Journal of Air Transport Management 48 (2015) 13–22

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

Responsible policy analysis in aviation security with an evaluation of PreCheck

Mark G. Stewart [a, *], John Mueller [b]

[a] The University of Newcastle, Australia
[b] Ohio State University and Cato Institute, United States

ARTICLE INFO

Article history:
Available online 14 July 2015

Keywords:
Terrorism
Risk
Aviation security
Cost-benefit analysis
PreCheck
Decision-making
Acceptable risk

ABSTRACT

Officials serving the public are tasked at the most fundamental level to spend funds in a manner that most effectively and efficiently keeps people safe. To do otherwise is irresponsible. In the case of counterterrorism policy-making, it is important, then, to evaluate the degree to which any gains in security afforded by counterterrorism measures are great enough to justify their cost. Risk analysis is an aid to responsible decisionmaking that does exactly that. We deal with four elements central to this approach—the cost per saved life, acceptable risk, cost-benefit analysis, and risk communication—and we discuss the degree to which risk analysis has been applied within the government to evaluate counterterrorism measures. We summarize our findings when this approach is used to assess the cost-effectiveness of airline and airport security measures, and then conclude by applying it to PreCheck, a measure that seems likely to bring considerable efficiencies to the screening process and great benefits to passengers, airports, and airlines while actually enhancing security somewhat.

1. Introduction

Terrorism is a hazard to human life, and it should be dealt with in a manner similar to that applied to other hazards—albeit with an appreciation for the fact that terrorism often evokes extraordinary fear and anxiety. While allowing emotion to overwhelm sensible analysis is both understandable and common among ordinary people however, it is not appropriate for officials charged with—responsible for—keeping them safe. As Sunstein (2006) puts it, "if people's values lead them to show special concern with certain risks, government should take that concern into account." But "any official response should be based on a realistic understanding of the facts," not on "factual mistakes".

Risk analysis is an aid to responsible decision making that has been developed, codified, and applied over the last few decades—or in some respects centuries (Stewart and Melchers, 1997; ISO 31000-2009; Bernstein, 1996). In Section 2 of this paper, we briefly summarize several elements central to this approach. We also assess the degree to which risk analysis has been coherently applied to counterterrorism efforts by the government—particularly by the U.S. government—in making or evaluating decisions that have cost taxpayers over a trillion dollars over the last dozen years. And we evaluate the degree to which responsible counterterrorism requires such an approach.

In Section 3, we summarize our findings when this approach is used to assess the cost-effectiveness of airline and airport security measures. Section 4 summarizes some to the security measures that have been relaxed. And finally in Section 5, we apply cost-effectiveness and risk-analytic approaches to PreCheck, concluding that the measure is likely to bring considerable efficiencies to the screening process and great benefits to passengers, airports, and airlines while actually enhancing security somewhat.

2. Risk analysis and responsible policy-making

We assess four issues central to a risk-analytic approach and apply them to the hazard presented by terrorism: the cost per saved life, acceptable risk, cost-benefit analysis, and risk communication. We then evaluate the degree to which they have been applied by policy-makers and we assess their importance to responsible policy-making. For a fuller explication of the issues in this section, see Mueller and Stewart (2011, 2014). This type of analysis is often referred to as probabilistic terrorism risk assessment (e.g., Willis et al., 2007; Ezell et al., 2010). For a full literature review of

* Corresponding author. Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales, 2308, Australia.
E-mail address: mark.stewart@newcastle.edu.au (M.G. Stewart).

http://dx.doi.org/10.1016/j.jairtraman.2015.06.007
0969-6997/

probabilistic terrorism risk assessment see Stewart and Mueller 2013a). See also Stewart and Mueller 2008, 2013b, 2014a,b.

2.1. Four elements in risk analysis

2.1.1. Cost per life saved

When regulators propose a new rule or regulation to enhance safety, they are routinely required to estimate how much it will cost to save a single life under their proposal, and some general tendencies and limits have been established over time. Thus, Paté-Cornell (1994) suggests that a ceiling of $3.5 million per life saved, inflation adjusted to 2014 dollars, seems roughly appropriate in current practice. In general, regulators and administrators begin to become unwilling to spend more than $1 million to save a life, and they are quite reluctant to spend over $10 million, preferring instead to expend funds on measures that save lives at a lower cost. A study for the U.S. government's Department of Homeland Security suggests that the best estimate of a value of a saved human life for homeland security analysis would be about $7.5 million in 2014 dollars while the value of a human life "more involuntary, uncontrollable, and dread risks" like terrorism might be some $15 million (Robinson et al., 2010).

The United States spends about $100 billion per year on seeking to deter, disrupt, or protect against domestic terrorism (Mueller and Stewart, 2011). If each saved life is valued at $15 million, it would be necessary for the counterterrorism measures to prevent or protect against between 6000 and 7000 terrorism deaths in the country each year, or twice that if the lower figure of $7.5 million for a saved life is applied. The total number of people killed by Islamist extremist terrorists within the United States since 9/11 is 19, or less than two per year, a far cry, of course, from 6000 to 7000 per year. A defender of the spending might argue that the number is that low primarily because of the counterterrorism efforts. Others might find that to be a very considerable and improbable reach, suggesting that, among other things, defenders would need to explain why there were no attacks in the West in the immediate aftermath of 9/11, or in the years that followed before enhanced homeland security measures, and spending, were put in place.

2.1.2. Acceptable risk

Another way to approach the issue is to compare the annual fatality rates caused by terrorism with those caused by other hazards. The central analytic issue here is whether the likelihood of being killed by a hazard is unacceptably high, or whether it is low enough to be acceptable. That is, just how safe is safe enough? Although we often say that there is nothing more important than the value of human life, we regularly and inescapably adopt policies in which human lives are part of the price—allowing the private passenger car to exist, for example.

Practice suggests risks are deemed unacceptable if the annual fatality risk is higher than 1 in 10,000 or perhaps higher than 1 in 100,000. They are deemed acceptable if the annual fatality risk is lower than 1 in 700,000 or perhaps 1 in 1 million or 1 in 2 million (Mueller and Stewart, 2011). Clearly, hazards that fall in the unacceptable range should generally command the most attention and the most resources. Those hazards in the acceptable range would generally be deemed of little or even negligible concern—they are risks we can live with—and further precautions would scarcely be worth pursuing unless they are quite remarkably inexpensive.

Almost all annual terrorism fatality risks from terrorism for the developed world are less than 1 in a million—for the United States, Great Britain, Canada, and Australia, they are less than 1 in 4 million per year (Mueller and Stewart, 2011). Therefore they generally lie within the range deemed by regulators internationally to be safe or acceptable and do not require further regulation (see also Bogen and Jones, 2006; Gardner, 2008). Applying conventional standards, then, terrorism currently presents a threat to human life in the Western world that is, in general, acceptable, and efforts, particularly expensive ones, to further reduce its likelihood or consequences are scarcely justified.

