Journal of Air Transport Management 35 (2014) 19–28

Contents lists available at ScienceDirect

Journal of Air Transport Management

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

Cost-benefit analysis of airport security: Are airports too safe?

Mark G. Stewart [a,*], John Mueller [b,c,1]

[a] Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales 2308, Australia
[b] Mershon Center for International Security Studies, Ohio State University, USA
[c] Cato Institute, Washington, D.C., USA

Keywords:
Risk
Cost-benefit analysis
Airports
Security
Terrorism

ABSTRACT

This paper assesses 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. The analysis considers threat likelihood, the cost of security measures, hazard likelihood, risk reduction and expected losses to compare the costs and benefits of security measures to decide the optimal security measures to airports. Monte-Carlo simulation methods were used to propagate hazard likelihood, risk reduction and loss uncertainties in the calculation of net benefits that also allows probability of cost-effectiveness to be calculated. It is found that attack probabilities had to be much higher than currently observed to justify additional protective measures. Overall, then, it is questionable whether special efforts to further protect airports are sensible expenditures. Indeed, some relaxation of the measures already in place may well be justified.

1. Introduction

Much research on aviation security focuses on airplanes due no doubt to the events of September 11 2001 and to the more recent attempts to bomb U.S. bound flights in 2001, 2006 and 2009. Although there may be special reasons to protect airplanes, however, it is not at all clear that there are any special reasons to protect airports. Elias (2010) states that these areas have ‘unique vulnerabilities because it is unsecured’. However, compared with many other places of congregation, people are more dispersed in airports, and therefore a terrorist attack is likely to kill far fewer than if, for example, a crowded stadium is targeted. The 2011 suicide bombing in the baggage claim area of Moscow's Domodedovo airport did kill 37 and injure many others, and this shows that airports are not unattractive targets. However, in the previous year suicide bombers targeted the Moscow metro killing 25, and the year before that, derailed the Moscow to St. Petersburg high-speed train killing 27.

In the fourteen year period 1998–2011, the Global Terrorism Database recorded 20 attacks on airports in the U.S. and Europe, killing 64 people. Notable among these are the attempted bombing of the Glasgow international airport in 2007 and the shooting of two people at the El Al ticket counter at Los Angeles International Airport (LAX) in 2002. Over the same period there were 31 attacks on aircraft. In total, attacks on aviation accounts for only 0.5% of all terrorist attacks, and attacks on airports comprise less than half of these. This experience has led the 2007 U.S. National Strategy for Aviation Security to conclude that ‘reported threats to aviation infrastructure, including airports and air navigation facilities are relatively few.’ A study of 53 cases that have come to light since 9/11 in which Muslim terrorists planned, or in many cases vaguely imagined, doing damage in the United States finds only two in which an airport facility was on the target list (Mueller, 2013).

A risk and cost-benefit assessment quantifies risk reduction of security measures, losses from a successful attack, threat likelihood, probability that attack is successful, and cost of security measures. This allows costs and benefits of security measures to be compared and optimal security measures to be selected. In earlier work evaluating in-flight airline security measures we have considered cost per life saved as the sole decision-support criterion (Stewart and Mueller, 2008), and we later conducted a systems reliability analysis with a more detailed cost-benefit assessment that included other losses from a terrorist attack (Stewart and Mueller, 2013a,b; see also Jackson et al., 2012). These analyses considered single point estimates of risk reduction and losses. In this paper, we characterise probability of attack success, risk reduction, and losses as probabilistic variables allowing confidence intervals to be calculated (for preliminary efforts, see Stewart and Mueller, 2011). For a literature review of probabilistic terrorism risk assessment see Stewart and Mueller (2013a).

[*] Corresponding author. Tel.: +61 2 49216027.
E-mail addresses: mark.stewart@newcastle.edu.au (M.G. Stewart), bbbb@osu.edu (J. Mueller).
[1] Tel.: +1 614 2476007.

