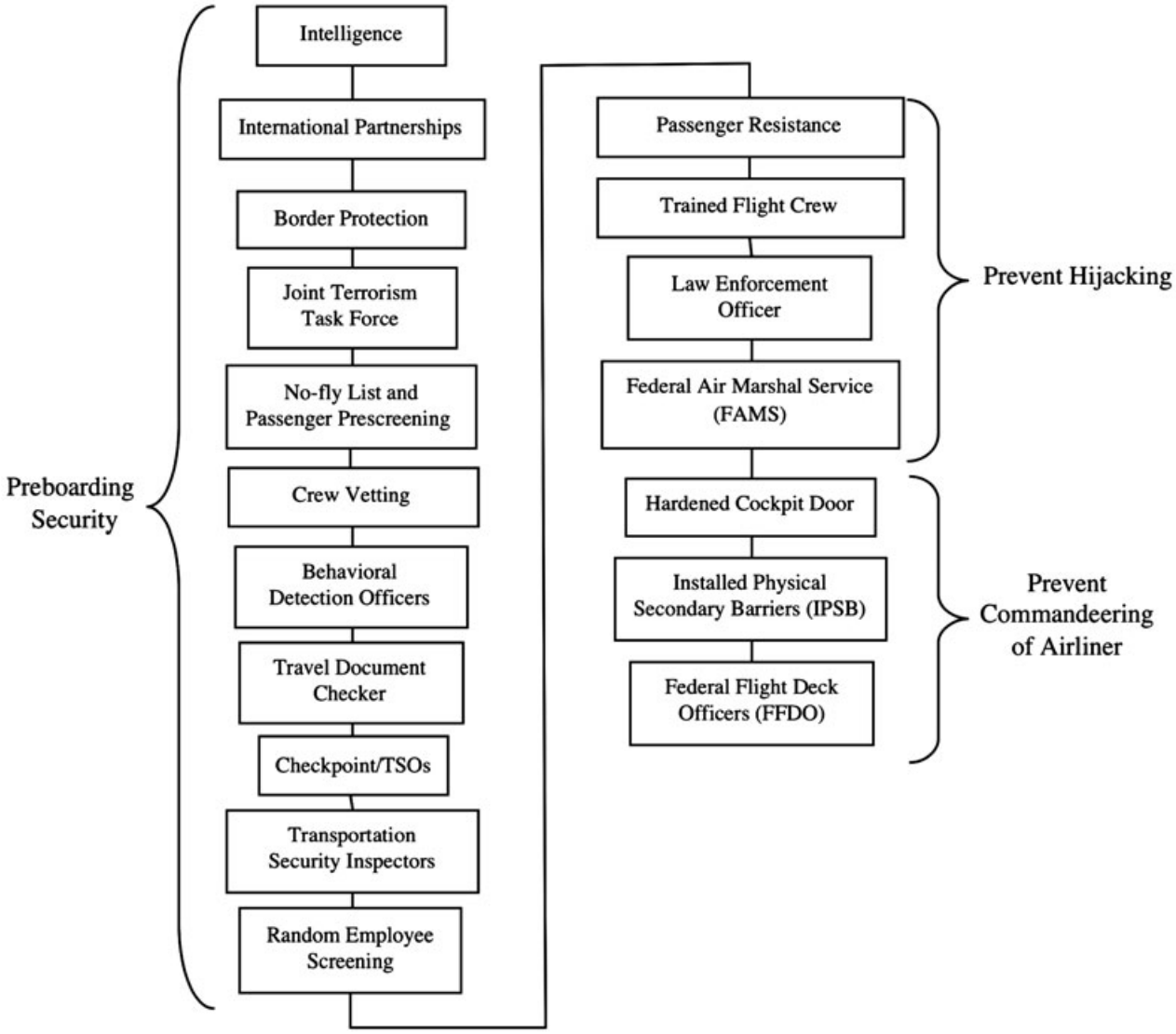

Fig. 1. Reliability block diagram for aviation security measures.

4. COST-BENEFIT ASSESSMENT OF AVIATION SECURITY

4.1. Costs and Characteristics of the In-Flight Security Measures

4.1.1. Passenger Resistance

One reason for the extent of the losses of 9/11 was the reluctance of crew and passengers to confront and resist the hijackers. The 9/11 suicide attacks on the World Trade Center and Pentagon radically changed this perception. As demonstrated on the fourth plane, where passengers had news of what had happened on the first three, passengers and crew will now fight back, particularly if there is any indication that the terrorists' intent is to enter the cockpit.[47] Indeed, Thomas Kean, chair of the 9/11 Commission, believes that the "best defense is always still going to be the flying public." Beyond hijacking, passenger and crew reactions have also been effective in averting efforts to set off bombs in airliners as in the cases of the shoe bomber of 2001 and the underwear bomber of 2009.

Yet, the issue may not be quite so clear-cut. As noted, the RTCA study finds the time required for hijackers to take over the flight deck during a door

transition could conceivably be a matter of seconds. They do assume the hijackers to be "a team of highly trained, armed, athletic individuals," qualities not in great supply among extant terrorists it seems. However, under those circumstances, passengers would scarcely have time to assess the situation, realize the dire threat, communicate with other passengers, and process other information needed for them to summon the courage to fight back. The RTCA report concludes that, under that scenario, "passengers are not considered a predictably reliable option for preventing an attempted violent or sudden breach of the flight deck" and so it completely excludes "the possibility of passenger intervention as a mitigating measure" from its consideration.[45]

4.1.2 Trained Flight Crew

The training of flight attendants includes no instructions in the use of force. The TSA Crew Member Self Defense Training Program does provide one day of training at a cost of $3 million per year.[48] However, reportedly less than 1% of flight attendants have taken the course.[49] Nonetheless, many airlines have instituted procedures during door transition (such as galley trolleys to block access to the flight deck)—these are referred to as "human secondary barriers."[47] Test trials, using highly trained attackers and defenders, found that using blocking crew members without additional equipment (such as IPSB) did "not produce satisfactory results."[45] The flight deck is clearly vulnerable to flight deck intrusions during door transitions because of lack of training and to the very short reaction times required to defeat a team of armed, highly trained, and athletic attackers who manage to be in easy reach of the cockpit door when it happens to be opened.

