Journal of Transportation Security
https://doi.org/10.1007/s12198-018-0196-y

Risk and economic assessment of U.S. aviation security for passenger-borne bomb attacks

Mark G. Stewart[1] · John Mueller[2,3]

Received: 4 July 2018 / Accepted: 7 August 2018/Published online: 11 August 2018

Abstract

A systems reliability analysis is developed that includes 18 layers of security that might disrupt a terrorist organisation undeterred and intent on downing an airliner with a passenger-borne bomb. Overall, they reduce the risk that such an attack would be successful by 93%. The odds that a lone wolf will be successful in such an attack are considerably lower. This level of risk reduction is very robust: security remains high even when the disruption rates that make it up are varied considerably. The same model is used to explore the risk reduction of aviation security measures in other western countries and in Israel. The benefit-to-cost ratio is then calculated for most of the security measures. It considers the costs and the risk reduction of the layer, the losses from a successful terrorist attack, and the attack probability. It is found that the Joint Terrorism Task Force (JTTF) and police, PreCheck, Visible Intermodal Protection Response (VIPR) teams, and canines pass a cost-benefit assessment. However, it finds that air marshals and behavior detection officers, at a combined cost of nearly $1.3 billion per year, fail to be cost-effective. Accordingly, there are likely to be spending reductions that could be made with little or no consequent reduction in security.

Keywords Aviation security · Terrorism · Risk · Cost-benefit analysis · Transportation security administration · Risk reduction · Airline bombing

✉ Mark G. Stewart
mark.stewart@newcastle.edu.au

John Mueller
bbbb@osu.edu

[1] Centre for Infrastructure Performance and Reliability, The University of Newcastle, Callaghan, New South Wales 2308, Australia

[2] Mershon Center for International Security Studies, Department of Political Science, Ohio State University, 1501 Neil Avenue, Columbus, OH 43201, USA

[3] Cato Institute, 1000 Massachusetts Avenue, NW, Washington, DC 20001, USA

Introduction

Approximately $50 billion - about $10 billion in the United States - is spent annually world-wide in the quest to deter or disrupt terrorist attacks to aviation (Stewart and Mueller 2018). These are significant expenditures that have rarely been subject to systematic cost-benefit or risk analysis. This lack of scrutiny may lead to risk-averse and costly counterterrorism policies. This paper assesses the degree to which security measures currently in place provide safety. In particular, the paper focuses on determining what the likelihood is under current conditions that a terrorist organisation could down an airliner with a passenger-borne bomb or IED - an improvised explosive device. Put another way, how much have existing security measures reduced the risk of this terrorism scenario?

Another aim is to assess the cost-effectiveness of each security measure in an analysis that considers the risk reduction of each layer of security, its cost, losses from a successful terrorist attack, and the probability that there will be a terrorist attack.

Previous research has compared the costs and benefits of some aviation security measures, and recommended where savings can be made without unduly sacrificing risk reduction. Stewart and Mueller (2008) and Mueller and Stewart (2011) have assessed various security layers designed to prevent an airliner hijacking, finding that the $1 billion U.S. Federal Air Marshal Service (FAMS) fails to be cost-effective, but that hardening cockpit doors does prove to be cost-effective. Later studies found that Installed Physical Secondary Barriers (IPSB) and the Federal Flight Deck Officer (FFDO) program were highly cost-effective against hijackings (Stewart and Mueller 2013a). This work was then considerably extended by applying utility theory to quantify levels of risk aversion finding that 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 1% per year—a very high level of risk aversion that is exhibited by few, if any, other government agencies (Stewart and Mueller 2013b; Stewart et al. 2011). A systems reliability analysis and a cost-benefit assessment of Advanced Imaging Technologies (AIT) full-body scanners found the technology to be a questionable expense (Stewart and Mueller 2011). Later studies have also assessed the risks and cost-effectiveness of Transportation Security Administration (TSA) PreCheck, airport policing, measures to protect airport terminals, and the counter-terrorism efforts of the Federal Bureau of Investigation (Mueller and Stewart 2014, 2016a; Stewart and Mueller 2014a, b, 2017).

There is other research that looks at the risks and efficiencies of aviation security.[1] Few of these studies, however, estimate absolute risk and risk reduction. A key component of assessing absolute risk is to include the probability of an attack in the calculations. A relative risk assessment, in contrast, is often conducted conditional on an attack occurring and then ranking risks based on the relative likelihood of threats.

The system reliability model utilised herein is taken from our latest book (Stewart and Mueller 2018). However, this paper extends that work by considering risks from

[1] Jackson and LaTourette (2015), Jackson et al. (2012), Lee and Jacobson (2011), McLay et al. (2010), Sewell et al. (2013), Jacobson et al. (2006), Morral et al. (2012), Martonosi and Barnett (2006), von Winterfeldt and O'Sullivan (2006), Willis and LaTourette (2008), and Poole (2015). For a full review of probabilistic terrorism risk assessment see Stewart and Mueller (2013a).

terrorist IED attacks that are not deterred in the first place. It also integrates TSA PreCheck into checkpoint screening, and considers a decision criteria where the costs of a security measure are "acceptable" or "tolerable" only if the cost is not grossly disproportionate to the risk. This allows for modest risk aversion when there may be considerable doubt about costs and benefits.

We recognise 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 to where the most benefit can be attained.

Costs and benefits as taken as mean values - that is, as single-point or deterministic values. An advantage of this is that the calculations are straightforward. They can also be readily replicated and checked by others. However, this simplified approach ignores the uncertainties and variabilities in the parameter estimates - and uncertainties in the realm of terrorist intentions and predictions are large. Stewart and Mueller (2011, 2013b) have used Monte Carlo simulation methods to propagate vulnerability, risk reduction, and loss uncertainties in the calculation of net benefits. However, results from a probabilistic analysis shows similar trends to those obtained from a deterministic analysis.

Systems reliability analysis

Layers of security

The TSA has arrayed 21 "Layers of Security" to "strengthen security through a layered approach" (see Fig. 1). We exclude five of these layers. One of these, inspection of checked baggage, is irrelevant to the threat considered: that presented by passengers bearing bombs. Two others are crew vetting and random employee screening - though they are discussed a bit in Adaptive behaviour by terrorists section. We also exclude hardened cockpit doors and flight deck resistance enhanced by the FFDO program because these are irrelevant to a passenger-borne IED attack.