0969-6997/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jairtraman.2013.11.003

The U.S. Transportation Security Administration (TSA) has extensive security guidelines for airport planning, design and construction (TSA, 2011). However, there is little information about whether TSA guidelines satisfy a cost-benefit assessment. The U.S. Government Accountability Office and Congress have repeatedly urged the TSA to undertake risk and cost-benefit assessments of major programmes (GAO, 2011; Rogers, 2012). The TSA has used the Risk Management Analysis Tool (RMAT) to conduct risk assessments. However, a review by RAND (Morral et al., 2012) revealed a number of key deficiencies. Among them: 'RMAT does not attempt to describe the absolute risks to the system, rather just the relative risks, or changes in magnitude of risk', and thus RMAT can only 'partially meet' TSA needs. What is needed is a methodology that can assess 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.

This paper seeks to assess the absolute risks and cost-effectiveness of measures designed to protect airport terminals and associated facilities such as car parks from terrorist attack. These are areas where the general public has unrestricted access to before passengers undertake security screening and pass into secured (sterile) areas prior to aircraft boarding. We rely extensively on cost and risk reduction data for LAX compiled by RAND in 2004 (Stevens et al., 2004), which considered bombings or shooting attacks at the airport curbside or in other pre-screening areas of passenger terminal buildings. We evaluate security measures such as reducing congestion by additional check-in staff and TSA screening lines, making buildings blast-resistant, and screening of vehicles and luggage for IEDs (Improvised Explosive Devices). These range in cost from $2.5 to $60 million per airport per year. LAX is the sixth busiest airport in the world, and third busiest in the United States. Hence, LAX represents a typical large international airport in a class with London Heathrow, New York JFK, and Washington Dulles airports.

The paper first explains risk-based decision theory, and then describes the threats that airport terminal buildings are exposed to, enhanced security measures to deal with these threats, and their cost. The risk reduction for enhanced security measures, loss likelihood, and losses sustained in a successful attack are then inferred. Fatality risks, net present value and benefit-to-cost ratio are calculated for various attack probabilities. The probability of cost-effectiveness is also calculated. This allows the cost-effectiveness of security measures to be assessed and compared, and optimal security measures selected.

2. Risk-based decision theory

2.1. Definition of risk

A standard definition of risk or expected loss is:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequences} \tag{1}$$

This is consistent with the conceptual framework adopted by the TSA (NRC, 2010) and risk analyses for many applications (e.g., Kaplan and Garrick, 1981; Stewart and Melchers, 1997). This leads to a simplified formulation for risk:

$$E(L) = \sum \Pr(T)\Pr(L|T)L \tag{2}$$

where $\Pr(T)$ is the annual *threat* probability per target, $\Pr(L|T)$ is the conditional probability of loss (that the explosive will be successfully detonated or the gun will fire leading to damage and loss of life) given occurrence of the threat (*vulnerability*), and L is the loss or *consequence* (i.e., damage costs, number of people exposed to the hazard) if the attack is 100% successful. The summation sign in Eqn. (2) refers to the number of possible threats and losses.

Each threat has a certain relative likelihood $\Pr(T|\text{attack})$ such that $\Pr(T) = p_{\text{attack}} \times \Pr(T|\text{attack})$ where p_{attack} is the annual probability of attack absent of the security measure. Note that $\Pr(L|T)$ represents the likelihood that a terrorist will succeed in creating the desired hazard and loss. This will be influenced by task complexity (degree of difficulty in planning, acquiring materials, and carrying out an attack), competency of the individual, and security measures. If the attack is successful in achieving the desired effect and maximum losses then $\Pr(L|T) = 100\%$.

2.2. Cost-effectiveness of security measures

Three criteria may be used to compare the cost-effectiveness of adaptation strategies:

1. Net Present Value or NPV
2. Benefit-to-cost ratio or BCR
3. Break-even analysis that assesses how high the probability of an otherwise successful attack needs to be for a security measure to begin to be cost-effective or $\Pr(\text{BCR} > 1)$ or $\Pr(\text{NPV} > 0)$

The 'benefit' of a security measure is the losses averted due to the security measure, and the 'cost' is the cost of the security measure. The net present value NPV (or net benefit) is equal to benefit minus the cost. The decision problem is to maximise the net present value

$$\text{NPV} = \sum E(L)\Delta R + \Delta B - C_{\text{security}} \tag{3}$$

where ΔR is the reduction in risk caused by security measures, C_{security} is the cost of security measures including opportunity costs that reduces risk by ΔR, ΔB is the expected co-benefit from the security measure not directly related to mitigating vulnerability or hazard (such as reduction in crime, improved passenger experience, etc), and $E(L)$ is the 'business as usual' expected loss (risk) given by Eqn. (2). The risk reduction (ΔR) may arise from a combination of reduced likelihood of threat or hazard or loss, and can vary from 0% to 100%.