4.1.3. Hardened Cockpit Doors

The FAA required domestic and foreign airlines serving the United States to install hardened cockpit doors by 2003 to protect cockpits from intrusion and small-arms fire or fragmentation devices. The purchase and installation cost of each hardened cockpit door is typically $30,000–$50,000, and the total cost to airlines is estimated to be $300–$500 million over a 10-year period, including the cost of increased fuel consumption because of the heavier doors.[50] Although the effectiveness of these doors in restricting cockpit access to a determined hijacker has sometimes been questioned,[51] there is little doubt that they will deter and delay hijackers attempting to enter the cockpit.

Hardened cockpit doors may be useful in preventing a 9/11-type attack, but of course, they contribute little to the prevention or mitigation of other kinds of terrorist acts on airplanes such as detonation of explosives. Also, if attackers are somehow able to get into the flight deck during a door transition, the doors become a security device that could protect the attackers.

4.1.4. Installed Physical Secondary Barriers

Although some airlines have instituted procedures during door transition (such as galley trolleys to block access to the flight deck), these are not foolproof, leading the Airline Pilots Association (ALPA) to conclude that "the reinforced flight deck door does not provide a complete solution for securing the flight deck."[52] On many flights, the flight deck door cannot remain closed for the entire duration of the flight, as access is required for rest periods, toilet breaks, and meals. During the time of opening and closing ("door transition"), the protective benefits of a hardened cockpit door to protect the flight deck area is, as noted, reduced at least against armed, highly trained, and athletic hijackers.[45]

A secondary barrier to the cockpit could deal with this concern, further enhancing security. This is "a lightweight device, easy to deploy and stow, that is installed between the passenger cabin and the cockpit door that blocks access to the flight deck whenever the reinforced door is opened in flight"[52,53]—see Fig. 2. The barrier is normally stowed when the cockpit door is closed and locked. In 2004, United Airlines installed on its entire fleet of 500 passenger aircraft IPSBs that crew members must deploy before opening the flight deck door.[52,54] In addition, Boeing and Airbus have designed IPSBs as options on certain models of their next generation aircraft.[55] Further security is provided by the fact that a cabin crew member is generally required to be at the scene when the secondary barrier is put into place, something that adds another complication for would-be hijackers—and at little or no cost.

The cost of an IPSB for a single aircraft is approximately $30,000 in 2011 dollars,[53,54] but some suggest the cost can be as low as $10,000 each.[53] Because there are approximately 6,000 commercial aircraft in the United States, this equates to $180 million. If we round this up to $200 million, and annualize this cost over the 20-year design life of an aircraft

Fig. 2. Fully deployed installed physical secondary barrier.[52]

with a 3% discount rate, this equates to a present value cost of $13.5 million per year.

4.1.5. FAMS and Law Enforcement Officers

There are now some 2,500 to 4,000 air marshals in the United States, up from 33 before 9/11.[2,56] The FY2011 budget for the FAMS is $950 million.[57] In addition, airlines are expected to provide free seats to air marshals (including off-duty air marshals on their way home after completion of their duties). These seats are generally in first class to allow observation of the cockpit door, and FAMS often gives short notice of the need for them.[53] In 2005, the Air Transport Association estimated that this costs airlines $220 million per year in lost revenue,[58] which adjusted for inflation is $250 million in 2011 dollars. Airlines may well have overstated their costs, but there is an opportunity cost in bumping premium (first and business class) passengers to another flight, or to coach. And there is also a customer-loyalty opportunity loss because they can bump fewer of their prime customers up to first class when there are fewer empty seats there. A best estimate of the annual cost to government and airlines for the FAMS, then, is $1.2 billion.

It has been estimated that air marshals fly on less than 5% of flights in the United States.[2,53,59,60] However, Thomas Quinn, former director of the FAMS, has dismissed such reports and, while declining to give specifics, insists his agents cover "more than 5%" of the 28,000 daily commercial flights in the United States.[61] These are often flights designated to be high-risk ones based on intelligence reports.[2,62] Air marshals have made several dozen arrests since 2001, but none of these has been related to terrorism.[56,63]

Additional law enforcement officers may be on some flights for reasons other than countering terrorism, such as escorting prisoners or protecting VIPs. However, their numbers will not significantly boost the percentage of flights that have an armed officer onboard.

The potential presence of air marshals or other law enforcement officers is likely to have something of a deterrent effect,[64] but this is ameliorated somewhat by the low percentage of flights that they can cover. It might even be argued that some crew and passengers may be reluctant to be the first to confront a hijacker if they believe an air marshal is onboard, a hesitation that could conceivably give attempted hijackers the time they need to execute their plans. On the positive side, FAMS may provide more flexibility than many other security measures as they can be deployed at short notice for emerging threats, and this would also apply equally to other law enforcement officers.

The goal of the air marshals is primarily to prevent a replication of 9/11—a reason for putting them in the first class section upfront. Conceivably, they could be helpful in other terrorist situations—for example, if a passenger tried to blow up the airliner—but their added value over crew and passenger resistance is likely to be rather small because they are present on only a rather small percentage of flights and because they are likely to be seated far from

where a potential bomber is located. In addition, in a door-transition attack by highly trained, armed, and athletic attackers that can take place in seconds, it is not at all clear that air marshals could act fast enough to waylay the attempt.

4.1.6. Federal Flight Deck Officers

Flight crews have shown interest in the FFDO Program, which allows pilots and crew members who volunteer for the program to transport and carry firearms to defend the flight deck of an aircraft against acts of criminal violence or air piracy.[2,53] The FFDO Program is managed by the FAMS, and provides the "last line of defense" against a hijacking. It has dramatically increased in size since its inception in 2003.[65] It is estimated that 10% of pilots in the United States were FFDOs in 2008, that this would grow to 16.1%, or to nearly 15,000 pilots, by 2011,[66] and that FFDOs provide five times more coverage than the FAMS.[67] Hence, we assume that if FFDOs are present on the flight deck, they are likely to be as effective as any air marshals who happen to be present on the aircraft. It should also be kept in mind that, with the horrific experience of 9/11 behind them, flight crew personnel are very likely to put up a fight against any cockpit penetration whatever their training or armaments.