The remaining pre-boarding security layers are:

1. Intelligence
2. International partnerships
3. Customs and border protection
4. Joint Terrorism Task Force (JTTF)
5. No-fly list and passenger pre-screening
6. Visible Intermodal Protection Response (VIPR) teams
7. Canines
8. Behavior Detection Officers (BDOs)
9. Travel document checkers
10. Checkpoint screening with Transportation Security Officers (TSOs)
11. Transportation security inspectors
12. Bomb appraisal officers

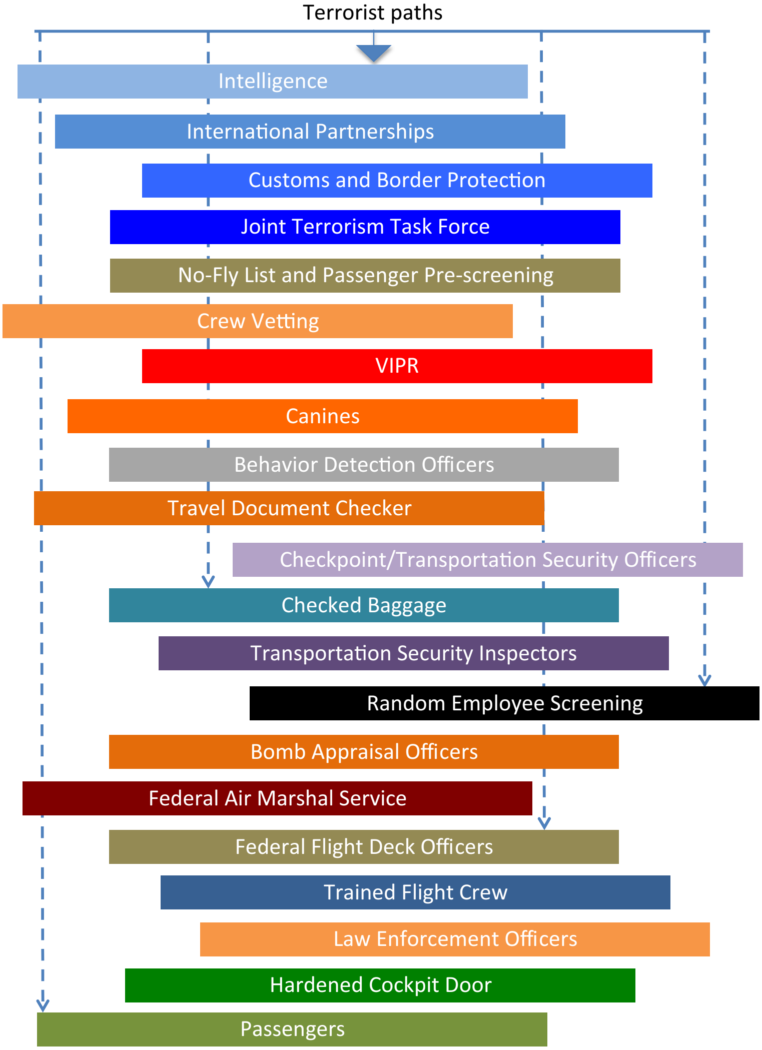
Terrorist paths
Intelligence
International Partnerships
Customs and Border Protection
Joint Terrorism Task Force
No-Fly List and Passenger Pre-screening
Crew Vetting
VIPR
Canines
Behavior Detection Officers
Travel Document Checker
Checkpoint/Transportation Security Officers
Checked Baggage
Transportation Security Inspectors
Random Employee Screening
Bomb Appraisal Officers
Federal Air Marshal Service
Federal Flight Deck Officers
Trained Flight Crew
Law Enforcement Officers
Hardened Cockpit Door
Passengers

Fig. 1 TSA's 21 layers of security. Source: Transportation Security Administration

The remaining in-flight security layers are:

13. Passenger resistance
14. Cabin crew resistance
15. Law enforcement officers on board
16. Federal Air Marshal Service (FAMS)

To this array we add two additional layers that may cause an effort to down an airliner with a passenger-borne bomb to be unsuccessful:

17. IED proves to be defective
18. The aircraft survives even if the bomb is successfully detonated

Assessing and evaluating the layers of security

The analysis is designed to be comprehensive by including all layers that might disrupt a terrorist plot if terrorists are undeterred and intent on downing an airliner with a passenger-borne bomb. Throughout, it is assumed that a bombing attempt is by a terrorist organisation. Terrorists who are undeterred represent a small subset of terrorist plots. Indeed, no terrorist has attempted to bomb an airliner in the U.S. for several decades. Moreover, most terrorist plots are waylaid by the authorities well before the perpetrators even arrive at an airport.

The cost and effectiveness at disrupting a terrorist effort is estimated for each of the 18 layers. Since there is little quantitative data on disruption rates, it is more tractable to assign words of estimative probability such as "probably not" and "chances about even" adapted from Fletcher (2011) as in Table 1, and to translate them into probabilities. Nearly all measures have some chance of being effective at least in extreme cases or in an unlikely combination of circumstances. We designate disruption rates at 1% for those measures deemed to make a negligible contribution to risk reduction. A sensitivity analysis is conducted later to assess changes in risk reduction when these estimates of disruption rates are changed.

The results of this examination are summarised in Table 2. Many of the disruption rates are taken from previous studies (Stewart and Mueller 2011, 2013a, b, 2017). Stewart and Mueller (2017) suggest that TSA PreCheck will reduce disruption rates for low risk passengers by nearly 40%, but increase disruption rates for high risk passengers by close to 30% as PreCheck allows more scrutiny to be placed on screening high risk passengers. In the scenario where 50% of all passengers go through PreCheck, the disruption rate at the checkpoint due to PreCheck increases from 25% before PreCheck to 30% with PreCheck. Table 2 also includes the estimate of the FY2016 costs for each layer where we are able to make them. Costs as inferred from Congress (2015, 2016), DHS (2016) and the Government Accountability Office. For cost details see Stewart and Mueller (2018).

The estimated disruption rates for the pre-boarding layers are mostly modest, with the most effective being the JTTF (policing and tip-offs which have been responsible for many foiled terrorist plots in the U.S. - though mostly outside the aviation area - see Mueller and Stewart 2016a, Mueller 2018), and checkpoint screening. Of the in-flight layers, only passenger resistance rises above the modest level.

Table 1 Words of estimative probability (Fletcher 2011)

Certain	100%
Almost certain	95%
Highly probable	85%
Probable	75%
Chances about even	50%
Less likely than not	40%
Probably not	25%
Highly improbable	15%
Almost certainly not	5%
Impossible	0%

Table 2 Costs and disruption rates for aviation security measures in the United States, for a passenger-borne bombing attack

	Cost ($ millions) FY 2016	Disruption rate
Pre-boarding security		
1. Intelligence	1450	15%
2. International Partnerships	?	5%
3. Customs and Border Protection	?	5%
4. JTTF (including FBI and police)	500	25%
5. No-fly list & passenger pre-screening	180	5%
6. VIPR Teams	50	5%
7. Canines	80	5%
8. Behavior Detection Officers	200	1%
9. Travel document checkers	–	5%
10. Checkpoint/TSOs (including PreCheck)	3500 (includes layer 9)	30%
11. Transportation Security Inspectors	?	1%
12. Bomb Appraisal Officers	?	5%
In flight security		
13. Passenger resistance	0	25%
14. Cabin crew resistance	3	5%
15. Law enforcement officer	0	1%
16. Federal Air Marshal Service (FAMS)	1055	NA
Probability that air marshals are on-board: 20%		
IED detonation prevented by air marshals if air marshals on board		5%
17. IED proves to be defective	–	35%
18. Aircraft survives even if IED detonates	–	50%

NA Not Applicable

?: Not Known

The analysis does not directly include one important impediment to a successful attack: the general incompetence and poor tradecraft of most terrorists, particularly in complicated plots (Kenney 2010; Jenkins 2011; Mueller and Stewart 2012; Aaronson 2013; Mueller and Stewart 2016a; Mueller 2018). Some of this quality is included in the model in layer 17 which deals with defective bombs and bomb-making. Also, at least some of the disruption rates presented in the analysis take terrorist inadequacies into account in that a high rate of disruption implies less than perfect terrorist competence and tradecraft.