A complementary decision metric is the benefit-to-cost ratio

$$\text{BCR} = \frac{\sum E(L)\Delta R + \Delta B}{C_{\text{security}}} \tag{4}$$

Maximising NPV (but not BCR) will lead to optimal outcomes when prioritising the cost-effectiveness of various security measures (e.g., OMB, 1992). In terms of risk communication, the concept of a BCR has some appeal to policy makers. However, prioritising security measures based on maximising BCR may lead to suboptimal outcomes as a high BCR can be achieved if the cost is small, but NPV may be lower than other security measures (OMB, 1992; OBPR, 2009). There are some advantages to BCR, as the Australian Government Office of Best Practice and Regulation explains "BCR is only preferred to NPV in situations where capital projects need to be funded from a limited pool of funds. In this case, it can be shown that allocating funds by way of the BCR criterion results in a higher net social benefit than by using NPV. However, regulatory CBA [cost benefit analysis] rarely deals with making capital investments from fixed funding pools." (OBPR, 2009). Either way, if a security measure has NPV > 0 then clearly BCR > 1.

We recognise that perceptions of risk and risk averseness are commonly cited as reasons to overinvest in homeland security measures. Mueller and Stewart (2011a,b) discuss this phenomenon in some detail, and these issues also arise for other low probability-high consequence activities such as nuclear power. Ultimately, however, we follow guidance from the U.S. Office of Management and Budget (OMB) and other regulatory agencies that strongly recommend risk-neutral attitudes in public policy decision-making as described by Eqn. (2) (e.g., OMB, 1992; Sunstein, 2002; Ellingwood, 2006; Stewart et al., 2011). This entails using mean or average estimates for risk and cost-benefit calculations, and not worst-case or pessimistic estimates.

If input parameters are random variables then the output of the analysis (NPV or BCR) is also variable. This allows confidence bounds of NPV and BCR to be calculated, as well as the probability that a security measure is cost-effective denoted herein as $\Pr(\mathrm{NPV} > 0)$ and $\Pr(\mathrm{BCR} > 1)$. Clearly, $\Pr(\mathrm{BCR} > 1) = \Pr(\mathrm{NPV} > 0)$. If $\mathrm{NPV} > 0$ or $\mathrm{BCR} > 1$ then there is a net benefit and so the adaptation measure is cost-effective. The above equations can be generalised for any time period, discounting of future costs and more detailed time-dependent cost and damage consequences.

A key challenge is the prediction of attack probability p_{attack} and relative threat likelihood $\Pr(T|\mathrm{attack})$. A scenario-based approach assess benefits by simply assuming that $\Pr(T) = 100\%$ – i.e., that the attack will occur. This is the approach adopted by Stevens et al. (2004), Zycher (2003) and others when comparing costs and benefits of security measures. However, they are engaging in a form of probability neglect – they leave out of consideration the likelihood of a terrorist attack. Not surprisingly, such an approach tends to find that security measures are cost-effective. This however, is most unrealistic, as there is no certainty that an attack will occur at that specific item of infrastructure in the next year. Although the probability of a terrorist attack somewhere, sometime may be high, the probability that any particular target will be attacked is very low.

There is clearly uncertainty in any prediction of $\Pr(T)$, particularly in a dynamic threat environment where the threat may arise from an intelligent adversary who may adapt to changing circumstances to maximise likelihood of success. It is true, of course, that some terrorist attacks are carefully planned. However, many, quite possibly most, terrorist target selection effectively becomes something like a random process (Mueller and Stewart, 2011a,b). In most cases, target selection may not have been random in their minds but would essentially be so in the minds of people trying specifically to anticipate their next move. Nonetheless, a more workable solution is a 'break-even' analysis where the outcome of the analysis is the minimum attack probability needed for a security measure to be cost-effective.