The FY2011 budget for the FFDO Program is approximately $22 million. The cost of each federal air marshal is around $3,300 per flight, whereas FFDOs cost approximately $15 per flight.[67] With its modest cost and much greater coverage than the FAMS, Lee Moak, President of the ALPA International, argues that the "FFDO program has been acknowledged by industry and government to be an extremely successful and costeffective layer of aviation security."[65] He goes on to suggest that the "FFDO program is in need of a significant increase in funding," and the Coalition of APLAs recommends doubling the FFDO budget over five years.[38] Seidenstat argues that "[a]rming pilots and training crew members to deal with hijackers appear to serve as substitutes for placing marshals on flights and seem to be effective and far less costly."[2]

4.2. Losses Sustained in a Successful Attack

The loss of an aircraft and the ensuing economic and social disruption costs might be considerable. A RAND study concludes that the downing of an airliner by a shoulder-fired missile could cause a shutdown of U.S. airspace for a week, and losses in the following months would lead to a total economic loss of more than $15 billion assuming a 15% drop in air travel in the six months following the attack.[68]

To establish something of an upper bound for such losses, it may be best to begin with estimates of the costs inflicted by the terrorist attack that has been by far the most destructive in history, that of September 11, 2001. That attack resulted in the deaths of nearly 3,000 people at an associated loss of approximately $20 billion. In addition, 9/11 caused great direct physical damage, amounting to approximately $30 billion in 2010 dollars, including rescue and clean-up costs.[69] The impact on the U.S. economy of the 9/11 attacks ranges from 0.3% to 1% of GDP or $50 to $150 billion in 2010 dollars, adjusting for inflation.[70] An upper bound estimate of the losses of 9/11 might thus approach $200 billion.

However, this is the total cost for four aircraft hijackings, not one. Most of the losses arose from the devastating attacks on the World Trade Center by two separate aircraft, so for a single aircraft we divide this figure by two, generating a loss of $100 billion for a hijacked aircraft that is subsequently flown into a significant building or target. This is a high, upper-bound estimate because it would obviously be difficult for terrorists to again inflict such a huge loss of life and treasure as was accomplished with the attacks on the World Trade Center. Somewhat more plausible, actually, would be an attack like that on the Pentagon on 9/11. In that case, the damage bill came to $700 million, while compensating the families of the 184 victims brings the cost up to $1.2 billion if we use $6.5 million as the value of life.[71] With the additional costs of social and business disruptions, loss of tourism, and the like, the total cost in this case might total $10 billion.

The $10 billion in losses from the 9/11 attack on the Pentagon, or the $15 billion proposed by the RAND study, would be a plausible lower value of economic loss. Moreover, a $100 billion loss, mainly because of loss of GDP, and equivalent to the 9/11 losses from a single aircraft, is a plausible upper bound on losses. A mean of $50 billion is thus reasonable.

4.3. Reduction in Risk Due to the Security Measures

We are interested in the additional risk reduction (ΔR) achieved by the IPSB, FAMS, and/or

FFDOs when compared to the overall risk reductions achieved by all other security measures. This soon becomes a multidimensional decision problem with many possible interactions between security measures, threat scenarios, threat probabilities, risk reduction, and losses. Fault trees and logic diagrams, together with systems engineering and reliability approaches, will aid in assessing these and other complex interactions involving threats, vulnerabilities, and consequences.[72,73] Information about risk reductions can also be inferred from expert opinions, scenario analysis, and statistical analysis of prior performance data, as well as system and reliability modeling. With this in mind, the systems approach to modeling effectiveness of aviation security measures we have described can be instructive, and we will apply it here.

For these purposes, we assume:

(1) The probability that a terrorist is detected by any one of the 11 TSA layers of preboarding security is very low (10%). This is quite conservative. For example, the "checkpoint/security layer" includes passenger and carry-on item screening by metal detectors, X-ray machines, and AIT full-body scanners, and will have high probability of deterring terrorists or detecting weapons concealed on the passenger or in carry-on items for use in a hijacking attempt. Martonosi and Barnet[15] expect this to be approximately 50%, and Fletcher[74] (who was a TSA employee) estimates 75–85%. The extra and more vigilant intelligence, immigration and passport control, and other preboarding security measures implemented since 9/11 should result in a substantial likelihood of detection and apprehension of terrorists. Added to this are the much enhanced policing and investigatory efforts that have caught potential terrorists, including those in the United Kingdom who were planning to blow up U.S.-bound airliners in 2006.[46]

(2) Passengers have a very low chance (5%) of foiling a terrorist attempt to hijack and commandeer an aircraft. As discussed earlier, it could well be argued that the largest deterrent to an attempted hijacking is crew and passenger resistance—particularly when their ability to contact the outside is considered. Thus, one could readily justify (far) more than a 5% chance that passengers would foil or deter an attempted hijacking.

(3) Flight crew has a low (10%) chance of foiling a terrorist attempt to hijack and commandeer an aircraft. There are standard operating procedures in place to minimize the vulnerability of the flight deck during door transitions, but the flight deck is vulnerable to flight deck intrusions during door transition because of lack of training and because of the very short reaction times needed to defeat an attacker.

(4) Onboard law enforcement officers have a negligible 1% chance of foiling a terrorist attempting to hijack an aircraft (because of very low probability such officers will be on a hijacked flight).

(5) Hardened cockpit doors are 75% effective in preventing entry to the cockpit. This is likely to underestimate the actual likelihood, but we select a lower value in recognition that there are scenarios in which the flight deck may be vulnerable during door transitions.

Because there are uncertainties with these probability estimates, sensitivity analyses are conducted to assess the robustness of the results.