There is, of course, no guarantee that the frequencies of the past will necessarily persist into the future. However, those who wish to discount such arguments and projections need to demonstrate why they think terrorists will suddenly get their act together and inflict massively increased violence, visiting savage discontinuities on the historical data series.

$$\text{Benefit} = \left\{ \begin{array}{c} (\text{probability of a successful attack absent the security measure}) \\ \times \\ (\text{losses sustained in the successful attack}) \\ \times \\ (\text{reduction in risk furnished by the security measure}) \end{array} \right\} \tag{1}$$

2.1.3. Cost-benefit analysis

Cost-benefit analysis brings this all together, and compares the costs of a security measure with its benefits as tallied in lives saved and damages averted. The benefit of a security measure is a multiplicative composite of three considerations: the probability of a successful attack absent the security measure, the losses sustained in a successful attack, and the reduction in risk furnished by the security measure.

These considerations can be usefully wrinkled around in a procedure known as "break-even analysis." In this, we seek to determine what the probability of a successful terrorist attack would have to be for a security measure to begin to justify its cost. Thus, we set the cost of the security measure equal to its benefit, and the break-even analysis gives

$$(\text{probability of a successful attack absent the security measure}) = \frac{(\text{cost of the security measure})}{(\text{losses sustained in the successful attack}) \times (\text{reduction in risk furnished by the security measure})} \tag{2}$$

We have applied this approach to the overall increase in domestic homeland security spending in the United States by the federal government (including for national intelligence) and by state and local governments. That is, we assume homeland security measures in place before the 9/11 attacks continue, and we evaluate the cost-effectiveness of the additional funds that have been allocated to homeland security - some $75 billion per year. We find that, in order for added homeland security expenditures to be deemed cost-effective under our approach—which substantially biases the consideration toward finding them effective—there would have to be 333 successful $500 million attacks something like the Boston bombing in 2013 - nearly one attack per day - without any security measures in place (for a fuller discussion, see Mueller and Stewart, 2011). If the added measures managed to deter, disrupt, or protect against about half of these (three per week), they would begin to become cost-effective.

However, there may be specific measures that are cost-effective. While the protection of a standard office-type building would be cost-effective only if the likelihood of a sizable terrorist attack on the building is a thousand times greater than it is at present (Stewart, 2008), the hardening of cockpit doors on aircraft appears to be cost-effective. However, the provision for air marshals on the planes decidedly is not, and the cost-effectiveness of full-body scanners is questionable at best. We discuss our findings on airline and airport security measures more fully below.

2.1.4. Risk communication

The U.S. Office of Management and Budget requires that governments expending tax money in a responsible manner need to be neutral when assessing risks, something that entails focusing primarily on mean estimates in risk and cost-benefit calculations, not primarily on worst-case or pessimistic ones (e.g., OMB, 1992).

The willingness to accept risk, however, is influenced not only by its objective likelihood but by a variety of psychological, social, cultural, and institutional processes (e.g. Slovic et al., 1980). It is important, then, for officials to communicate risk objectively. If they can convince their constituents to adopt a risk-neutral perspective, they will be in a far better position to expend pubic funds in ways that most enhance public safety. However, just about the *only* official in the United States who has ever openly put the threat presented by terrorism in some sort of context is New York's Mayor Michael Bloomberg who in 2007 pointed out that people should "get a life" and that they have a greater chance of being hit by lightning than of being struck by terrorism (Chan, 2007). It might be noted that this unconventional outburst did not have negative consequences for him. Although he had some difficulties in his reelection two years later, his blunt, and essentially accurate, comments about terrorism were not the cause.

2.2. Application of risk analysis to terrorism by the government

As far as we can see, Department of Homeland Security decision-makers do not follow robust risk assessment methodology of the sort suggested here. This observation is supported by a committee of the U.S. National Academy of Sciences in a 2010 report. After spending the better part of two years investigating the issue, the committee could not find "any DHS risk analysis capabilities and methods" adequate for supporting the decisions made about spending on terrorism, and noted that "little effective attention" was paid to "fundamental" issues. With one exception, it was never shown "any document" that could explain "exactly how the risk analyses are conducted," and it looked over reports in which it was not clear "what problem is being addressed." This situation is particularly strange because, as the committee also notes, the risk models used in the department for *natural* hazards are "near state of the art" and "are based on extensive data, have been validated empirically, and appear well suited to near-term decision needs." (NRC, 2010). Moreover, when it comes to terrorism, DHS appears to be exceptionally risk-averse: its decisions cannot be supported even with the most risk-averse utility functions possible, and its level of risk aversion is exhibited by few, if any, government agencies including the U.S. Nuclear Regulatory Commission and Environmental Protection Agency (Stewart et al., 2011; Stewart and Mueller, 2013b). Much the same appears to hold throughout the world for counterterrorism security measures.

2.3. Responsible counterterrorism policy-making

In seeking to evaluate the effectiveness of the massive increases in homeland security expenditures since September 11, 2001, the common and urgent query has been "are we safer?" This, however, is the wrong question. Of course, we are "safer"—the posting of a single security guard at one building's entrance enhances safety, however microscopically. The correct question is "are the gains in security worth the funds expended?" Or, as it was posed shortly after 9/11 by risk analyst Howard Kunreuther, "How much should we be willing to pay for a small reduction in probabilities that are already extremely low?" (Kunreuther, 2002). Working to answer this absolutely central question involves dealing with considerations of cost per saved life and acceptable risk as fed into cost-benefit methodology.

Looking more broadly, any responsible analysis must also include a consideration of what else could have been done with the effort and money being expended on the policy proposed (Schneier, 2003). When we spend resources on regulations and procedures that save lives at a high cost, we forgo the opportunity to spend those same resources on measures that can save more lives at the same cost or even at a lower one (Tengs and Graham, 1996).

If diversions of funds would easily save many lives, a government obliged to allocate funds in a manner that best benefits society must explain why it is spending billions of dollars on security measures with very little proven benefit and why that policy is something other than a reckless waste of resources. This disregard of basic cost-benefit considerations not only wastes money but costs lives.

We recognize that risk and cost-benefit considerations should not be the sole criterion for public decision making. Nonetheless, they provide important insights into how security measures may (or may not) perform, their effect on risk reduction, and their cost-effectiveness. They can reveal wasteful expenditures and allow limited funds to be directed where the most benefit can be attained. If risk and cost-benefit advice is to be ignored, the onus is on public officials to explain why this is so and to detail the trade-offs and cuts to other programs that will inevitably ensue.

To be irrational with your own money may be to be foolhardy, to give in to guilty pleasure, or to wallow in caprice. But to be irrational with other people's money, particularly where public safety is concerned, is to be irresponsible. In the end, it becomes a dereliction of duty that cannot be justified by political pressure, bureaucratic constraints, or emotional drives.