3. Protection of airport terminals

3.1. Threats, enhanced security measures, and their cost

We consider four significant threat scenarios aimed at airport terminal buildings and associated landside facilities:

T_1 large truck bomb – detonated in front of a crowded terminal.
T_2 curbside car bomb – detonated in front of a crowded terminal.
T_3 luggage or vest bomb – detonated in curbside or inside a crowded terminal.
T_4 public grounds shooting attack – terrorists attempt to shoot as many people as possible.

These threats have been called 'major vulnerabilities' or 'major' threats that can kill a large number of people (Stevens et al., 2004; Elias, 2010). We assume relative threat likelihood $\Pr(T|\mathrm{attack})$ to be equal for all threats such that $\Pr(T|\mathrm{attack}) = 25\%$. Other threats to airport facilities seem unlikely (Stevens et al., 2004).

There is a paucity of realistic cost data on the costs of airport security measures, a phenomenon Mueller and Stewart (2011a,b) refer to as 'cost neglect': much of the literature on homeland security dwells on vulnerabilities and recommends enhanced security measures with little or no attention paid to how such security measures will actually cost. A notable exception is the 2004 RAND study which compiled a list of measures that would enhance security at LAX, and more importantly, estimated their expected annual cost (Stevens et al., 2004). LAX is also already one of the more secure airports in the U.S., but enhanced security measures aimed at deterring, disrupting, preventing, foiling or protecting against the threats identified above are (Stevens et al., 2004):

1. Add permanent vehicle search checkpoints with bomb detection capability

A quick examination of vehicles entering the airport may help detect large vehicle bombs (VBIED). Brief (10 s) examinations will allow the largest bombs to be detected.

2. Add skycaps, check-in personnel, and more TSA lines

Lines or queues of people at check-in and security screening could pose an attractive target due to high densities of people. Improving airport efficiency by adding more personnel at curbside check-in (skycaps), airline counter check-in, and security screening lanes reduce line lengths by 80–90%.

3. Enhance training of airport police rapid reaction team to SWAT standards

Airport police trained to SWAT (special weapons and tactics) standards could 'modestly' reduce vulnerability to a well trained and coordinated attack by terrorists with automatic weapons and/or hand grenades, and is a relatively inexpensive measure.

4. Direct all vehicles to remote lots

Establish distant areas for passenger dropoff and pickup, bussing passengers to and from the terminal.

5. Add curbside blast deflection and shatterproof glass

Glass walls are a major shrapnel hazard, so utilising blast-resistant glazing and adding 6-feet high reinforced concrete blast walls will reduce the severity of VBIED attacks.

6. Eliminate the lane closest to terminals

Increases stand-off from VBIED, thus reducing the vulnerability of damage to the terminal, but not necessarily to people on the curb.

7. Add additional support columns for upper level roadway

Reduces the vulnerability of elevated roadway to a VBIED by providing additional or stronger supporting columns.

8. Search all luggage entering terminals

This assumes a cursory search of luggage (30 s) and high staff levels so queues are kept to a minimum (to reduce the density of people).

9. Add 30 handheld bomb sniffers

Bomb-detection equipment that is fast and reliable will provide for rapid inspections (i.e. low manpower requirements).

10. Add 30 bomb sniffing dogs

Officers with dogs trained to detect bombs can be deployed in terminals to randomly examine people and their luggage. Assume one dog and handler per terminal.

Table 1 shows the total annual cost for each security measure for LAX estimated by Stevens et al. (2004). It is the sum of recurring operating cost and capital expenditures for a 10 year service life with 4.5% discount rate. All costs are inflation adjusted to 2012 dollars.

It is important to stress that costs such as inconveniencing and deterring passengers are not considered. As will be discussed in Section 4.3, such opportunity costs associated with some security measures might be considerable. Thus the establishment of remote drop-off and pickup lots would reduce the vulnerability of the airport itself to VBIEDs, but at significant cost and inconvenience to passengers. The same holds for parking restrictions near the terminal and extra search and screening measures. Not only will these delay some passengers, but visible physical security measures directed at terrorism can enhance fear and anxiety (Grosskopf, 2006). Ultimately, such delays and anxiety can deter many from flying at all.