The threat scenario considered is a commercial passenger airline being commandeered, kept under control for some time, and then crashed into a specific target. Following our assumptions, the probability that terrorists will be foiled, deterred, or disrupted from boarding an aircraft because of the 11 preboarding security measures is:

$$\begin{aligned}&\Pr(\text{success in preboarding security})\\&\quad = 1-(1-0.1)^{11} = 69\%.\end{aligned} \tag{3}$$

This result is broadly consistent with Martonosi and Barnet,[15] who suggest that preboarding security screening by TSOs has a detection rate of 50%, and with Fletcher,[74] who estimates 75–85% detection rates for X-ray screening and physical bag searches by TSOs, 85% for intelligence databases, 60% for behavior observations, 15% for identity and travel document checks, and 85% for detecting a terrorist before boarding. If we add to this the effect of full body scanners, the estimate of overall risk reduction by preboarding security measures of 69% is plausible, and most likely a lower bound. For example, if the TSO preboarding screening (TSA Layer 11) is increased from 10% to 50%, the Pr(success of preboarding security) = 83%, which is consistent with Fletcher.[74]

The probability of a hijacking being foiled, deterred, or disrupted by the preboarding measures and

by all the in-flight measures except for IPSBs, FFDOs, and FAMS is:

$$\begin{aligned}&\Pr(\text{hijacking foiled})\\&\quad = 1-(1-0.1)^{11}(1-0.05)(1-0.10)\\&\quad (1-0.01)(1-0.75) = 93\%.\end{aligned} \tag{4}$$

This likelihood of foiling a hijacking will be increased, and therefore the potential for risk reduction by the three security measures under examination will be decreased, if any of the 11 TSA layers of preboarding security have detection rates higher than 10%. This is highly likely for passenger and carry-on items screening by metal detectors, X-ray machines, and/or AIT full-body scanners, which have high probability of deterring or detecting weapons concealed on the passenger or in carry-on items. That is, an estimate that in total all security measures besides IPSB, FFDOs, and FAMS reduce the risk of a successful hijacking by 93% is probably quite low.

As noted, the ALPA (International) requests that the "FFDO program is in need of a significant increase in funding," and the Coalition of ALPAs recommends doubling the FFDO budget over five years.[48] A policy mix taking this recommendation into account might involve doubling the budget, and effectiveness, of the FFDO Program, while at the same time reducing funding to FAMS by 75%, leaving roughly 500–1,000 air marshals available for deployment—still easily enough for FAMS to target "high-risk" flights in those instances in which there is a credible threat. Although there are a myriad of possible policy alternatives, we will examine this policy scenario as a plausible illustration.

Accordingly, we calculate risk reductions for these conditions:

(1) IPSB only (no FAMS or FFDO)
(2) FAMS only (no IPSB or FFDO)
(3) FFDO only (no FAMS or IPSB)
(4) IPSB + 25% FAMS + 200% FFDO

4.3.1. IPSB Only (No FAMS or FFDO)

If an IPSB is installed, and if we assume it is equally effective as hardened cockpit doors at preventing a hijacking at 75%, the probability a hijacking will be foiled, deterred, or disrupted with all the security measures in place except for FFDOs and FAMS increases from 93% as seen in Equation (4) to 98%, or by some 5 percentage points.

Because risk reduction is an uncertain variable, it is calculated for the following alternative conditions (see Table I):

(1) IPSB is deemed to be half as effective as assumed above (37.5%).
(2) Passengers and crew are deemed to have zero likelihood of deterring or foiling hijackers.
(3) The detection rate for each of the 11 TSA layers of preboarding security is halved to only 5%.
(4) The detection rate for the preboarding screening by TSOs is increased from 10% to 50%.
(5) Hardened cockpit doors are deemed to be only half as effective as assumed above (37.5%).

The sensitivity analysis for these alternative conditions is included in Table I, and it suggests that the lower and upper bound risk reductions when IPSB and all other security measures are in place except for FAMS and FFDO are 3% and 15%.

4.3.2. FAMS Only (No IPSB or FFDO)

If air marshals are on a flight, we will assume them to be nearly 100% effective in foiling a hijacking—although the RTCA study suggests this could actually be lower. This is conditional on air marshals being on the aircraft, however, whereas the probability of air marshals being on the hijacked flight is only some 5%. Although air marshals are more likely to be on "high-risk" flights based on intelligence reports, experience with the Australian air marshal program suggests that "there is little intelligence indicating which flights are at risk," and air marshals there now only "have random assignments or fly to protect VIPs."[62] Nonetheless, to be conservative we will assume that the probability of air marshals being on a plane is 10% to account for their increased likelihood of being present on higher risk flights. Hence: $\Pr(\text{foiled by FAMS}) = 0.1 \times 100\% = 10\%$. It follows that the probability of a hijacking being foiled, deterred, or disrupted with FAMS and all other security measures in place except for IPSB and FFDO increases about 1 percentage point from 93% to 94%, with our best estimate being an increase of 0.6%.

A lower bound estimate may be based on air marshals being on only 5% of flights, hence $\Delta R = 0.3\%$. If it is believed that air marshals are on "high-risk" flights or have a higher deterrent

Table I. Sensitivity Analysis for Additional Risk Reduction (ΔR)

	Additional Risk Reduction (ΔR)					
Security Measure	Best Estimate	IPSB is Half as Effective (37.5%)	Zero Likelihood of Passengers and Crew Foiling a Hijacking	Detection Rates of 11 TSA Layers of Preboarding Security Reduced to 5%	Detection Rate of Transportation Security Officers Increased to 50%	Hardened Cockpit Door Only Half as Effective (37.5%)
IPSB only (no FAMS or FFDO)	5%	3%	6%	9%	3%	15%
FAMS only (no IPSB or FFDO)	1%	–	1%	1%	0%	2%
FFDO only (no FAMS or IPSB)	2%	–	2%	3%	1%	4%
IPSB + 25% FAMS + 200% FFDOs	6%	5%	7%	11%	3%	15%

Note: Results rounded to nearest percent.

capability, then Pr(foiled by FAMS) may increase to $0.25 \times 100\% = 25\%$, resulting in $\Delta R = 1.7\%$. When combined with the sensitivity analysis in Table I, lower and upper bound risk reductions for FAMS when all other security measures except for IPSB and FFDO are in place are 0% and 2%.

4.3.3. FFDO Only (No FAMS or IPSB)

If FFDOs are in every cockpit, we expect them to be near 100% effective in foiling a hijacking. This is conditional on an FFDO being on the flight deck. Because the probability of air marshals being on a hijacked flight is only near 5%, and because FFDOs provide five times more coverage than the FAMS,[67] we take the probability that FFDOs are on a plane to be 25%. Hence: Pr(foiled by FFDO) $= 0.25 \times 100\% = 25\%$. It follows that the probability of a hijacking being foiled, deterred, or disrupted when FFDOs and all the security measures are in place except for IPSB and FAMS increases by 2 percentage points from about 93% to 95%, with our best estimate being an increase of 1.6%.