If officials are incapable of carrying out their jobs in a manner that provides the most public safety for the money expended, they should frankly admit they are being irresponsible—that they

consider retaining their position to be more important than providing for public safety—or they should refuse to take the job in the first place. People who join the army or become fire-fighters accept the possibility that at some point they may be put in a position in which they are shot at or required to enter a burning building. People who become decision-makers should in equal measure acknowledge that in order to carry out their job properly and responsibly, they may be required on occasion to make some difficult, even career-threatening, decisions.

3. Applications of cost-benefit analysis to airline and airport security measures

In our first published study (Stewart and Mueller, 2008), we assessed various security layers designed to prevent another airliner hijacking. We found that the U.S. Federal Air Marshal Service (FAMS) fails to be cost-effective, but that hardening cockpit doors does prove to be cost-effective. However, this study considered only cost per life saved as the decision-support criterion while the consequences of terrorist attacks also include considerable costly damage to infrastructure, business, tourism, and GDP, as well as other indirect losses. For example, the full cost inflicted by the 9/11 attacks amounted to up to $200 billion (Mueller and Stewart, 2011). In our book, we took into account the full costs of a successful hijacking but the conclusions about the relative value of the security measures designed to prevent or foil such an attack remained the same (Mueller and Stewart, 2011).

We have also conducted a systems reliability analysis and a detailed cost-benefit assessment of Advanced Imaging Technologies (AIT)—full-body scanners that inspect a passenger's body for concealed weapons, explosives, and other prohibited items (Stewart and Mueller, 2011). Since there is uncertainty and variability in the parameters, probability models were used to characterize risk reduction and losses, and Monte-Carlo simulation methods were used to propagate these uncertainties in the calculation of benefits. We find that the minimum attack probability necessary for AITs to be cost-effective needs to exceed 1.6 to 3.3 attacks per year in the United States to be 90% certain that AITs are cost-effective.

We then developed a systems reliability model for aviation security using single point estimates of risk reduction and losses, and a risk-neutral decision analysis (Stewart and Mueller, 2013a). It was found that Installed Physical Secondary Barriers (IPSB) are cost-effective if, without them, there would be one successful attack every 200 years, and that the Federal Flight Deck Officer (FFDO) program is cost-effective if the annual attack probability exceeds 2% or one attack every 50 years. On the other hand, for FAMS to be cost-effective, the successful foiling of more than two otherwise successful attacks every year is required. A policy that includes IPSBs, an increased budget for FFDOs, and a reduced budget for FAMS seems a more viable policy alternative and could save considerable amounts of money (both for the taxpayers and for the airlines) by reducing spending for an expensive program (FAMS) while increasing spending on an inexpensive one (FFDO).

Utility theory can be used to factor risk aversion into the decision process, and in Stewart and Mueller (2013b) we extend earlier work considerably. We include the effect of deterrence in estimating risk reduction, develop conditional probabilities for detection rates because security measures are not perfectly substitutional, characterize detection rates, risk reduction, and losses as probabilistic variables allowing confidence intervals of policy preferences to be calculated, and apply utility theory to quantify levels of risk aversion. FAMS would need to foil 2.6 otherwise successful attacks per year to be 90% sure that the program is cost-effective whereas IPSBs have more than 90% chance of being cost-effective even if they foil an otherwise successful terrorist only once every 16 years. A risk neutral analysis finds a policy option of adding IPSBs but not FAMS to the other measures to be preferred for all attack probabilities. However, a very risk averse decision-maker is 48% likely to prefer to retain the expensive FAMS program even if the attack probability is as low as one percent per year—a very high level of risk aversion that is exhibited by few, if any, other government agencies. Overall, it seems that, even in an analysis that biases the consideration toward the opposite conclusion, far too much may currently be spent on security measures to address the problem of airline hijacking, and there are likely to be spending reductions that could be made with little or no consequent reduction of security.

We have also assessed the risks and cost-effectiveness of Australian Federal Police counterterrorism policing at Australian airports (Stewart and Mueller, 2014a). Such policing is cost-effective if it reduces risk by approximately 25% and if the probability of an otherwise successful attack at any airport in Australia exceeds 5% per year—a rate that is not being observed. However, the co-benefits of airport counterterrorism policing—such as reduction in crime and reassurance to the traveling public—might be considerable, and, if so, would dramatically improve the cost-effectiveness of such policing.

Our most recent research focuses on the risks and cost-effectiveness of measures designed to further protect airport terminals and associated facilities such as car parks from terrorist attack in the U.S., Europe, and the Asia-Pacific area (Stewart and Mueller, 2014b). We find that current fatality risks from terrorist attacks to airports are extremely low, some 100–1000 times lower than risk levels generally held to be acceptable. Adding curbside blast protection and blast-resistant glazing, and increasing the number of skycaps, check-in personnel, and security lines were the most cost-effective protective measures. However, attack probabilities would have to be much higher than currently observed to justify even those protective measures.

There is other research that looks at the risks and efficiencies of aviation security, such as Jackson et al. (2012), Jacobson et al. (2006), Morral et al. (2012), Martonosi and Barnett (2006), Willis and LaTourette (2008), and Poole (2008). Few of these studies, however, take our approach of estimating absolute risk and risk reduction. A key component of assessing absolute risk is including the probability of an attack in the calculations, whereas a relative risk assessment is often conducted conditional on an attack occurring and then ranking risks based on the relative likelihood of threats.

4. Relaxations in airline and airport security measures

A potential dilemma for decision-makers concerns the now-iconic (albeit, as noted, essentially wrong-headed) query, “are we safer?” This formulation seems to preclude any reduction in security measures because any cutback will necessarily be seen to make us less safe, however microscopically. However, despite this problem, there have already actually been some modest relaxations in airline security, ones that seem to have been sensible and to have reduced costs. In addition, they have been essentially accepted by the flying public, have not led to a decline in airline passenger traffic, and have not generated focused cries of alarm from politicians and interested groups. Among them are:

- Passengers in the United States are no longer routinely required to undergo the process of answering questions about whether they packed their luggage themselves and have had their bags with them at all times.

- Beginning in late 2005, passengers in the United States were allowed to take short scissors and knives with them on planes, as these were deemed too insignificant to pose much of a security risk. Australia soon followed suit.
- The ritual of forcing passengers to remain in their seats during the last half hour of flights to Washington's Ronald Reagan National Airport has been eliminated.
- Considerations of permanently closing Washington's Ronald Reagan National Airport, potentially a very costly venture, were abandoned.
- Harassment of automobiles picking up and dropping off passengers appears to have been relaxed.
- Domestic passengers in the United States no longer need to show their identification at the gate.
- The orange alert American airports were put on after an airline bomb plot was rolled up in distant Britain in 2006 was abandoned in 2011 when the color-coded scheme was officially abandoned.
- The number of Federal Air Marshals has presumably been reduced with a hiring freeze that began in 2012 (DHS, 2013).
- Children and people 75 and older are not required to remove shoes or jackets when going through screening.