Calculation of overall risk reduction

The probability that a passenger-borne bomb attempt will be disrupted is

$$R_{\text{bombing}} = 1 - \left\{ \begin{array}{l} [1-\Pr(\text{disrupted by pre-boarding measures})] \\ \times[1-\Pr(\text{disrupted by in-flight measures})] \\ \times[1-\Pr(\text{IED is defective and does not detonate})] \\ \times[1-\Pr(\text{aircraft survives if IED detonates})] \end{array} \right\} \quad (1)$$

where

$$\Pr\left(\begin{matrix}\text{disrupted by}\\ \text{pre-boarding measures}\end{matrix}\right) = 1 - \left\{\begin{matrix}[1-\Pr(\text{disrupted by intelligence})]\\ \times[1-\Pr(\text{disrupted by international partnerships})]\\ \times[1-\Pr(\text{disrupted by customs and border protection})]\\ \times[1-\Pr(\text{disrupted by JTTF, police, FBI, tip-offs})]\\ \times[1-\Pr(\text{disrupted by no fly list \& passenger pre-screening})]\\ \times[1-\Pr(\text{disrupted by VIPR teams})]\\ \times[1-\Pr(\text{disrupted by canines})]\\ \times[1-\Pr(\text{disrupted by Behavior Detection Officers})]\\ \times[1-\Pr(\text{disrupted by travel document checkers})]\\ \times[1-\Pr(\text{disrupted by checkpoint/TSOs})]\\ \times[1-\Pr(\text{disrupted by transportation security inspectors})]\\ \times[1-\Pr(\text{disrupted by bomb appraisal officers})]\end{matrix}\right\} \tag{2}$$

and

$$\Pr\left(\begin{matrix}\text{disrupted by}\\ \text{in-flight}\\ \text{measures}\end{matrix}\right) = 1\left\{\begin{matrix}[1-\Pr(\text{foiled by passengers})]\\ \times[1-\Pr(\text{foiled by cabin crew})]\\ \times[1-\Pr(\text{foiled by Law Enforcement Officer})]\\ \times[1-\Pr(\text{FAMS on flight})\times\Pr(\text{IED detonation prevented by FAMS})]\end{matrix}\right\} \tag{3}$$

where the term Pr() represents a probability, such that, for example, Pr (disrupted by pre-boarding measures) is the probability that pre-boarding security measures will disrupt, prevent or foil a terrorist attack. The analysis assumes that disruption rates are statistically independent and can be modelled as a series system, assumptions to be discussed more fully in Substitution effects: interactions and interdependencies among the layers section.

Applying the data from Table 2, the probability that a bombing attempt by a well-organised and undeterred terrorist organisation will be disrupted is 93.1%. This suggests that, because of existing security measures, even a well planned and executed terrorist bombing attempt has perhaps at best one chance in ten of being successful. If the rates of deterrence are estimated using a similar procedure and then added in for all layers, overall risk reduction increases to over 98%, while a similar analysis for hijackings reveals an overall risk reduction of over 99% (for more details see Stewart and Mueller 2018).

That the risk is low is borne out by the data - there have been no successful terrorist attacks on US airliners since 2001, and a statistical analysis of the Global Terrorism Database (GTD) shows that the probability that an airline passenger will be killed in a single flight in a terrorist attack world-wide is 1 in 110 million for the years since 2001 (Stewart and Mueller 2018).

Things are even worse for the lone wolf. Although a lone wolf is probably less likely to be detected by intelligence and policing measures, a lone assailant is likely to experience more difficulties in clearing checkpoint security (layer 10) and in making a bomb that is not defective and then successfully detonating it (layer 17). Accordingly, if it is assumed in the model that the rates of disruption for intelligence and policing are cut in half (layers 1 and 4), that the checkpoint disruption rate (layer 10) is increased by half to 45%, and that the odds that an IED will be defective (layer 17) is increased to 80% (as obtained by Grant and Stewart 2012, 2015 for Western countries), the overall risk reduction for a lone wolf bombing attempt increases from 93.1 to 97.9%. That is, the odds that a lone wolf will be successful is about 1 in 50. Note that some results are rounded so as not to imply a precision higher than the precision of input detection rates and costs.

Sensitivity analysis

The results of this model are robust. Table 3 shows that changing the disruption rates in Table 2, often very substantially, alters the overall risk reduction mostly by no more than ±4%. For example, if the likelihood that air marshals are on board is taken to be 5% rather than 20% (which is considerably more realistic), the risk reduction declines only marginally from 93.1 to 93.0%. The rate of IED disruption by air marshals would need to increase six-fold to 30% before there is a noticeable increase in overall risk reduction for that scenario.

If the terrorist arrives at the airport undetected—that is, if disruption rates for layers 1–4 are set to zero - the risk reduction from the remaining security measures at the airport and on board the aircraft remains high at 88.0%.

It should also be kept in mind that many of the disruption rates estimated in Table 2 might be considered low - in our estimates, we have often given the terrorist the benefit of a doubt. For example: although passenger and crew reactions were effective in subduing the shoe bomber of 2001 and the underwear bomber of 2009, the analysis estimates quite low rates of disruption for terrorist attacks: 25% for passengers and 5%

Table 3 Sensitivity analysis of overall risk reductions in the United States

Existing security measures	93.1%
Increase in overall risk reduction:	
Passenger and cabin crew resistance increased by 50%	94.4%
Rate of IED disruption of FAMS increased six-fold to 30%	93.4%
Rate of disruption for checkpoint screening increased by 50%	94.6%
Probability that aircraft survives if IED detonates increased by 50%	96.5%
Passenger and cabin crew resistance disruption rates increased by 100%	95.6%
Rates of disruption for all layers increased by 25%	95.5%
Rates of disruption for all layers increased by 50%	97.3%
Decrease in overall risk reduction:	
Probability of air marshals on flight reduced from 20 to 5%	93.0%
Rate of disruption for checkpoint screening reduced by 50%	91.6%
Rate of disruption by passengers is reduced from 25 to 5%	91.2%
Rate of disruption for checkpoint screening reduced to 5%	90.6%
Rate of disruption for checkpoint screening reduced to 0%	90.1%
Probability that aircraft survives if IED detonates reduced by 50%	89.6%
Rates of disruption for all pre-boarding measures reduced by 50%	85.6%
Only effective pre-boarding security measures are checkpoint screening, intelligence, and the JTTF (including FBI, police)	89.9%
Probability that IED is defective reduced by 50%	91.2%

for crew for bomb attacks. If these rates of disruption are doubled, the overall risk reduction increases to 95.6%. On the other hand, if it is believed that passenger resistance is secondary to an IED not detonating, then overall risk reduction reduces to 91.2% if passenger resistance is reduced to 5%.