A lower-bound estimate may be based on FFDOs being on only 10% of flights, hence $\Delta R = 0.6\%$. When combined with the sensitivity analysis in Table I, lower and upper bound risk reductions are thus 1% and 4%.

4.3.4. IPSB + 25% FAMS + 200% FFDOs

If the budget of the FFDO program is doubled to $44 million per year, the number of FFDOs would also double, leading the probability that FFDOs were on a plane to be 50%. Under that condition, Pr(foiled by FFDO) $= 0.50 \times 100\% = 50\%$. If the funding for FAMS is reduced 75% to $300 million per year, the proportional reduction in Pr(foiled by FAMS) falls from 10% to 2.5%.

The probability that a hijacking will be foiled, deterred, or disrupted under this new scenario increases by 6 percentage points from around 93% to over 99% with our best estimate being an increase of 5.8%. Table I suggests that the lower and upper bound risk reductions are 3% and 15%.

By way of comparison, if the FAMS is not reduced at all, risk reduction increases negligibly—in our best estimate, a meagre 0.1% from 5.8% to 5.9%. This observation alone provides strong evidence that the FAMS is not costeffective: spending $900 million per year on FAMS to reduce risk by 0.1% would seem to be a poor tradeoff.

4.4. Break-Even Sensitivity Analysis

The analysis will apply an expected value cost-benefit analysis using single-point estimates and mean values. In principle, a probabilistic analysis could be attempted, such as that described by Stewart and Mueller,[26,28] for the cost-benefit assessment of AITs where risk reduction and losses were treated as random variables. However, in this case, the information required to accurately assess detection rates for TSA security measures is scarce, so a sensitivity analysis will be conducted using a range of parameter values likely to represent the best and worse cases of risk reduction and losses. Also note that some

Table II. Minimum Annual Attack Probability for IPSB to be CostEffective

Additional Risk Reduction Caused by IPSB (ΔR)	Losses from a Successful Terrorist Attack (C_{loss})			
	$10 billion	$50 billion	$100 billion	$200 billion
3%	4.5%	0.9%	0.5%	0.2%
5%	2.7%	0.5%	0.3%	0.1%
15%	0.9%	0.2%	0.1%	0.1%

Table III. Minimum Annual Attack Probability for FAMS to be CostEffective

Additional Risk Reduction Caused by FAMS (ΔR)	Losses from a Successful Terrorist Attack (C_{loss})			
	$10 billion	$50 billion	$100 billion	$200 billion
0%	–	–	–	–
1%	1,200%	240%[a]	120%	60%
2%	600%	120%	60%	30%

[a]2.4 attacks per year.

Table IV. Minimum Annual Attack Probability for FFDOs to be CostEffective

Additional Risk Reduction Caused by FFDOs (ΔR)	Losses from a Successful Terrorist Attack (C_{loss})			
	$10 billion	$50 billion	$100 billion	$200 billion
1%	22.0%	4.4%	2.2%	1.1%
2%	11.0%	2.2%	1.1%	0.6%
4%	5.5%	1.1%	0.6%	0.3%

results are rounded so as not to imply a precision higher than the precision of input detection rates and costs.

4.4.1. IPSB Only (No FAMS or FFDO)

For the case in which IPSB, but not FAMS or FFDO, is added to the other security measures, the issue under consideration is: What does the yearly probability of an otherwise successful $50 billion attack—where hijackers commandeer an airliner and crash it into a building—have to be to justify spending $13.5 million per year to reduce the total risk of this possibility by 5%? The minimum attack probability for IPSB to be costeffective is thus calculated from Equation (1) to be 0.5% per year. Thus, a mean rate of attack of anything more than one attack every 200 years would pass an expected value cost-benefit analysis. Doubling the cost estimate for IPSB to $27 million would increase the minimum attack probability required for the security measure to be costeffective to 1% per year, or once every century.

The break-even analysis is applied to a range of risk reductions and losses in Table II. It is seen that, for the lowest combination of risk reduction and losses, the attack probability needs to exceed 5% per year for the IPSB to be costeffective, and less than 3% for all other likely combinations of risk reduction and losses. These are relatively low threshold attack probabilities, suggesting that the IPSB is an effective and cost-efficient security measure.

4.4.2. FAMS Only (No IPSB or FFDO)

If the FAMS reduces the risk by 1% at a cost of $1.2 billion per year when it, but not IPSB or FFDO, is added to other security measures, the yearly probability of an otherwise successful $50 billion attack where hijackers commandeer an airliner and crash it into a building has to exceed 240%—or more than two attacks a year—for the security measure to pass a cost-benefit assessment (see Table III). Moreover, more than one attack every two years (or 60% per year) is required to justify the FAMS even when we double the risk reduction and double the losses. Such high attack probabilities are scarcely being observed, strongly suggesting that the FAMS fails a cost-benefit assessment.

4.4.3. FFDO Only (No FAMS or IPSB)

If the FFDO program reduces the risk by 2% at a cost of $22 million per year when it, but not FAMS or IPSB, is added to other security measures, the yearly probability of an otherwise successful $50 billion attack where hijackers commandeer an airliner and crash it into a building has to exceed 2%—or more than one attack every 50 years—for the security measure to pass a cost-benefit assessment (see Table IV). When break-even analysis is applied to a range of risk reductions and losses, it is seen that, for the lowest combination of risk reduction and losses, the attack probability needs to exceed 22% per year—or one every five years—for the FFDO program to be costeffective, and 11% or less for all other likely combinations of risk reduction and losses. These are relatively low threshold attack

Table V. Minimum Annual Attack Probability for a Policy Scenario in Which IPSB is Installed, FAMS is Cut by 75%, and FFDOs are Doubled to be CostEffective

Additional Risk Reduction (ΔR)	Losses from a Successful Terrorist Attack (C_{loss})			
	\$10 billion	\$50 billion	\$100 billion	\$200 billion
3%	120%[a]	24%	12%	6%
6%	60%	12%	6%	3%
15%	24%	5%	2%	1%

[a]1.2 attacks per year

probabilities, suggesting that the FFDO program is an effective and cost-efficient security measure.