3.2. Risk reductions due to enhanced security measures – ΔR

The risk reductions for the ten enhanced security measures identified in Section 3.1 are now discussed and quantified.

1. Adding permanent vehicle search checkpoints with bomb detection capability will, according to Stevens et al. (2004), 'greatly reduce vulnerability' for large vehicle bombs and so $\Delta R = 85\% \pm 10\%$, but will only provide 'some effectiveness' against smaller (car) bombs. In a review of 20 studies, Mosteller and Youtz (1990) find that the expression 'sometimes' corresponds to a probability of 18–35%, and so risk reduction is $\Delta R = 25\% \pm 10\%$ for car bombs. This security measures is viewed as 'not very effective' for a luggage bomb which translates to the complement of 'very effective' and so $\Delta R = 15\% \pm 10\%$. Such checkpoints might also detect smaller explosives such as those used in a suicide bomb vest. As there is uncertainty about risk reductions, we assume upper and lower bounds of ±10% for all risk reductions.
2. Stevens et al. (2004) states that adding skycaps, check-in personnel, and more TSA lines, will 'greatly reduce vulnerability', and that this will reduce the number of passengers vulnerable to luggage bomb attack by 80–90%. However, the measure will be ineffective for the arrivals hall where passengers congregate to collect their luggage or outside the luggage claim area where friends and family congregate to meet arriving passengers. In these cases, the density of people is large, and presumably this is why this area was the target of the 2011 Domodedovo airport bombing. Since the number of departing and arriving passengers are roughly similar, the risk reduction of 80–90% for the departure hall, and 0% for arrivals hall might suggest an average risk reduction of $\Delta R = 45\%$. This is most likely an overestimate as a terrorist can select the location of an attack, and if the arrivals hall has more people, a luggage bomb or a suicide bomb can be detonated in that location. In this case, risk reduction is nearer to zero. A similar risk reduction might occur for VBIEDs since a reduction in airport crowding will reduce potential fatalities considerably, hence we assume that $\Delta R = 45\% \pm 10\%$.
3. Enhanced training of airport police rapid reaction team to SWAT standards is viewed as a security measure that will 'modestly' reduce vulnerability (Stevens et al., 2004), which according to Mosteller and Youtz (1990) translates into a 40–59% risk reduction with $\Delta R = 50\% \pm 10\%$.
4. Diverting all vehicles to remote car parking lots is seen as 'unaffordable' at $60 million per year since there are cheaper (and 'nearly as effective') security measures: adding permanent vehicle search checkpoints with bomb detection capability, adding skycaps, check-in personnel, and more TSA lines, and adding curbside blast deflection and shatterproof glass (Stevens et al., 2004). Since adding permanent vehicle search checkpoints with bomb detection capability gives $\Delta R = 85\%$, this provides a benchmark for other security measures. In this case, diverting all vehicles to remote car parking lots is seen as more effective, so we assume that $\Delta R = 90\% \pm 10\%$.
5. Stevens et al. (2004) suggest that adding curbside blast deflection and shatterproof glass has similar effectiveness to adding permanent vehicle search checkpoints with bomb detection capability and so $\Delta R = 85\% \pm 10\%$. The risk reductions for a curbside car bomb will be similar for a large truck bomb.
6. Eliminating a lane closest to the terminal will increase VBIED stand-off by approximately 3–5 m which can reduce the damaging effects of a bomb. However, this assumes that the truck or car bomb does not breach the standoff by ramming the vehicle into the terminal (e.g. Glasgow airport attack). A small increase in stand-off will not have a significant effect on damage, and so a modest risk reduction of $\Delta R = 25\% \pm 10\%$ is assumed for truck and car bombs.
7. Adding support columns for the upper level roadway, is according to Stevens et al. (2004), only 'slightly effective'. A risk reduction of $\Delta R = 25\% \pm 10\%$ is assumed herein.

Table 1
Annual cost of security measures for a large airport (adapted from Stevens et al., (2004)).