Substitution effects: interactions and interdependencies among the layers

As noted, the analysis has assumed that disruption rates are statistically independent. This assumption may not hold in every instance (Stewart and Mueller 2013a, b). Thus, security measures may not be perfectly substitutional: removing one layer of security may alter the systems model and/or detection rates of other layers of security. For example, if passengers or crew know there is an air marshal aboard, they may be less willing to jump a would-be bomber. However, for the most part it seems correct to assume that the layers are statistically independent. Checkpoint screening effectiveness, for example, is not influenced by whether FAMS are on-board. Canines do not care whether there is an air marshal aboard. Do TSOs work less hard because there are BDOs around?

If it is believed that complete independence may not be strictly correct for some layers, the sensitivity analysis suggests that disruption rates can be doubled or halved with little effect on overall risk reduction. This high level of robustness strongly suggests that substitution and/or independence issues wouldn't make much difference even insofar as they may be valid.

Adaptive behaviour by terrorists

It is important to recognise that some terrorists may exhibit adaptive behaviour. Jackson and LaTourette (2015) have developed a set of adaptation strategies: substitute target or location, substitute tactic or attack mode, hide from or deceive defence, avoid defence at the target, attack defence directly, and absorb defence effects.

Adaptive behaviour is inherently difficult to model in a risk analysis, but scenario-based analyses can be enlightening by considering changes such behaviour might make in rates of disruption. Duping someone into unwittingly boarding an aircraft with a bomb concealed in their carry-on luggage is one way to avoid detection from intelligence services, no-fly lists, JTTF, FBI or police. However, even if disruption rates are reduced to zero for these security layers (1, 4, and 5), the overall risk reduction for a passenger-borne bombing declines from 93.1 to 88.6%. Moreover, detonating the bomb would need to be done using either a timer or a pressure trigger, and both of these approaches would complicate bomb design, concealment, and the odds of a successful detonation. If the probability that the bomb is defective in that it becomes more difficult to detonate (layer 17) is increased from 35 to 50%, risk reduction rises from 88.6 to 91.2%. In this case, adaptive behaviour does reduce the effectiveness of some layers, but it also increases the odds of disruption in others.

The insider threat is another example of adaptive behaviour. For example, in an attempt to down a Somali airliner in 2016, an airport-based employee handed the laptop containing the IED to the passenger after he passed through the security checkpoint (Baum 2016). We can model this insider threat by setting disruption rates to zero for the checkpoint layer, VIPR teams, canines, transportation security inspectors, and bomb appraisal officers and by assuming a 5% disruption rate for an added TSA layer of random employee screening. Under those conditions, overall risk reduction declines from 93.1 to 88.3% – that is, the odds of the undeterred terrorist succeeding is increased more than 50% from one in 15 to nearly one in 9. It is also effectively assumed in this analysis that the inside accomplice was able to successfully smuggle the IED into the secured (sterile) area of an airport - an assumption that increases the odds of success, but one that may be overly generous. While an insider threat increases the risk in this example, there are so many potential layers to deter or disrupt an attack that the odds of success remain stacked against the attacker. In the Somali case, it was aircraft resiliency, layer 18, that prevented the airliner from crashing.

To reduce these odds further, one could screen airport workers as they arrive for work. Although there is 100% screening of workers at many foreign airports, there currently is only random screening of airport employees in the United States. If it is assumed that 100% screening of workers leads to the same disruption rate as passenger checkpoint screening (30%), overall risk reduction increases to 91.8%. Whether more rigorous screening of airport employees is cost-effective, our reliability model of the overall system of aviation security can be adapted to the issue, to other threats, and to adaptive behaviour by terrorists.

Overall, the results suggest that it is difficult to imagine a scenario in which an adaptive terrorist working with an organisation is likely to be able to dramatically alter the odds of pulling off a passenger-borne bombing attack. Thus targeting airliners, particularly ones departing from U.S. airports, is not a very feasible strategy for terrorists, and this may help explain why there have been no terrorist attempts on airliners in the United States at all since 9/11. The most sensible form of "adaptive" behaviour would be to abandon airliners as a target entirely and seek out other ones. If the goal is to kill people, the number of potential targets is near infinite (Mueller and Stewart 2011).

Comparisons with other countries

The aviation security layers in Europe, Canada, and Australia are very similar to those in the United States. Although the nomenclature may vary, the intent remains the same. For example, the JTTF is unique to the United States, but the concept of coordination between security services, police, airports, and airlines is not.

However, many European Union countries have fewer air marshals on flights, or even none at all, and they do not require the removal of shoes at the screening checkpoint. The sensitivity analysis in the American case shows that, if the likelihood that air marshals are on board is reduced from 20 to 5%, the overall risk reductions for bombings are essentially unchanged. The same holds true whether shoes are removed, or not removed, during checkpoint screening. Thus, risk reductions estimated for the United States are most likely to apply as well to other Western countries, including Australia.

It is often argued that Israel has the most effective aviation security. All passengers are interviewed by Israeli security officials, air marshals are on every flight, secondary barriers to the cockpit (or double doors) are fitted to all aircraft, and each is equipped with anti-missile defences (Elias 2010). When Richard Reid, the December 2001 shoe bomber, flew on El Al in the summer of 2001, Israeli security "didn't like the look of him, so they checked everything in his bags, and everything he was wearing, and then put an armed sky marshal in the seat right next to him" (Kohn 2002). While Reid was not carrying a bomb at the time, it could be argued that Israeli authorities were perceptive enough to recognise a potential threat and deal with it appropriately. In 1986, a 6 months pregnant Irish woman was interviewed by Israeli security officials at London's Heathrow Airport before her planned El Al flight to Tel Aviv. The interview was "inconclusive," so officials searched her bags, discovering a bomb hidden in the lining of her luggage (Baum 2016). The bag had been given to her by her Jordanian fiancé. This, and other examples, may attest to the effectiveness of the interview process - there has been no successful attack on an El Al airliner in nearly 50 years, which is, as Elias (2010) observes, "a somewhat remarkable feat given terrorist animosities toward Israel."