4.4.4. IPSB + 25% FAMS + 200% FFDOs

The results above show that, although the FAMS does reduce risk, almost all of that benefit can be obtained with far less expensive measures: the IPSB and FFDOs. Hence, a policy scenario that reduces reliance on FAMS, and increases the role of FFDOs should be explored. A scenario in which the budget of the FFDO Program is doubled and funding for FAMS is cut by 75% reduces the risk by 6% at a cost of \$357.5 million per year. In this case, the yearly probability of an otherwise successful \$50 billion attack where hijackers commandeer an airliner and crash it into a building has to exceed 12%—or once every eight years—for the policy scenario to pass a cost-benefit assessment (see Table V).

Break-even analysis is applied to a range of risk reductions and losses in Table V. The highest minimum attack probability is 120% for the combination of lowest risk reduction and lowest losses. For other combinations of risk reduction and losses, the attack probability needs to exceed one attack every two years to one attack every 100 years for this policy scenario to be costeffective.

4.4.5. Summary of Results

Table VI summarizes the risk reduction, cost, and minimum annual attack probability required for each security measure to be costeffective for losses sustained in an otherwise successful attack of \$50 billion. Note that there is no correlation between effectiveness and levels of investment.

Table VI. Summary of Results

Security Measure	Additional Risk Reduction (ΔR)	Cost (\$ Million)	Minimum Annual Attack Probability for Security Measure(s) to be CostEffective for Losses of \$50 Billion
IPSB only (no FAMS or FFDO)	5%	13.5	0.5%
FAMS only (no IPSB or FFDO)	1%	1,200	240%[a]
FFDO only (no FAMS or IPSB)	2%	22.0	2%
IPSB + 25% FAMS + 200% FFDOs	6%	357.5	12%

[a]2.4 attacks per year.

4.5. Discussion and Future Research

Although we have tried to err on the generous side—toward approving the costeffectiveness of the FAMS, FFDOs, or IPSB—we recognize that the probability estimates for effectiveness of security measures are uncertain and subjective. If the assumed effectiveness of passengers and crew is doubled from 5% and 10%, respectively, to 10% and 20%—still low estimates in the view of some—risk reduction in our best estimate reduces slightly to $\Delta R = 4.2\%$ for IPSB, $\Delta R = 0.6\%$ for FAMS, and $\Delta R = 1.4\%$ for FFDO. These risk reductions are still within the range depicted in Tables II–IV. Moreover, if opportunity costs are considered, this would increase the threshold attack probabilities. The sensitivity analyses also show that changes in detection rates of even 50% will not change the overall conclusions, and that, even if the costs of IPSB and FFDO were 100% higher and the costs of FAMS 50% lower, the overall trends will not change.

It may be argued that many security measures may provide a type of "security theatre" that will make travelers feel safer, an effect that in itself is beneficial. Any security theatre benefits are likely to be small, however, as there is little evidence that FAMS, FFDOs, or IPSB, all of which are substantially invisible to passengers, will by themselves make travelers feel much safer. However, this is an area for further research.

We have sought to explore the utility of systems and reliability modeling for cost-benefit analysis for homeland security expenditure. The results suggest that the threat likelihood needs to be exceedingly

high for FAMS to be costeffective. But we recognize that the preliminary cost-benefit analysis conducted here will not necessarily give a definitive answer to whether FAMS, FFDOs, or IPSB are costeffective. Although the analysis provides a snapshot of risk reductions and costeffectiveness under present conditions, terrorists may adapt their threats in reaction to new security measures, security measures may lose effectiveness with time, evolving threats may lead to the potential for higher losses, etc. However, the competence of terrorists, and the destruction they inflict, do not appear to be on the rise, and 9/11 is increasingly standing out as an aberration, not a harbinger.[75]

Moreover, the assumption of statistical independence may not always hold for Equations (1) and (2), multiple threats and consequences might need to be considered, and security measures may also not be perfectly substitutional. Other decision metrics might also be appropriate, such as expected utility or expected time between attacks. This article provides a starting point for this type of analysis. The assumptions and quantifications made here can be queried, and alternate hypotheses can be tested in a manner that over time will minimize subjectivity and parameter uncertainty inherent in an analysis for which there are little accurate data. This should lead to more widespread understanding and agreement about the relative costeffectiveness of aviation and other counterterrorism security measures.

It should be a key responsibility for any government agency such as TSA to quantify the benefit of billions of dollars it spends each year. Our approach and results highlight a system and reliability approach to aviation security that can help inform decisionmakers about risk reduction and costeffectiveness, and it should help TSA decide on the optimal mix of aviation security measures. Clearly, policy decisions should be made after a more detailed systems model is developed using threat and operational experience from TSA and other security agencies. The next challenge is quantifying detection rates or other performance data because, in general, the higher the fidelity of a systems model, the larger the data requirements. The balance between model complexity and data availability is an important one, and in the security sphere the limitation is often in the latter, not the former. Ultimately, an understanding of interactions between security measures and their risk reduction will help shape future policy decisions with the potential to save hundreds of millions of dollars each year.

5. CONCLUSIONS

We have generally underestimated the likely risk reduction supplied by existing security measures. However, even with these assumptions in place, it appears that the FAMS fails a cost-benefit assessment. Moreover, insofar as FAMS does reduce risk, virtually all of that benefit can be obtained with a less expensive mix of security measures: the installation of physical secondary barriers (IPSBs) to entering the cockpit for those brief and fleeting moments when the cockpit door is opened during flight, and doubling the budget of the FFDO program. This is in agreement with some other studies.[2,76] Thus Seidenstat,[2] who concludes that: "As there are many alternative uses for U.S. security dollars, it would seem that a reallocation of marshals to other security activities might be prudent." Overall, a policy that includes IPSBs, an increased budget for FFDOs, and a reduced budget for FAMS may be a viable policy alternative, potentially saving hundreds of millions of dollars per year with consequences for security that are, at most, negligible.