5. An evaluation of PreCheck

Then there is the recent institution of PreCheck. This program allows expedited screening for a huge portion of passengers—potentially half of them—selected from frequent flier programs and from Global Entry and other trusted traveler programs. These passengers do not need to take off belts, shoes, or jackets, nor do they need to remove liquids and laptops from their carry-on luggage. In addition, they are not required to undergo full-body screening. Even though this program might, in some sense, be seen to make us less safe, it appears to have generated no opposition. Indeed, if it has created any clamor among the public, it has come from those who are anxious to join up.

By end of April 2014, Transportation Security Administration (TSA) Administrator John Pistole testified that 40% of passengers were now eligible for PreCheck (TSA, 2014). This was achieved by including 5-year $85 memberships to non-frequent fliers, by using Behavioral Detection Officers (BDOs) for "managed inclusions" in which people in regular screening lines are invited to join the PreCheck lanes, and by including all members of the military.[1] Poole (2014) reports a further expansion of PreCheck is planned to 50% of passengers. Pistole also testified that each PreCheck lane provides "the capability for doubling hourly throughput" - an impressive efficiency gain. PreCheck seems to be one of the few TSA programs that is risk-based—or at least it is determined by screening passengers on the basis of risk.[2]

In justifying the program, Pistole likes to point out that "Our ability to find the proverbial needle in the haystack is improved every time we are able to reduce the size of the haystack" (Pistole, 2012). The goal of PreCheck is to allow screeners to concentrate their efforts on passengers who are a higher risk by removing part of the haystack.

In principle, this is a worthy initiative. It does not treat all passengers as if each poses an equal threat, and it allows for more efficient and faster screening thus reducing opportunity costs that deter travelers from flying, cause them to miss flights, etc. The key question is, however, how have the risks been affected by PreCheck?

For the Department of Homeland Security, the standard definition of risk is:

$$(\text{Risk}) = (\text{Threat}) \times (\text{Vulnerability}) \times (\text{Consequence}) \tag{3}$$

where

- Threat is the annual probability of a terrorist attempt
- Vulnerability is the probability of loss (that the explosive will be successfully detonated or the gun will fire leading to damage and loss of life) given the attempt
- Consequence is the loss (economic costs, number of people harmed) if the attack is successful in causing damage.

Since there is no particular reason to expend funds to deal with terrorist attempts that are unsuccessful (that is, cause no damage), Equation (3) can be simplified to deal with successful attacks—ones that actually do damage—the approach outlined earlier in this paper:

$$\text{Risk} = \left\{ \begin{array}{c} (\text{probability of a successful attack absent the security measure}) \\ \times \\ (\text{losses sustained in the successful attack}) \end{array} \right\} \tag{4}$$

Or in our notation:

$$\text{Risk} = p_{\text{attack}} \times \text{Loss} \tag{5}$$

We start a risk-based evaluation of the PreCheck program by defining the benefit as

$$\text{Benefit} = p_{\text{attack}} \times \text{Loss} \times (\text{risk reduction generated by PreCheck}) \tag{6}$$

[1] On the face of it, allowing serving military to access PreCheck makes sense. However, it is worth noting that the largest terrorist incident in the United States since 9/11 was the 2009 shooting of over 30 victims at Fort Hood in Texas by an army psychiatrist, Major Nidal Hasan. In addition, the 2013 Washington Navy Yard shooting that killed 12 people was committed by a former full-time U.S. Navy reservist who held a Department of Defence security clearance. Although these are isolated events, it is clear that allowing all serving members of the military to access PreCheck is not a risk-free proposition.

[2] Related developments in the United States are found elsewhere. The International Air Transport Association (IATA) is developing the Checkpoint of the Future (CoF) whose main concepts are: "(1) strengthened security by focusing resources where risk is greatest, (2) supporting this risk-based approach by integrating passenger information into the checkpoint process, and (3) maximizing throughput for the vast majority of travelers who are deemed to be low risk with no compromise on security levels" (IATA, 2011). According to IATA's Global Passenger Survey, queuing time is the most frequent complaint with security. In late 2013 the CoF morphed into "Smart Security"—a collaborative venture between IATA and Airports Council International. The Smart Security concept goes well beyond PreCheck, and will involve redesign of screening lanes to include new and emerging screening technologies (IATA, 2013).

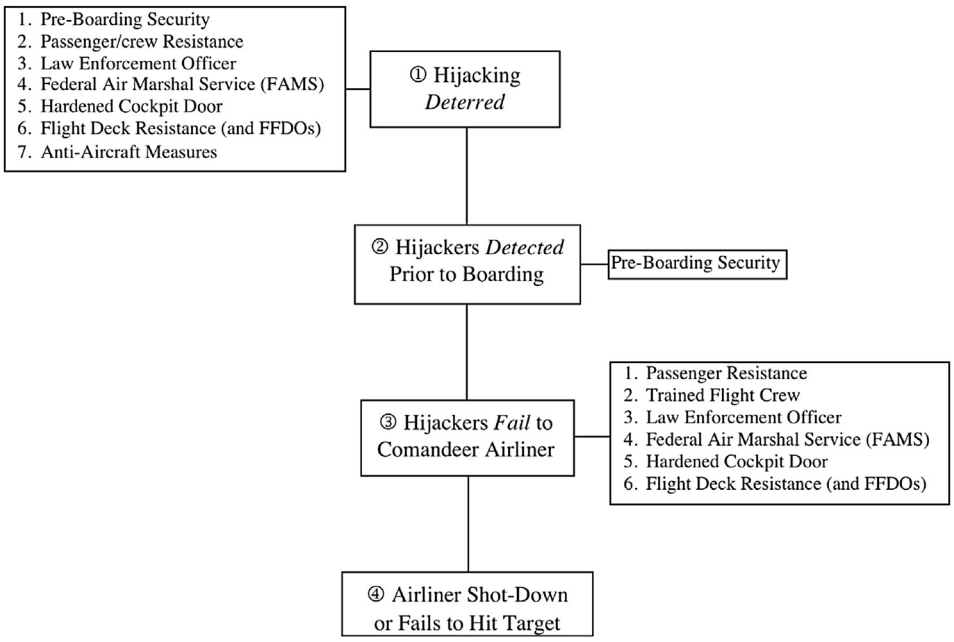

Fig. 1. Reliability block diagram for aviation security measures.

Risk reduction is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack. Like almost all airline security measures, PreCheck reduces risk by lowering the likelihood of a successful attack. It does not reduce the consequences of a successful attack by, for example, making the airliner more crash-proof as protective measures do for buildings or bridges.

The benefit of a security measure may be enhanced by a co-benefit if the security measure not only reduces the terrorism risk but also supplies other benefits such as reducing crime or, particularly important in the case of PreCheck, improving the passenger experience or reducing screening costs. TSA expects nearly 1500 less screeners and screening costs to be reduced by $100 million in FY 2015 due to PreCheck efficiencies at the checkpoint (DHS, 2015).