To reflect the enhanced security measures used by El Al, we increase the rate of disruption for BDOs from 1 to 50% and the probability that air marshals are on a flight to 100%. This model raises overall risk reduction from 93.1 to 96.6%. Increasing the effectiveness of BDOs further to 75% raises the overall risk reduction for bomb attacks to 98.3%. In other words, the odds of a successful bombing attack are reduced nearly three-fold to 1 in 50.

The Israeli approach comes at a considerable cost, however. TSA Administrator John Pistole estimates that Israel spends "about 10 times as much as we spend here in the U.S. per passenger" (Balakrishnan 2016). To duplicate the Israeli approach in the United States would roughly require boosting U.S. government and private spending on aviation security from its current level of $10 billion per year to $100 billion per year. It is highly doubtful that such a spending increase is a worthwhile investment if it reduces risk only by an additional 3–5%. The laws of diminishing returns applies – the first dollars spent on counterterrorism measures are likely to be more worthwhile than the last ones.

Cost-benefit analysis

Estimation of benefit-to-cost ratio

To determine the benefit-to-cost ratio for a security layer the *benefit* is calculated as:

$$\begin{aligned} \textit{Benefit of a security measure} = {} & \textit{probability of a successful attack absent all security measures} \\ & \times \textit{losses sustained in the successful attack} \\ & \times \textit{reduction in risk furnished by the security measure} \end{aligned} \tag{4}$$

This *benefit* is then divided by the *cost* of the security measure to generate an easy to understand decision-making metric – the benefit-to-cost ratio (BCR).

A risk-neutral approach to decision-making indicates that if the BCR exceeds one, the benefits exceed the cost and the measure is deemed to be cost-effective. However, government safety regulations also prefer that safety risks be As Low As

Reasonably Practicable (ALARP) or So Far As is Reasonably Practicable (SFARP). For example, when considering *Reasonably Practicable* judgements, the UK Health and Safety Executive (HSE) advises that the appropriate rule is that the measure must be adopted unless the sacrifice is grossly disproportionate to the risk. Hence, even if the costs outweigh benefits, the security measure could still be reasonably practicable to introduce. How much costs can outweigh benefits before being judged "grossly disproportionate" depends on the factors surrounding the risk. For example the larger the risk, the greater can be the disproportion between the cost and the benefit. The UK HSE provides some guidelines for Disproportionate Factors (DF), noting that DFs of 3 are common for workplace environments, but may extend as high as 10 under some circumstances (HSE 2013). A DF of 3 may be considered appropriate for terrorist threats (Grant and Stewart 2018). This makes sense, as modest risk aversion is tolerable when there is considerable doubt about costs and benefits. Hence, we will assume here that the cost of a security measure is acceptable if the BCR exceeds 0.33 (i.e., 1/DF).

Cost of the security measure

Table 2 shows the estimated cost for most of the layers devoted to deterring and disrupting terrorist attacks to aviation in the United States. For most layers, it is assumed that the security costs are split equally between hijacking and bombing terrorist threats. For example, we assume that 50% of costs for TSO/Checkpoint and travel document checkers, $1.75 billion, is devoted to deterring and disrupting a hijacking, while the other $1.75 billion is devoted to deterring and disrupting an on-board bomb attack. However, some layers, like FAMS, are designed primarily to avoid a repetition of another hijacking attack but may be helpful for a bombing attack. In these cases, it is assumed that 80% of the costs are directed to combating the hijacking threat and 20% to thwarting a bomb attack. On the other hand, canines and VIPR teams are primarily in place to deter or detect bombs (and possibly shooter attacks). For these layers, 80% of the costs are directed to combating bomb attacks and 20% to thwarting a hijacking.

Most of the security measures arrayed in Table 2 have a deterrent role as well as a disruptive one. Stewart and Mueller (2018) show that deterrence and disruption rates are quite similar. Hence, it is assumed that security costs are split 50–50 between their effectiveness at deterring or disrupting a terrorist attack. For example, intelligence (layer 1) is assumed to cost 25% of the total cost given in Table 2 – i.e., of the total cost of $1.45 billion, 25% or $362.5 million is allocated to disrupting, preventing, or foiling a bombing attack. The cost estimates for disrupting, preventing, or foiling (but not for deterring) a bombing attack are shown in Table 4.

Losses sustained in a successful attack

Stewart and Mueller (2011) show that the direct and indirect losses from a successful bombing attack on airliners range from $2.5 billion for the Lockerbie bombing, to an upper bound $50 billion for a suicide bombing (or a series of bombings) that leads to direct and indirect losses approaching those inflicted on 9/11. We take the mean losses for a bombing to be $25 billion.

Table 4 Risk reductions and cost-effectiveness for security measures

	Cost to disrupt a bombing attack ($ millions) FY 2016	Risk reduction	Benefit-to-cost ratio
Acceptable:			
TSA PreCheck	−55 (saving)	0.5%	>>1.0
Passenger and cabin crew resistance	0.75	2.8%	140
JTTF (including FBI and police)	125	2.3%	0.69
VIPR teams	20	0.37%	0.69
Canines	32	0.37%	0.44
Marginal:			
No-fly list & passenger pre-screening	45	0.37%	0.31
Not cost-effective:			
Travel document checkers and Checkpoint/TSOs	900	3.5%	0.15
Intelligence	362.5	1.2%	0.12
Behavior Detection Officers	50	0.07%	0.05
Federal Air Marshal Service	105.5	0.07%	0.02
Not known:			
International partnerships	?	0.37%	–
Customs and Border Protection	?	0.37%	–
Law enforcement officers	–	0.07%	–
Transportation Security Inspectors	?	0.07%	–
Bomb Appraisal Officers	?	0.37%	–
IED proves to be defective	NA	3.7%	–
Aircraft survives even if IED detonates	NA	6.9%	–

Assumes that the probability that terrorist are undeterred is 15% per year. The losses sustained in a successful terrorist attack are assumed to be $25 billion for a bombing

The Benefit-to-Cost ratio cannot be calculated for layers whose cost is unknown

NA Not Applicable

?: Not Known

Probability of an otherwise successful terrorist attack absent all security measures

No terrorist bombing attacks have been attempted on airliners in the U.S. for several decades. A device suspected of being a bomb was discovered in a suitcase of a man who boarded a Haiti Air flight at Kennedy International Airport in 1985. If the last time someone tried to smuggle a bomb onto an aircraft cabin in the United States was over 30 years ago, the historical threat probability is one attack divided by 30 years or 3.3% per year. Moreover, of the 124 cases of planned Islamist terrorism in the United States since 9/11, none targeted airliners in the U.S. (Mueller 2018). Although the shoe and underwear bombers did not board their flights in the U.S., and although the foiled effort to blow up transatlantic airliners with liquid bombs in 2006 was based in London, those experiences show that the threat is real. Accordingly, a very conservative estimate of the threat likelihood over the past 15 years increases to two attacks divided by 16 years (2002–2017) or 12.5%. This is rounded up to 15% per year or one attack every 6 or 7 years in which the attacker is not deterred by the array of security measures.