ACKNOWLEDGMENTS

The first author appreciates the financial support of the Australian Research Council, which supports his Australian Professorial Fellowship. The second author appreciates the financial support of a Distinguished Scholar Award at Ohio State University.

REFERENCES

1. Stewart MG, Mueller J. A risk and cost-benefit assessment of U.S. aviation security measures, Journal of Transportation Security, 2008; 1(3):143–159.
2. Seidenstat P. Federal air marshals: The last line of defense Pp. 149–159 in Seidenstat P and Splane FX (eds). Protecting Airline Passengers in the Age of Terrorism. Santa Barbara: Greenwood Publishing Group, 2009.
3. Friedman BH. Managing fear: The politics of homeland security. Pp. 185–211 in Benjamin HF, Harper J, Christopher A Preble (eds). Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix it. Washington, DC: Cato Institute, 2010.
4. Hahn RW. An Analysis of the 2008 Government Report on the Costs and Benefits of Federal Regulations, Regulatory Analysis 08–04, AEI Center for Regulatory and Market Studies, December 2008, pp. 8–9.
5. Poole RW. Towards Risk-Based Aviation Security Policy, OECD/ITF Round Table on Security, Risk Perception and Cost-Benefit Analysis, International Transport Forum. Discussion Paper No. 2008–23, December 11–12, 2008.

6. Twisdale LA, Sues RH, Lavelle FM. Reliability-based design methods for protective structures. Structural Safety. 1994; 15(1–2):17–33.
7. Low HY, Hao H. Reliability analysis of direct shear and flexural failure modes of RC slabs under explosive loading. Engineering Structure, 2002; 24(2):189–198.
8. Stewart MG, Netherton MD, Rosowsky DV. Terrorism risks and blast damage to built infrastructure. Natural Hazards Review 2006; 7(3):114–122.
9. Stewart MG, Netherton MD. Security risks and probabilistic risk assessment of glazing subject to explosive blast loading. Reliability Engineering and System Safety, 2008; 93(4):627–638.
10. Cox LA. Improving risk-based decision-making for terrorism applications, Risk Analysis, 2009; 29(3): 336–341.
11. Dillon RL, Liebe R, Bestafka T. Risk-based decision making for terrorism applications, Risk Analysis, 2009; 29(3):321–335.
12. Jackson BA, Chan EW, LaTorette T. Assessing the security benefits of a trusted traveler program in the presence of attempted attacker exploitation and compromise, Journal of Transportation Security, 2012; 5(1):1–34.
13. Feng Q. On determining specifications and selections of alternative technologies for airport checked-baggage-security screening, Risk Analysis, 2007; 27(5):1299–1310.
14. Jacobson SH, Karnani T, Kobza JE, Ritchie L. A cost-benefit analysis of alternative device configurations for aviation checked baggage security screening, Risk Analysis, 2006; 26(2):297–310.
15. Martonosi SE, Barnett A. How effective is security screening of airline passengers? Interfaces, 2006; 36(6):545–552.
16. McLay LA, Jacobson SH, Kobza JE. The tradeoff between technology and prescreening intelligence in checked baggage screening for aviation security. Journal of Transportation Security. 2008; 1(2):107–126.
17. Virta JL, Jacobson SH, Kobza JE. Analyzing the cost of screening selectee and non-selectee baggage. Risk Analysis, 2003; 23(5):897–908.
18. Little RG. Cost-effective strategies to address urban terrorism: A risk management approach. Pp. 98–115 in Richardson HW, Gordon P, Moore JE II (eds). The Economic Costs and Consequences of Terrorism. Cheltenham, UK: Edward Elgar Publishing, 2007.
19. Willis H, LaTourette T. Using probabilistic terrorism risk-modeling for regulatory benefit-cost analysis: Application to the western hemisphere travel initiative in the land environment. Risk Analysis, 2008; 28:325–339.
20. von Winterfeldt D, O'Sullivan TM. Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? Decision Analysis, 2006; 3(2):63–75.
21. Stewart MG. Cost-effectiveness of risk mitigation strategies for protection of buildings against terrorist attack. Journal of Performance of Constructed Facilities, ASCE, 2008; 22(2):115–120.
22. Stewart MG. Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure. International Journal of Critical Infrastructure Protection, 2010; 3(1):29–40.
23. Stewart MG. Life safety risks and optimisation of protective measures against terrorist threats to infrastructure. Structure and Infrastructure Engineering, 2011, 7(6):431–440.
24. Ezell BC, Bennett SP, von Winterfeldt D, Sokolowski J, Collins AJ. Probabilistic risk analysis and terrorism risk. Risk Analysis, 2010; 30(4):575–589.
25. Willis HH, LaTourrette T, Kelly TK, Hickey S, Neill S. Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection. Santa Monica, CA: RAND Corporation, 2007.
26. Mueller J, Stewart MG. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security. New York: Oxford University Press, 2011.
27. Mueller J, Stewart MG. The price is not right: The U.S. spends too much money to fight terrorism. Playboy, 2011; 58(10), 149–150.
28. Stewart MG, Mueller J. Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. Journal of Homeland Security and Emergency Management, 2011; 8(1):Art. 30.
29. Cox LA. Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks. Risk Analysis, 2008; 28(6):1749–1761.
30. Brown GG, Cox LA. How probabilistic risk assessment can mislead terrorism risk analysts. Risk Analysis, 2011; 31(2):196–204.
31. Kenney M. "Dumb" yet deadly: Local knowledge and poor tradecraft among islamist militants in Britain and Spain. Studies in Conflict and Terrorism, 2010; 31:1–22.
32. Brooks RA. Muslim "Homegrown" terrorism in the United States: How serious is the threat? International Security, 2011; 36(2):7–47.
33. Eilstrup-Sangiovanni M, Jones C. Assessing the dangers of illicit networks: Why al-Qaida may be less dangerous than many think. International Security, 2008; 33(3):7–44.
34. Pate-Cornell E, Guikema S. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among counter-measures. Military Operations Research, 2002; 7(4):5–23.
35. Farrow S, Shapiro S. The benefit-cost analysis of security focused regulations. Journal of Homeland Security and Emergency Management, 2009; 6(1):Art. 25.
36. Ellig J, Guiora A, McKenzie K. A Framework for Evaluating Counterterrorism Regulations, Policy Resource No. 3, Mercatus Center, George Mason University, September, 2006.
37. Akhtar J, Bjornskau T, Veisten K. Assessing security measures reducing terrorist risk: Inverse ex-post cost-benefit and cost-effectiveness analyses of Norwegian airports and seaports. Journal of Transportation Security, 2010; 3:179–195.
38. OBPR. Best Practice Regulation Handbook, Office of Best Practice Regulation. Canberra: Australian Government, 2010.
39. Sunstein CR. The Cost-Benefit State: The Future of Regulatory Protection. Chicago: ABA Publishing, American Bar Association, 2002.
40. Ellingwood BR. Mitigating risk from abnormal loads and progressive collapse. Journal of Performance of Constructed Facilities, 2006; 20(4):315–323.
41. OMB. Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs (Revised), Circular No. A-94, October 29, 1992, Office of Management and Budget, Washington, DC.
42. Stewart MG, Ellingwood BR, Mueller J. Homeland security: A case study in risk aversion for public decision-making. International Journal of Risk Assessment and Management, 2011; 15(5/6):367–386.
43. Mueller J. Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them. New York: Free Press, 2006.
44. TSA, 2012. Available at: http://www.tsa.gov/what_we_do/layers/index.shtm, Accessed December 10, 2011.
45. RTCA. Aircraft Secondary Barriers and Alternative Flight Deck Security Procedures. Washington, DC: Final Report, Radio Technical Commission for Aeronautics, Special Committee 221, RTCA DO-329, September 28, 2011.
46. Mueller J (ed). Terrorism Since 9/11: The American Cases. Mershon Center, Columbus, OH: Ohio State University, 2011.
47. Schneier B. Beyond Fear: Thinking Sensibly About Security in an Uncertain World. New York: Copernicus, 2006.