If the sum of the benefit and the co-benefit of a security measure exceeds the cost of the security measure, the security measure is deemed to be cost effective. We assume PreCheck is essentially free—it reorganizes the screening process without imposing additional costs. The potential problem for PreCheck is not in its costs, but that, due to applying screening measures that are more lax, it might reduce the benefit by increasing the likelihood that a terrorist plot to bring down an airliner would pass through screening undetected.

In our analysis, we consider risk reduction, threat likelihood, and losses for a 9/11 type attack where an airliner is commandeered by terrorists, kept under control for some time, and then crashed into a specific target. Later, we will consider the co-benefit associated with improved passenger experience. We do not consider threats from passenger borne-explosives or from other forms of improvised explosive devices. However, the methodology for estimation of risk reductions and benefits in these scenarios would be similar to that described below.

5.1. Existing benefit of aviation security without PreCheck

Fault trees and logic diagrams, together with systems engineering and reliability approaches, aid in assessing complex interactions involving threats, vulnerabilities and consequences (e.g., Stewart and Melchers, 1997). Applying this approach, Fig. 1 shows a block diagram used to represent the system of four stages of deterring, foiling, or reducing the damage from a terrorist hijacking on a commercial airplane employing existing security measures (Stewart and Mueller, 2013b):

Stage 1: Deterrence. All security measures contribute to this.
Stage 2: Pre-boarding. Relevant security measures include intelligence, customs and border protection, joint terrorism task forces, the no-fly list, passenger prescreening, behavioral detection officers, travel document checkers, checkpoint/transportation security officers, transportation security inspectors, crew vetting, and random employee screening.
Stage 3: In-flight protection. Relevant security measures include passenger resistance, a trained flight crew, law enforcement officers on board, air marshals on board, hardened cockpit door, flight deck resistance (and FFDOs)
Stage 4: Post-takeover: Relevant are anti-aircraft measures that can shoot down a hijacked airliner or force it down before it reaches its target. This is the only airline security measure that seeks to reduce the consequences of a successful hijacking rather than its likelihood, although it does have an affect on deterrence.

Stewart and Mueller (2013b) assessed that the probability that an attempt to hijack an aircraft is deterred or fails to be successful is a measure of total risk reduction which includes the effect of deterrence, pre-boarding measures, measures designed to keep the terrorists from being able to commandeer the aircraft, and anti-aircraft measures. Total risk reduction, combining all four stages, is

$$\begin{aligned} R = 1 - \{&[1 - \Pr(\text{deterred})] \times [1 \\ &- \Pr(\text{detected pre} - \text{boarding})] \times [1 \\ &- \Pr(\text{failed to commandeer aircraft})] \times [1 \\ &- \Pr(\text{anti} - \text{aircraft measures})]\} \end{aligned} \quad (7)$$

where Pr ( ) refers to a probability; thus, the probability of deterrence is: Pr (deterred).

Table 1
Deterrent rates for aviation security measures (stage 1) (adapted from Stewart and Mueller, 2013b).

1. Hijacking Deterred	Deterrence rate	Notes
Pre-boarding	30%	Probably not. Screening technologies are imperfect.
Passengers/crew	30%	Probably not. May not be able to react in time.
Law Enforcement officer	1%	Very low probability of being on a flight.
FAMS	7%	Almost certainly not. FAMS are on a very small proportion of flights. May not react in time.
Hardened cockpit door	30%	Probably not. Flight deck still vulnerable during 'door transitions' for a well planned and coordinated attack.
Flight Deck Resistance	30%	Probably not. Probability of FFDOs being on a plane is 15–20%.
Anti-aircraft measures	30%	Probably not. Particularly when their ability to contact the outside is considered.

Table 2
Disruption rates for aviation security measures (stages 2–4) (adapted from Stewart and Mueller, 2013b).

	Disruption rate	Notes
2. Pre-boarding	50%	Chances about even. Metal detectors, X-ray machines and/or full-body scanners will have high disruption rates. Adaptive terrorists may develop a scheme that bypasses many layers of security.
3. In-flight protection		
Passenger resistance	7%	Almost certainly not.
Flight crew	7%	Almost certainly not. The flight deck is vulnerable during door transition due to lack of training and to the short reaction times needed to defeat an attacker.
Law enforcement officer	1%	Very low probability of being on a flight.
FAMS on flight	20%	FAMS are on no more than 5% of flights, but are placed on 'high risk' flights so assume 20% coverage.
Foiled by door if no FAMS on board	75%	Probable. Flight crew careful about door transitions.
Foiled by door if FAMS on board	85%	Highly probable. FAMS will react quickly enough to detain hijacker, or slow hijacker allowing door to be closed.
Flight deck resistance	15%	If FFDOs are in every cockpit, they are 80–90% effective in foiling a hijacking. The probability of FFDOs being on a plane is 15–20%. Assumes only trained FFDOs will fight for their lives.
4. Anti-aircraft measures	30%	Probably not. Authorities may not be able to deploy anti-aircraft measures in time.

Single-point (mean) estimates were applied to deterrence and disruption rates for the security measures as shown in Tables 1 and 2. The systems reliability analysis based on an expanded version of Eqn. (7) found that existing measures as outlined in Tables 1 and 2 reduce the total risk by R = 99.1% against a 9/11-style hijacking attack (Stewart and Mueller, 2013b). That is, due to existing security measures, a hijacking effort has only about one chance in 100 of being successful. In addition, some might consider some of the deterrence and disruption rates estimated in Tables 1 and 2 to be too low. Thus, Smith (2007) believes that crew and passenger resistance on its own almost guarantees failure for a hijacking attempt. Others may question whether only flight crews trained in the FFDO program will fight for their lives. For further details of the modeling, data requirements, and results see Stewart and Mueller (2013b). Note that Stewart and Mueller (2013b) conducted a Monte-Carlo simulation analysis where deterrence and detection rates were treated as random variables. In this case, mean risk reduction was 98.8%. The present analysis is based on mean values only.

To evaluate PreCheck we will begin by conservatively assuming that 99.99% of passengers have a 99.9% lower than average threat probability than the remaining 0.01% of passengers. In this case, the higher risk passengers in total have an attack likelihood 9990 times higher than the average. Under that assumption,

$$\begin{aligned}\text{Existing Benefit} &= p_{attack} \times \text{Loss} \times (\text{risk reduction furnished by existing security measures}) \\ &= [(99.99\% \times 0.001p_{attack}) + (0.01\% \times 9990p_{attack})] \times \textit{Loss} \times 99.1\% \\ &= 99.1\% \times p_{attack} \times \textit{Loss}\end{aligned} \tag{8}$$

where p_{attack} is the average probability that a terrorist attack would successfully down the airliner if there are no security measures in place at all and that the attack originates at a U.S. airport, and Loss is the consequences of that successful attack. For example, if we expect one successful attack every ten years then p_{attack} is 10%.