Assessing the risk reduction and the cost-effectiveness of security measures

Table 4 assesses the individual risk reduction of a security measure by removing it, and then seeing how that affects overall risk reduction. Table 4 also shows the benefit-to-cost ratios for those layers for which cost data are available or could be estimated. The most cost-effective measures are those with high risk reduction, low cost, or a combination of the two.

Federal air Marshal Service

The FAMS is one of TSA's most expensive layers, and in previous research it has failed to be found to be cost-effective against hijacking threats (Stewart and Mueller 2008, 2013a). We find that Federal Air Marshals are unlikely to be important contributors to dealing with other terrorist efforts, such as seeking to down an airliner by exploding bombs in carry-on luggage, as well. The risk reduction supplied by FAMS for that scenario is 0.07%. The attack frequency is a high 0.15 bombing attacks per year, leading to a BCR of 15% × 0.07% × $25 billion)/$105.5 million = 0.02 if losses sustained in a successful terrorist attack is assumed to be $25 billion. This means that $1 of cost buys only two cents of benefit. Even if the risk reduction furnished by FAMS and the losses sustained in the attack are each doubled, the analysis still finds a significant lack of cost-effectiveness: the BCR is no more than 0.08.

Table 4 shows that FAMS has the lowest BCR of all the security layers that could be calculated. It is not surprising, then, that airline CEOs consider it to be the "biggest waste of money we have going in the country today," and members of the House Oversight Committee have called for its elimination (Robinson 2016).

In the aftermath of 9/11, restrictions were placed on Law Enforcement Officers (LEOs) carrying concealed firearms onto aircraft (Shobe 2003). While there is some logic to reducing weapons on aircraft, there would seem to be a pool of LEOs who otherwise would be armed on flights, and they could act as defacto air marshals - and at zero cost (e.g., Wynne 2002). It is unclear if this policy option has been assessed, but it should be one worth considering in light of the billion dollar cost per year for FAMS.

Passenger and cabin crew resistance

Passenger resistance is essentially free, and cabin crew resistance is nearly so. With very high risk reduction and negligible costs, passenger and cabin crew resistance prove to be one of the most cost-effective layers of security (Table 4).

JTTF (including FBI and police)

The contribution of policing which includes the FBI and the free vigilance of the public, supplies a risk reduction of 2.3% (Table 4). As Table 4 illustrates, the BCR ratio is 0.69, which exceeds our minimum acceptable BCR of 0.33. Consequently, this measure is “acceptable” in terms of cost-effectiveness. Added to this, it is possible that the analysis erred on the low side when estimating the effectiveness, and therefore the cost-effectiveness, of this layer. Many plots are foiled by the FBI and police, often relying on tips from the public - although, as noted, none of these has been a plot to take down an airliner (Mueller and Stewart 2016a, b; Mueller 2018). It might be reasonable to assume very considerable success for the FBI because it is the lead agency for investigating the crime of terrorism and because it has a great many agents assigned to the counterterrorism enterprise (Mueller and Stewart 2016a, b). If the disruption rate of this layer is doubled, its overall risk reduction nearly doubles, and it becomes even more cost-effective with a BCR well in excess of unity.

VIPR teams

The Visible Intermodal Protection Response (VIPR) teams are deployed to protect airports and associated facilities, and are comprised of Federal Air Marshals, transportation security inspectors, behavior detection officers, explosives specialists, and local law enforcement and airport officials. Their effect on overall risk reduction is slight, and, as can be seen in Table 4 the BCR is 0.69. However, since this exceeds 0.33 this measure is “acceptable” in terms of cost-effectiveness. Moreover, the high visibility of VIPR teams may have a larger impact on deterrence.

Canines

Although it has been contended that “canine programs have been one of the most consistently successful explosive detection programs in the history of aviation security” and that they constitute the “gold standard” in bomb detection (Price and Forrest 2013), they probably have a modest effect on disruption rates because of their relatively low numbers. The National Explosives Detection Canine Team Program (NEDCTP) provides the same risk reduction as that observed for VIPR teams. However, canines barely pass the decision metric; the BCR is a relatively low 0.44. On the other hand, Stewart and Mueller (2018) suggest that the high visibility of canine teams may have a larger impact on deterrence than that observed for VIPR teams. The measure is accordingly deemed acceptable in terms of cost-effectiveness.

No-fly list and passenger pre-screening

The risk reduction furnished by no-fly list and passenger pre-screening is also 0.39%, and Table 4 shows that the BCR is 0.31. While the no-fly list and passenger pre-screening layer thus barely fails a cost-benefit analysis, it is marginal.

Checkpoint/TSOs and travel document checkers

The travel document checkers are accorded their own layer by TSA, yet for budgetary purposes, checkpoint/TSOs and travel document checkers, a workforce of 30,000, are included in the same line budget. All are TSOs, and all are classified as screening personnel. The risk reduction furnished by passenger and carry-on screening checkpoints (which includes PreCheck) and by travel document checkers is 3.5%. These risk reduction effects are quite high, and they are 50 times higher than that observed for BDOs. However, the estimates of disruption rates for this layer may be on the low side. For example, because checkpoint screening is the most visible layer of aviation security, and because passengers and their carry-on luggage have to run the gauntlet of metal detectors, full-body scanners, X-ray equipment, and explosives trace detection systems, this layer may have a higher probability of detecting weapons or bombs. Martonosi and Barnett (2006) expect this to be approximately 50% while Fletcher (2011), who was TSAs Chief Risk Officer, estimates 75–85%. On the other hand, covert testing by the GAO revealed that checkpoint screening "often failed" to detect concealed IEDS (Elias 2009).

If the disruption rate in Table 2 is increased from 30 to 45%, for example, the contribution to risk reduction for this layer increases from 3.5 to 4.5%. However, this is the security layer with the highest cost at $3.5 billion per year. Hence, even with higher disruption rates, the BCR is relatively low at 0.19. Thus, the screening layer, comprising checkpoint TSOs and travel document checkers, fails a cost-benefit assessment. Stewart and Mueller (2018) find that the screening costs per passenger in Australia and Denmark are about half those of the TSA in the United States. The Screening Partnership Program (SPP) allows for the screening of passengers and property to be performed by TSA-approved private-screening contractors in some American airports, and a U.S. House of Representatives Report finds that that such private screening is 42% cheaper than TSA screening (House 2011). If this cost efficiency could be applied to TSA screening, the BCR would approach 0.4, and its costs would be deemed to be acceptable.