Security measure	Annual cost $C_{security}$ ($ million)
1. Add permanent vehicle search checkpoints with bomb detection capability	14.0
2. Add skycaps, check-in personnel, and more TSA lines	5.0
3. Enhanced training of airport police rapid reaction team to SWAT standards	2.5
4. Direct all vehicles to remote lots	60.0
5. Add curbside blast deflection and shatterproof glass	3.5
6. Eliminate lane closest to terminals	2.5
7. Add additional support columns for upper level roadway	6.0
8. Search all luggage entering terminals	22
9. Add 30 handheld bomb sniffers	3.5
10. Add 30 bomb sniffing dogs	5.0

8. Searching all luggage entering a terminal is viewed as 'very effective' which according to Mosteller and Youtz (1990) translates into an 80–90% risk reduction. However, this would prove ineffective in detecting a suicide bomber wearing a concealed vest IED. A halved risk reduction of $\Delta R = 45\% \pm 10\%$ is appropriate.

9. and 10. Adding 30 handheld bomb detectors, and adding 30 bomb sniffing dogs are viewed as 'not very effective' for a luggage bomb which translates to the complement of 'very effective' and so $\Delta R = 15\% \pm 10\%$.

Table 2 summarises risk reductions for each threat and security measure. We have relied on risk reductions either explicitly stated or inferred from Stevens et al. (2004). However, expert judgements, and fault trees and logic diagrams, together with systems engineering and reliability approaches, will aid in assessing complex interactions involving threats, vulnerabilities and consequences (e.g., Stewart and Mueller, 2011, 2013a,b for airliner security). A more detailed and comprehensive study is required to properly model the complex interactions and interdependencies in airport passenger terminal security. Nonetheless, the risk reductions in Table 2 provide a basis to assess the influence and sensitivity of policy options on risk reduction and cost-effectiveness of security measures.

3.3. Loss likelihood – Pr(L|T)

In principle, an IED is relatively simple to design and manufacture if done by well trained personnel, resulting in reliabilities in excess of 90% (Grant and Stewart, 2012). However, the probability of an IED creating a damaging effect (casualties) reduces to 19% for terrorists in Western countries where there is less opportunity for IED operational skills to be acquired (Grant and Stewart, 2012). This was clearly evident from the second attack on the London Underground on 21 July 2005 where four IEDs failed to initiate, and Glasgow international airport in 2007 and Times Square in 2010 where VBIEDs failed to initiate. Note that loss likelihood $\Pr(L|T)$ increases to 65% for terrorists or insurgents in the Middle East.

Hence, we assume that device complexity is less and placement issues are fewer for a luggage bomb (T_3) and consequently that loss likelihood is $\Pr(L|T_3) = 30\%$. This reduces to $\Pr(L|T_1) = \Pr(L|T_2) = 15\%$ for complex and large IEDs such as a VBIED (T_1 and T_2) where placement and timing is more crucial to achieve maximum damaging effects thus posing substantial difficulties for terrorists.

Indeed, since 9/11 terrorists in the United States have been able to detonate bombs in only one case (in Boston in 2013) and the same holds for the United Kingdom (the bombings of London transport on 7 July 2005)(Mueller and Stewart, 2012). These estimates, then, are likely quite generous overestimates of the capacities of actual terrorists.

A grounds shooting attack (T_4) is much easier to accomplish as semi-automatic weapons and ammunition in the U.S. are relatively easy to acquire. Hence a well trained and coordinated shooting and/or grenade attack has high chance of success (e.g. Mumbai, 2008) leading to $\Pr(L|T_4) = 85\%$.

A triangular probability distribution is used to represent uncertainty of $\Pr(L|T)$, see Table 3.

3.4. Losses sustained in a successful attack – L

Since there have been few successful attacks on airports, it may be instructive to first consider losses imposed by attacks on aircraft. A 2005 RAND study hypothesised that the downing of an airliner by a shoulder fired missile would lead to a total economic loss of more than $15 billion (Chow et al., 2005). The September 11, 2001, attack directly resulted in the deaths of nearly 3000 people with an associated loss of approximately $20 billion. In addition, 9/11 caused approximately $30 billion in physical damage, and the impact on the U.S. economy of the 9/11 attacks range from $50–150 billion in 2010–11 dollars (e.g. Mueller and Stewart, 2011a). An upper bound estimate of the losses of 9/11 might approach $200 billion. Global airline losses from 9/11 total at least $100 billion (Gordon et al., 2007; IATA, 2011). These losses were mainly due to a 1–5% drop in airline passengers in 2001 and 2002. The next attack is unlikely to cause the same (dramatic) response, and losses from 9/11 were also magnified by the recession.