We assume in this case that one out of every 10,000 passengers (0.01%) has a threat likelihood 10 million times higher than the remaining 9999 passengers. In other words, 9999 out of every 10,000 passengers have a likelihood of being a terrorist that is close to, but not quite, zero. And only one out of every 10,000 passengers is highly likely to be a terrorist. Since there are 2.2 million enplanements in the United States every day (BTS, 2013), and since no passenger has tried to hijack an airliner in the U.S. since September 11, 2001, this is likely an exaggeration of the threat that terrorist hijacking presents under current conditions.

5.2. Benefit of aviation security with PreCheck

If PreCheck screens 50% of all air travelers, it is important that it correctly selects the passengers with the lower threat likelihood, ($0.001p_{attack}$) to join the PreCheck line. However, PreCheck is unlikely to be 100% fool-proof in only selecting low risk passengers. The worst-case is to assume that passengers are selected at random for which line to go through. We set out to determine whether PreCheck selection procedures prove to be an improvement over random selection in benefit.

The less rigorous screening at PreCheck lanes will reduce the likelihood terrorists and their prohibited items will be detected. In

our earlier study (Stewart and Mueller, 2013b) we conclude, as noted, that existing security measures reduce the risk—the likelihood of, and/or the losses sustained in—a successful hijacking by 99.1%. As part of this, we assume that pre-boarding screening technologies have a 30% chance of deterrence (Table 1) and a 50% chance of detecting or disrupting terrorists (Table 2).

To be conservative, we will now assume that the pre-boarding deterrence and disruption rates are cut in half for the PreCheck lines. According, the rates then become 15% and 25%, respectively. If we use the same systems reliability model as used for assessing existing security measures but cut screening deterrent and disruption rates in half for the 50% of passengers in the PreCheck line, the overall risk reduction is lowered by 0.7% from 99.1% for all existing security measures but without PreCheck to 98.4% when PreCheck is added.

Since the stated TSA aim of PreCheck is to "focus our resources on those passengers who could pose the greatest risk" (Pistole, 2012), we will next assume that pre-boarding deterrent and disruption rates in regular lanes, through which the remaining 50% of the passenger are routed, each increase by 50%. Thus the deterrence rate in regular lanes rises from 30% as in Table 1 to 45%, while the disruption rate rises from 50% as in Table 2 to 75%. This leads to an overall risk reduction of R = 99.6%, increasing risk reduction by 0.5% from those that hold for existing security measures (99.1%).

Under these assumptions the PreCheck program increases risk by 0.7% for the passengers using the PreCheck lanes even as it reduces risk by 0.5% for those undergoing regular screening. If PreCheck screens 50% of all air travelers and passengers are selected randomly, the benefit of the PreCheck program then becomes

$$\begin{aligned}\text{Benefit} &= \text{Benefits of PreCheck lanes} \\ &\quad + \text{Benefits of Regular lanes}\end{aligned}$$

$$\text{Benefit} = \{50\% \times (99.99\% \times 0.001p_{attack} + 0.01\% \times 9990p_{attack}) \times 98.4\% + 50\% \times (99.99\% \times 0.001p_{attack} + 0.01\% \times 9990p_{attack}) \times 99.6\%\} \times Loss = 99.0\% \times (p_{attack} \times Loss) \tag{9}$$

Under these assumptions then, the PreCheck program reduces the overall benefit supplied by the full array of security measures from 99.1% to 99.0%, or a reduction of 0.1%.

The reduced benefit contributed by PreCheck is higher if the portion of passengers going through the PreCheck line increases. For example, if 60% are in PreCheck, there is a reduction in benefit of 0.2%. If 40% of passengers are in PreCheck there is an increase in benefit of only 0.02%. However, if risk reduction in non-PreCheck lanes actually increases a bit more than we have assumed because screeners are able to be more careful, there could be an increase in overall benefit even if more than 50% of passengers go though PreCheck.

The results are robust to changes in parameter values. If the relative threat probability of 'low risk' passengers is zero, the benefit for PreCheck remains at −0.1%. If the portion of 'low risk' passengers increases to 99.9999%–that is, only one passenger in a million is likely to be a terrorist–the benefit of PreCheck remains at −0.1%. If all passengers have the same threat probability, the reduced benefit of PreCheck also remains at 0.1%. Clearly, most realistic combinations of parameter values lead to similar benefits for the PreCheck program.

Finally, if we assume that PreCheck makes no mistakes in selecting its 50% of passengers and only selects passengers with the lower threat likelihood ($0.001p_{attack}$),

$$\text{Benefit} = \{(50\% \times 0.001p_{attack} \times 98.4\%) + [(99.99\% - 50\%) \times 0.001p_{attack} + (0.01\% \times 9990p_{attack})] \times 99.6\%\} \times Loss = 99.6\% \times (p_{attack} \times Loss) \tag{10}$$

Under these assumptions, the PreCheck program results in an overall benefit of 0.5%, significantly better than if the program effectively uses a random process to select passengers for PreCheck screening. This makes sense, as a program than directs highest risk passengers to more rigorous screening will result in effectively the same risk reduction as if all passengers are subject to more rigorous screening, hence a benefit of 99.6%.

It should be pointed out that terrorists constitute a miniscule percentage of airline passengers—for the U.S. with over 800 million enplanements per year, they might constitute one in billions. If that condition is taken fully into account, it would be difficult to come up with any PreCheck selection algorithm that is better than random.

5.3. Additional considerations: acceptable risk, reduced costs, and co-benefits

In our discussion, we have concluded that existing security measures reduce the risk (the consequences and/or the likelihood) of a successful 9/11-like airliner hijacking by 99.1%. That is, under current conditions, we suggest, a terrorist hijacking attempt has one chance in 111 of being successful.

Assuming that pre-boarding security is reduced by a full 50% in PreCheck lines but is improved by 50% in non-PreCheck lines, we conclude that the PreCheck program has little effect on security one way or the other when 40% go through PreCheck, and very slightly reduces security when 50% of passengers are assigned to the PreCheck line.

In this regard, it might be useful to assess another, rather extreme, condition: what is the security situation if current screening methods are abandoned entirely and *all* passengers go through PreCheck? Following our approach, this would mean that overall risk reduction would decline from 99.1% to 98.4%. That is, the terrorists' chances of success would rise from one in 111 to one in 63.

Is that condition acceptable? Several issues should be considered in a full evaluation.

First, the one in 111 estimate of terrorist success, and therefore the one in 63 estimate with PreCheck in place, may be too generous to the terrorists because the impact of several security measures (ones that would not be affected by a change in screening procedures) may have been underestimated in our model. As can be seen in Tables 1 and 2, in coming up with our estimate we assumed that crew and passengers have a quite low likelihood of disrupting a hijacking attempt even though the experience on the fourth plane on 9/11 can be taken to suggest that crew and passengers are now willing to fight, and to fight desperately, to prevent a hijacking. Similarly, we assumed that only 15% of flight crews would successfully fend off a takeover attempt. And we did not include in our considerations a potentially effective security layer that costs nothing at all: incompetence and poor tradecraft of terrorists, particularly in complicated plots (Kenney, 2010; Mueller, 2014; Aaronson, 2013).