While the screening layer fails to be cost-effective overall, this does not mean that all aspects of this layer are not worthwhile. An example of a worthwhile endeavour is TSA PreCheck (Stewart and Mueller 2017). Approximately 50% of passengers were now eligible for PreCheck and each PreCheck lane provides "the capability for doubling hourly throughput" - an impressive efficiency gain (TSA 2014). Indeed, owing to PreCheck efficiencies, the number of TSA screeners declined by over 1500 and screening costs were reduced by $110 million in FY2016 (DHS 2016). The additional risk reduction due to the implementation of TSA PreCheck is 0.5%. This is a prime example where security can be increased or maintained at *reduced* cost. Not only does PreCheck reduce overall screening costs, but it provides a very substantial additional co-benefit by improving the passenger experience, generating a co-benefit of up to $3 billion per year (Stewart and Mueller 2018). This makes PreCheck a win-win security measure for the Department of Homeland Security (DHS), for passengers, for airlines, and for airports.

Behavior detection officers

After reviewing more than 400 separate studies about detecting deception, the Government Accountability Office found that "the ability of human observers to accurately identify deceptive behavior based on behavioural cues or indicators is the same as or slightly better than chance," and it noted that after ten years of implementing and testing, "TSA cannot demonstrate that the agency's behavior detection activities can reliably and effectively identify high-risk passengers who may pose a threat to the U.S. aviation system" (GAO 2010, 2013). As an indicator in the loss of faith in behavior detection, BDOs and explosives trace detection personnel have not been used since September 2015 to direct passengers not enrolled in PreCheck to the PreCheck (or "expedited") screening lanes. They have been replaced by canine explosives detection teams (Elias et al. 2016).

Since 9/11, some 10 billion passengers have passed through American airports, and although there are no data on how many of these have been observed by BDOs, it appears that not a single one has proved to be a terrorist with active designs to do damage on the flight. In an important sense, Behavior Detection Officers are the ultimate ghost-chasers—they have had a perfect record of not finding anything. Not surprisingly, then, the inspector general of the DHS has concluded that TSA is unable to "show that the program is cost-effective" (Winter and Currier 2015). The analysis supports this conclusion. When BDOs are added to the security layer array, risk reduction goes up by less than 0.1% (Table 4), and, at $200 million per year, this is not an inexpensive layer. The resulting BCR for BDOs is very low at 0.05. The costs for the program are thus about 20 times higher than the benefit. A sensitivity analysis shows that the only way that BDOs would be cost-effective is if the attack probability is increased from 0.15 attacks per year to one attack per year, or if the layer's disruption rate estimate is increased seven-fold. Behavior Detection Officers quite convincingly fail a cost-benefit assessment. The program has the second lowest benefit-to-cost ratio of those examined. Only FAMS does worse.

Discussion

The risk analysis finds that the FAMS and BDOs, at a combined cost of nearly $1.3 billion per year, fail to be cost-effective. In general, we have biased the consideration toward leaving FAMS and BDOs with a perhaps somewhat unrealistically high amount of risk to reduce. However, even with that assumption in place, it appears that neither program reduces risk enough to justify its high cost. The considerable cost of screening passengers at the checkpoint is also likely not to be a good investment. However, TSA PreCheck is a welcome development that will help to improve the efficiency and reduce the cost of checkpoint screening without adversely affecting safety.

Based on descriptions of aircraft bombings since 1960 (Baum 2016), there is a 50–50 chance that an airliner will survive and land safely in the event of a successful IED detonation in the cabin. In Table 4, we estimate, then, that aircraft resiliency (layer 18) contributes more to overall risk reduction than any other layer. Aircraft, like other types of infrastructure, are more robust and resilient than we often give them credit for. The next highest risk reduction is the inability of a terrorist to successfully construct and detonate an IED in-flight (layer 17). This too, reflects the reality that the challenges faced in crafting an IED that is small enough to evade detection at airport checkpoints, but large enough to severely damage an airliner, are daunting indeed. Even if terrorists have access to bomb making materials and training, the probability of a failed detonation is 35% as suggested by experience in the Middle East and North Africa (Grant and Stewart 2012).

The analysis has concentrated on one terrorist threat to aviation: bombs borne by passengers. But there are other threats that would also need to be considered in a full evaluation of aviation security. Bombs in checked luggage was once a much feared terrorist tactic. However, of the tens of billions of pieces of checked luggage transported on American carriers in the period after a bomb planted in checked luggage caused a PanAm jet to crash into Lockerbie, Scotland, in 1988, not a single one exploded to down an aircraft. Terrorists could also try to down an airliner with shoulder-fired surface-to-air missiles. However, except for one miss by two missiles on an Arkia Israeli Airliner in Kenya in 2002, there have been no attacks against U.S. or Western aircraft, and, “No credible intelligence has been reported to the public that al Qaeda or other terrorist groups may be planning such attacks” (Elias 2010).

The analysis provides a snapshot of risk reductions and cost-effectiveness under present conditions. Of course, 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, and so forth. Nevertheless, it does not seem that the competence of terrorists and the destruction they inflict are on the rise, and 9/11 is increasingly standing out as an aberration, not a harbinger - indeed, scarcely any terrorist attack anywhere in the world has managed to do even one-tenth as much total damage. Also, as noted in Adaptive behaviour by terrorists section, it is difficult to imagine a scenario in which an adaptive terrorist is likely to be able to dramatically alter the odds of pulling off a hijacking or passenger-borne bombing attack.

The systems model provides a starting point for aviation 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. A more detailed and comprehensive study may be required to fully model the interactions and interdependencies between different threats in aviation security. Nonetheless, the analysis provides a basis for assessing the influence and sensitivity of policy options on risk reduction.

Conclusions

This paper developed a risk assessment of aviation security measures in the United States. A reliability analysis of the overall system of aviation security allows the rate of disruption to be estimated for bombing threats by terrorist groups to aircraft. The analysis is presented in a fully transparent manner: readers who wish to challenge or vary the analysis and assumptions are provided with the information, data, and framework with which to do so. The risk analysis finds that existing layers of aviation security reduce the risk of a successful attack by a bomb carried on board by an undeterred terrorist to be 93%. These levels of risk reduction are very robust: security remains high even when the parameters that make it up are varied considerably. Of the layers of security, the FAMS and BDOs failed a cost-benefit assessment, while efficiencies in checkpoint screening are needed for this layer to be deemed cost-effective and expenditures associated with the JTTF and police, TSA PreCheck, VIPR teams and canines are acceptable.

Acknowledgements The support of the Australian Research Council grant DP160100855 is acknowledged.