48. CAPA. Federal Flight Deck Officer (FFDO) Program. Washington, DC: Coalition of Airline Pilots Associations, 2011.
49. Wilber DQ. Defense training goes begging for airline crews. *Washington Post*, April 28, 2007.
50. FAA. Airlines Meet FAA's Hardened Cockpit Door Deadline. Washington, DC: Federal Aviation Administration Office of Public Affairs Press Release, 2003.
51. Lott JR. Marshals are good, but armed pilots are better. Wall Street Journal Europe, January 2, 2004.
52. ALPA. Secondary Flight Deck Barriers and Flight Deck Access Procedures: A Call for Action, ALPA White Paper. Washington, DC: Airline Pilots Association International, 2007.
53. Elias B. Airport and Aviation Security: U.S. Policy and Strategy in the Age of Global Terrorism. Boca Raton: CRC Press, 2009.
54. AT. United Airlines installing secondary security barrier for cockpit protection. Aviation Today, September 27, 2004.
55. RTCA. Airplane Secondary Barriers and Alternative Flight Deck Security Procedures, Terms of Reference, Radio Technical Commission for Aeronautics, Special Committee 221, RTCA Paper No. 116–10/PMC-801, Washington, DC, June 10, 2010.
56. Meckler L, Carey S. Sky patrol: U.S. air marshal service navigates turbulent times. Wall Street Journal, February 9, 2007.
57. DHS. Budget-in-Brief Fiscal Year 2011, U.S. Department of Homeland Security, Washington, DC, 2010.
58. Poe T. Department of Homeland Security Appropriations Act, 2006: Amendment No. 10. House of Representatives, May 17, 2005.
59. Hudson A. Air marshals cover only a few flights. Washington Times, August 16, 2004.
60. Griffin D. Sources: Air marshals missing from almost all flights, CNN.com, March 25, 2008.
61. Meeks BN. For air marshals, less equals more. MSNBC, September 15, 2004.
62. Kearney S. Air marshal's role now VIP security. Australian, 9 December, 2005.
63. Griffin D. Four arrests for $800M. CNN.com, February 4, 2010.
64. Kiekintveld C, Jain M, Tsai J, Pita J, Ordonez F, Tambe M. Computing optimal randomized resource allocations for massive security games. Pp. 689–696 in Sichman D, Sierra and Castelfranchi (eds). Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2009), Budapest, Hungary, 2009.
65. Moak L. Letter to House Subcommittee on Transportation Security. President of Airline Pilots Association International, 2011.
66. Frank T. More than 10% of pilots allowed to fly armed. USA Today, April 1, 2008.
67. Flagg MW. Statement of Marcus W. Flagg, President Federal Flight Deck Officers Association before the Committee on Homeland Security and Government Affairs, November 1, 2011.
68. Chow J, Chiesa J, Dreyer P, Eisman M, Karasik TW, Kvitky J, Lingel S, Ochmanek D, Shirley C. Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat. Santa Monica, CA: RAND Corporation, 2005.
69. Bram J, Orr J, Rapaport C. Measuring the effects of the September 11 attack on New York City. FRBNY Economic Policy Review, November, 5–20, 2002.
70. Blomberg SB, Rose AZ. Editor's introduction to the economic impacts of the September 11, 2001, terrorist attacks, peace economics. Peace Science, and Public Policy, 2009; 15(2):1–14.
71. Robinson LA, Hammitt JK, Aldy JE, Krupnick A, Baxter J. Valuing the risk of death from terrorist attacks. Journal of Homeland Security and Emergency Management, 2010; 7(1):Art. 14.
72. Stewart MG, Melchers RE. Probabilistic Risk Assessment of Engineering Systems. London: Chapman & Hall, 1997.
73. Biringer BE, Matalucci RV, O'Connor SL. Security Risk Assessment and Management. New Jersey: Wiley, 2007.
74. Fletcher KC. Aviation Security: Case for Risk-Based Passenger Screening. Master's Thesis, Naval Postgraduate School, Monterey, CA, December 2011.
75. Mueller J, Stewart MG. The terrorism delusion: America's overwrought response to September 11, International Security, 2012; 37(1):81–110.
76. Jackson BA, LaTourrette T, Chan EW, Lundberg R, Morral AR, Frelinger DR. Efficient Aviation Security: Strengthening the Analytic Foundation for Making Air Transportation Security Decisions. Santa Monica, CA: RAND Corporation, 2012.