Second, our assumption that the pre-boarding security is reduced by 50% in PreCheck lines may well be too severe. As noted above, pre-boarding security includes not only screening, but also several layers of security that are unaffected by changes in passenger screening procedures: intelligence, customs and border protection, joint terrorism task forces, the no-fly list, behavioral detection officers, travel document checkers, checkpoint/transportation security officers, transportation security inspectors, crew vetting, and random employee screening.

Third, PreCheck comes accompanied by a number of co-benefits that have not been included in our considerations. One of these arises from the fact that PreCheck reduces overall screening costs. Already, the TSA budget for FY 2015 proposes that full-time screeners be reduced by nearly 1500 a budget saving of $100 million (DHS, 2015). There may be an additional co-benefit from reducing the unpleasant burden on screeners that comes from requiring them to hassle passengers. This has the potential to improve employee morale and reduce turnover rates. Even today, screeners in PreCheck lines appear to be enjoying their jobs much more than those in the regular lines.

And finally, there is also a very considerable co-benefit attendant on the improvement in the passenger experience that PreCheck provides, a co-benefit that promises to save not only money but lives as well.

To begin with, if more efficient and faster screening reduces the number of travelers who are currently deterred from flying, this is obviously of great financial benefit to airlines. Moreover, all businesses pay special attention to regular customers, and PreCheck is likely to be especially pleasing to the passengers the airlines most treasure: frequent flyers. Adding to this financial co-benefit is the fact that the longer passengers wait to be screened, the more likely they are to be unsatisfied (Gkritza et al., 2006). Holguin-Veras et al. (2012) find that reducing waiting times from 10 to 5 min increased airline market share by 1% for a large airport in the U.S.—or $1.5 billion in additional U.S. airline revenues based on total annual U.S. airline revenues of $150 billion.

Moreover, security delays exact considerable costs to the economy more generally. Treverton et al. (2008) found that delays were 19.5 min in 2004, and that passengers value their time at about $40 per hour (in 2014 dollars). If the PreCheck program reduces waiting times for 25% of passengers by a modest 5 min, there would be savings of $600 million per year in passenger time[3] along with $375 million in increased airline revenues, a total co-benefit that approaches $1 billion per year. In a condition of 100% PreCheck, this would total nearly $4 billion per year.

In addition, some studies suggest there may be hundreds of automobile deaths yearly of people choosing to drive rather than fly short-haul routes (Blalock et al., 2007). If a hundred of these lives were saved each year because PreCheck brought some of the drivers back to the airports, the total gain, or co-benefit, using standard measures of the value of human life as discussed in section 2, would be $750 million.

These matters can be put into fuller perspective. Thus, we can assess the benefit of PreCheck under the 50% condition. Measured in terms of the increase in risk, this is $0.1\% \times p_{attack} \times$ Loss. If we estimate the average loss from a 9/11 type attack upon one airplane to be $50 billion (Stewart and Mueller, 2013b) and if the likelihood of that happening is assumed to be 10% per year (one attack every ten years), the reduced benefit of PreCheck in the 50% condition equates to only $5 million per year. Even if we posit that a 9/11 type threat would occur each year or that the one attack in ten years will cause $500 billion in losses, the yearly reduced benefit increases to $50 million These reduced benefits are small when compared to the co-benefits PreCheck supplies by improving the passenger experience.

The same approach can be used to put the effect of the decline of benefit in the 100% condition into dollar terms. The risk reduction in the 100% PreCheck condition declines by 0.7% (that is, from 99.1% to 98.4%), and if we assume a 9/11-type attack on one airplane per decade, the loss in benefit would equate to $35 million per year. This is about equivalent to the co-benefit that comes from reducing waiting times in security lines by 3 s.

6. Conclusions

Current fatality risks from terrorist attacks in the U.S., Australia, and the U.K. are extremely low, and at levels held to be acceptable. We also found that attack probabilities have to be very high to justify homeland security expenditures. For example, in order for added homeland security expenditures to be deemed cost-effective there would have to be 333 successful attacks something like the Boston bombing in 2013—about one attack per day—without any security measures in place.

We then directed our risk and cost-benefit method to assess the cost-effectiveness of the PreCheck program at airports in the United States. A system reliability model allowed the rate of deterrence and disruption to be inferred for 9/11 type terrorist threats to aircraft for all layers of aviation security. This allowed the checkpoint efficiencies for both the PreCheck and the regular screening lanes to be estimated. It was found that the overall increase in risk reduction of PreCheck is 0.5% when PreCheck correctly identifies low risk passengers, but that there is an overall decrease in risk reduction of 0.1% when PreCheck passengers are selected randomly. However, the co-benefits of PreCheck can significantly outweigh any modest loss of benefit from risk increases as a result of PreCheck. Moreover, we have assumed throughout that one in every 10,000 passengers is highly likely to be a dedicated terrorist when the actual number is likely to be far lower than that.

Acknowledgments

The support of the Australian Research Council is gratefully acknowledged. Professor Mueller appreciates the financial support of a Distinguished Scholar Award at Ohio State University.

References

Aaronson, T., 2013. The Terror Factory. Ig Publishing, Brooklyn, NY.

[3] Based on 815 million enplanements in the United States in 2012, and a waiting time cost of $40 per hour.