References

Aaronson T (2013) The terror factory. Ig Publishing, Brooklyn

Balakrishnan A (2016) Would you pay more for extra airport security? CNBC, March 24

Baum P (2016) Violence in the skies: a history of aircraft hijacking and bombing. Summerdale Publishers, Chichester

Congress (2015) House Report 114-125, Department of Homeland Security Appropriations Act, 2016, 114th Congress, Washington, DC, July 21

Congress (2016) Senate Report 114-264, Department of Homeland Security Appropriations Bill, 2017, 114th Congress, Washington, DC, May 26

DHS (2016) Budget-in-brief: fiscal year 2016. U.S. Department of Homeland Security, Washington, DC

Elias B (2009) Airport passenger screening: background and considerations for congress. Congressional research service, Washington, DC April 23

Elias B (2010) Airport and aviation security. CRC Press, Boca Raton

Elias B, Petermann DR, Frittelli J (2016) Transportation security: issues for the 114th congress. Congressional research service, Washington DC, May 9

Fletcher KC (2011), Aviation security: case for risk-based passenger screening. Master's Thesis, Naval Postgraduate School, California

GAO (2010) Aviation security: efforts to validate TSA's screening behavior detection program underway, but opportunities exist to strengthen validation and address operational challenges. Report GAO-10-763, United States Government Accountability Office, Washington DC, May

GAO (2013) Aviation security: TSA should limit future funding for behavior detection activities. Report GAO-14-159, United States Government Accountability Office, Washington DC, November

Grant M, Stewart MG (2012) A systems model for probabilistic risk assessment of improvised explosive device attack. International Journal of Intelligent Defence Support Systems 5(1):75–93

Grant M, Stewart MG (2015) Probabilistic risk assessment for improvised explosive device attacks causing significant building damage. J Perform Constr Facil 29(5):B4014009

Grant M, Stewart MG (2018) Postal IEDs and risk assessment of work health and safety considerations for postal workers. International Journal of Risk Assessment and Management (in press)

House (2011) TSA ignores more cost-effective screening model. United States house of representatives, committee on transportation and infrastructure, oversight and investigations staff report, June 3

HSE (2013) HSE principles for Cost Benefit Analysis (CBA) in support of ALARP decisions, Health & Safety Executive, United Kingdom, accessed at http://www.hse.gov.uk/risk/theory/alarpcba.htm on 16 Mar 2013

Jackson BA, LaTourette T (2015) Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries. Journal of Air Transport Management 35(March):26–33

Jackson BA, Chan EW, LaTourrette T (2012) Assessing the security benefits of a trusted traveler program in the presence of attempted attacker exploitation and compromise. J Transp Secur 5:1–34

Jacobson SH, Karnani T, Kobza JE, Ritchie L (2006) A cost-benefit analysis of alternative device configurations for aviation checked baggage security screening. Risk Anal 26(2):297–310

Jenkins BM (2011) Stray dogs and virtual armies: radicalization and recruitment to jihadist terrorism in the United States since 9/11. RAND Corporation, Santa Monica

Kenney M (2010) 'Dumb' yet deadly: local knowledge and poor tradecraft among Islamist militants in Britain and Spain. Studies in Conflict and Terrorism 33(10):911–932

Kohn D (2002) The safest airline: a security example set by Israel's El Al. 60 minutes, CBS, January 15

Lee AJ, Jacobson SH (2011) The impact of aviation checkpoint queues on optimizing security screening effectiveness. Reliab Eng Syst Saf 96(8):900–911

Martonosi SE, Barnett A (2006) How effective is security screening of airline passengers? Interfaces 36(6): 545–552

McLay LA, Lee AJ, Jacobson SH (2010) Risk-based policies for airport security checkpoint screening. Transp Sci 44(3):333–349

Morral AR, Price CC, Oritz DS, Wilson B, LaTourrette T, Mobley BW, McKay S, Willis HH (2012) Modeling terrorism risk to the air transportation system. RAND Corporation, Santa Monica

Mueller J (2018) Terrorism since 9/11: the American cases. Mershon Center, Ohio State University, Columbus, OH. http://politicalscience.osu.edu/faculty/jmueller/SINCE.pdf

Mueller J, Stewart MG (2011) Terror, security, and money: balancing the risks, benefits, and costs of homeland security. Oxford University Press, New York

Mueller J, Stewart MG (2012) The terrorism delusion: America's overwrought response to September 11. Int Secur 37(1):81–110

Mueller J, Stewart MG (2014) Evaluating counterterrorism spending. J Econ Perspect 28(3):237–248

Mueller J, Stewart MG (2016a) Chasing ghosts: the policing of terrorism. Oxford University Press, Oxford

Mueller J, Stewart MG (2016b) Misoverestimating ISIS: comparisons with Al-Qaeda. Perspectives on Terrorism 10(4):32–41

Poole RW (2015) Fresh thinking on aviation security. Journal of Air Transport Management 48(September):65–67

Price JC, Forrest JS (2013) Practical aviation security: predicting and preventing future threats. Butterworth-Heinemann, Oxford

Robinson W (2016) Just one Air Marshal a week deals with a disruptive passenger on a plane yet taxpayers still shell out $800 MILLION a year. Daily Mail, March 14

Sewell EC, Lee AJ, Jacobson SH (2013) Optimal allocation of aviation security screening devices. J Transp Secur 6:103–116

Shobe A (2003) Law enforcement officers flying armed: past, present, and future. Institute for Criminal Justice Education, September 30

Stewart MG, Mueller J (2008) A risk and cost-benefit assessment of U.S. aviation security measures. Journal of Transportation Security 1(3):143–159

Stewart MG, Mueller J (2011) Cost-benefit analysis of advanced imaging technology fully body scanners for airline passenger security screening. Journal of Homeland Security and Emergency Management 8(1):Article 30

Stewart MG, Mueller J (2013a) Terrorism risks and cost-benefit analysis of aviation security. Risk Anal 33(5): 893–908

Stewart MG, Mueller J (2013b) Aviation security, risk assessment, and risk aversion for public Decisionmaking. Journal of Policy Analysis and Management 32(3):615–633

Stewart MG, Mueller J (2014a) Risk and cost-benefit analysis of police counter-terrorism operations at Australian airports. Journal of Policing, Intelligence and Counter Terrorism 9(2):98–116

Stewart MG, Mueller J (2014b) Cost-benefit analysis of airport security: are airports too safe? Journal of Air Transport Management 35(March):19–28

Stewart MG, Mueller J (2017) Risk and economic assessment of expedited passenger screening and TSA PreCheck. J Transp Secur 10(1):1–22

Stewart MG, Mueller J (2018) Are we safe enough? Measuring and assessing aviation security. Elsevier, New York

Stewart MG, Ellingwood BR, Mueller J (2011) Homeland security: a case study in risk aversion for public decision-making. International Journal of Risk Assessment and Management 15(5/6):367–386

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

von Winterfeldt D, O’Sullivan TM (2006) Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? Decis Anal 3(2):63–75

Willis HH, 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 28:325–339

Winter J, Currier C (2015) TSA’s secret behavior checklist to spot terrorists. www.firstlook.org/theintercept, March 27

Wynne M (2002), Flying while armed - letting cops board planes with their sidearms will bolster homeland security. POLICE magazine, September 1