Bernstein, P.L., 1996. Against the Gods: the Remarkable Story of Risk. John Wiley & Sons, New York.
Blalock, G., Vrinda, K., Simon, D.H., 2007. The impact of Post- 9/11 airport security measures on the demand for air travel. J. Law Econ. 50 (4), 731–755. November.
Bogen, K.T., Jones, E.D., 2006. Risks of mortality and morbidity from worldwide terrorism: 1968–2004. Risk Anal. 26 (1), 56.
BTS, 2013. Total Passengers on U.S Airlines and Foreign Airlines U.S. Flights Increased 1.3% in 2012 from 2011. Press Release. U.S. Department of Transportation's Bureau of Transportation Statistics (BTS). April 4.
Chan, S., 2007. Buzz Over Mayor's 'Get a Life' Remark. nytimes.com. June 6, 2007.
DHS, 2013. Written Testimony of DHS Management Directorate, U.S. Customs & Border Protection, U.S. Immigration & Customs Enforcement and the Transportation Security Administration for a House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency Hearing, "The Impact of Sequestration on Homeland Security: Scare Tactics or Possible Threat?" April 12, 2013.
DHS, 2015. Budget-in-Brief Fiscal Year 2015. Department of Homeland Security, Washington, DC.
Ezell, B.C., Bennett, S.P., von Winterfeldt, D., Sokolowski, J., Collins, A.J., 2010. Probabilistic risk analysis and terrorism risk. Risk Anal. 30 (4), 575–589.
Gardner, D., 2008. The Science of Fear: Why We Fear the Things We Shouldn't—and Put Ourselves in Greater Danger. Dutton, New York.
Gkritza, K., Niemeier, D., Mannering, F., 2006. Airport security screening and changing passenger satisfaction: an exploratory assessment. J. Air Transp. Manag. 12 (5), 213–219.
Holguin-Veras, J., Xu, N., Bhat, C., 2012. An assessment of the impacts of inspection times on the airline industry's market share after September 11th. J. Air Transp. Manag. 23 (1), 17–24.
IATA, 2011. IATA Reveals Checkpoint of the Future. International Air Transport Association. Press Release No. 35, June 7.
IATA, 2013. Joint Press Release: ACI and IATA Collaborate to Deliver Smart Security, International Air Transport Association. Press Release No. 70, December 12.
ISO 31000–2009, 2009. Risk Management—Principles and Guidelines. International Standards Organization, Geneva, Switzerland.
Jackson, B.A., LaTourrette, T., Chan, E.W., Lundberg, R., Morral, A.R., Frelinger, D.R., 2012. Efficient Aviation Security. RAND Corporation, Santa Monica.
Jacobson, S.H., Karnani, T., Kobza, J.E., Ritchie, L., 2006. A cost-benefit analysis of alternative device configurations for aviation checked baggage security screening. Risk Anal. 26 (2), 297–310.
Kenney, M., 2010. 'Dumb' yet deadly: local knowledge and poor tradecraft among Islamist Militants in Britain and Spain. Stud. Confl. Terror. 31, 1–22.
Kunreuther, H., 2002. Risk analysis and risk management in an uncertain world. Risk Anal. 22 (4), 662–663.
Martonosi, S.E., Barnett, A., 2006. How effective is security screening of airline passengers? Interfaces 36 (6), 545–552.
Morral, A.R., Price, C.C., Oritz, D.S., Wilson, B., LaTourrette, T., Mobley, B.W., McKay, S., Willis, H.H., 2012. Modeling Terrorism Risk to the Air Transportation System. RAND Corporation, Santa Monica.
Mueller, J., 2014. Terrorism Since 9/11: the American Cases. http://politicalscience.osu.edu/faculty/jmueller/since.html.
Mueller, J., Stewart, M.G., 2011. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security. Oxford University Press, New York.
Mueller, J., Stewart, M.G., 2014. Responsible Counterterrorism Policy. Cato Institute Policy Analysis Series, Washington, DC. Number 755, September 10, 2014.
NRC, 2010. Review of the Department of Homeland Security's Approach to Risk Analysis. National Research Council of the National Academies, National Academies Press, Washington, DC.
OMB, 1992. Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs (Revised), Circular No. A-94, Office of Management and Budget, October 29, 1992, Washington, DC.
Paté-Cornell, M.E., 1994. Quantitative safety goals for risk management of industrial facilities,". Struct. Saf. 13, 145–157.
Pistole, J.S., 2012. Counterterrorism, Risk-Based Security and TSA's Vision for the Future of Aviation Security, National Press Club, March 5.
Poole, R.W., 2008. Towards Risk-based Aviation Security Policy. Discussion Paper No. 2008-23. In: OECD/ITF Round Table on Security, Risk Perception and Cost-Benefit Analysis, International Transport Forum, 11-12 December, 2008.
Poole, R.W., 2014. Pistole promises major expansion of PreCheck. Airpt. Policy News. Reason Foundation, Issue No. 101, August-September.
Robinson, L.A., Hammitt, J.K., Aldy, J.E., Krupnick, A., Baxter, J., 2010. Valuing the risk of death from terrorist attacks. J. Homel. Secur. Emerg. Manag. 7 (1).
Schneier, B., 2003. Beyond Fear: Thinking Sensibly about Security in an Uncertain World Copernicus. New York.
Slovic, P., Fischhoff, B., Lichtenstein, S., 1980. Facts and fears: understanding perceived risk. In: Schwing, R.C., Albers, W.A. (Eds.), Societal Risk Assessment: How Safe Is Safe Enough? Plenum, New York, pp. 181–216.
Smith, P., 2007. The Airport Security Follies. December 28. nytimes.com.
Stewart, M.G., 2008. Cost-effectiveness of risk mitigation strategies for protection of buildings against terrorist attack. J. Perform. Constr. Facil. ASCE 22 (2), 115–120.
Stewart, M.G., Melchers, R.E., 1997. Probabilistic Risk Assessment of Engineering Systems. Chapman & Hall, London.
Stewart, M.G., Mueller, J., 2008. A risk and cost-benefit assessment of U.S. aviation security measures. J. Transp. Secur. 1 (3), 143–159.
Stewart, M.G., Ellingwood, B.R., Mueller, J., 2011. Homeland security: a case study in risk aversion for public decision-making. Int. J. Risk Assess. Manag. 15 (5/6), 367–386.
Stewart, M.G., Mueller, J., 2011. Cost-benefit analysis of advanced imaging technology fully body scanners for airline passenger security screening. J. Homel. Secur. Emerg. Manag. 8 (1). Article 30.
Stewart, M.G., Mueller, J., 2013a. Terrorism risks and cost-benefit analysis of aviation security. Risk Anal. 33 (5), 893–908.
Stewart, M.G., Mueller, J., 2013b. Aviation security, risk assessment, and risk aversion for public decisionmaking. J. Policy Analysis Manag. 32 (3), 615–633.
Stewart, M.G., Mueller, J., 2014a. Risk and cost-benefit analysis of police counterterrorism operations at Australian airports. J. Polic. Intell. Count. Terror. 9 (2), 98–116.
Stewart, M.G., Mueller, J., 2014b. Cost-benefit analysis of airport security: are airports too safe? J. Air Transp. Manag. 35 (March), 19–28.
Sunstein, C.R., 2006. Misfearing: a Reply. John M. Olin Program in Law and Economics Working Paper No. 274. University of Chicago Law School.
Tengs, T.O., Graham, J.D., 1996. The opportunity costs of haphazard social investments. In: Hahn, R.W. (Ed.), Life-Saving, Risks, Costs, and Lives Saved: Getting Better Results from Regulation. American Enterprise Institute, Washington, DC, pp. 167–182.
TSA, 2014. Written Testimony of TSA Administrator John Pistole for a Senate Committee on Commerce, Science, and Transportation Hearing Titled "TSA Oversight: Confronting America's Transportation Security Challenges", April 30, 2014.
Treverton, G.F., Adams, J.L., Dertouzous, J., Dutt, A., Everingham, S.F., Larson, E.V., 2008. The costs of responding to the terrorist threats. In: Keefer, P., Loayza, N. (Eds.), Terrorism, Economic Development, and Political Openness. Cambridge University Press, New York.
Willis, H.H., LaTourrette, T., Kelly, T.K., Hickey, S., Neill, S., 2007. Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection. RAND Corporation, Santa Monica, CA.
Willis, H.H., LaTourette, T., 2008. Using probabilistic terrorism risk-modeling for regulatory benefit-cost analysis: application to the western hemisphere travel initiative in the land environment. Risk Anal. 28, 325.