IATA revenue projections to 2020 show approximately 5% annual increases in passengers and revenues, with world-wide revenues of $598 billion in 2011 (IATA, 2012). An attack at a major airport might result in a more wary travelling public and no global growth in revenue/passengers for one year, equivalent to a 5% revenue or passenger decrease for one year. This would entail a loss of at least $30 billion.

This is an extreme case, however. For from time to time, terrorists have been able to down airliners – the Lockerbie tragedy of 1988 high among them – but the response by the flying public was not nearly so extreme as in the aftermath of 9/11. Moreover after two Russian airliners were blown up by suicidal Chechen female terrorists in 2004, that country's airline industry seemed to have continued with little interruption. Airline passenger numbers after the attack did decline, but this has been attributed mainly to the 60 percent increase in fuel prices, and by the following year, passenger

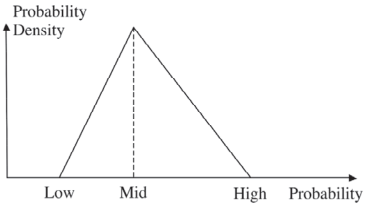
Table 2
Mean risk reduction for security measures at a large airport.

Security measure	Mean risk reduction ΔR			
	1. Large truck bomb	2. Curbside car bomb	3. Luggage or vest bomb	4. Public grounds shooting attack
1. Add permanent vehicle search checkpoints with bomb detection capability[a]	**85%**	**25%**	**15%**	–
2. Add skycaps, check-in personnel, and more TSA lines[a]	45%	45%	**45%**	45%
3. Enhanced training of airport police rapid reaction team to SWAT standards[a]	–	–	–	**50%**
4. Direct all vehicles to remote lots	90%	90%	–	–
5. Add curbside blast deflection and shatterproof glass	85%	85%	–	–
6. Eliminate lane closest to terminals	25%	25%	–	–
7. Add additional support columns for upper level roadway	25%	–	–	–
8. Search all luggage entering terminals	–	–	**45%**	–
9. Add 30 handheld bomb sniffers	–	–	**15%**	–
10. Add 30 bomb sniffing dogs	–	–	**15%**	–

Bold = Benchmark estimate from Stevens et al. (2004).
[a] Recommended by Stevens et al. (2004) as 'worthwhile'.

Table 3
Loss Likelihood Pr($L|T$).

	Low	Mid	High
1. large truck bomb	5%	15%	50%
2. curbside car bomb	5%	15%	50%
3. luggage bomb	5%	30%	50%
4. public grounds shooting attack	75%	85%	100%



traffic had increased by 3.9 percent (IATA, 2010). The suicide bomb attack at Moscow's Domodedovo airport in January 2011 also had little impact on Russian airlines; indeed Russian airlines increased passenger numbers in 2011 by 12.6% compared to 2010, and international passengers increased by 13.2% over the same period (Borondina, 2012). Hence, a $30 billion in airline losses is very much an upper bound of consequences of a terrorist attack at a U.S. airport. Losses for the four threats identified in Section 3.1 are now described.

1. A large truck bomb (T_1) containing 1800 kg of TNT detonated 11 m from the front wall of Dulles International Airport near Washington D.C. would wreak 'immense destruction' according to a threat and vulnerability analysis conducted by Weisz (2012) – causing 306 fatalities or severe injuries. By way of comparison, this scenario is similar to the 1995 Oklahoma City bombing that killed 165 people, the U.S. Embassy attack in Kenya in 1998 that killed 213 people, and the 2008 truck bombing of the Islamabad Marriott Hotel that resulted in the deaths of 54 people. These attacks, however, appear to be the exception, as the average number of fatalities from a VBIED is 36 and only 0.5% of bomb attacks had more than 30 fatalities (LaTourrette et al., 2006). Assuming an average of 50 fatalities from an on-ground explosion, and based on the value of a single life (VSL) of $6.5 million (Robinson et al., 2010), an economic loss of 50 fatalities comes to $325 million. Note that Morral et al. (2012) conclude that 50 fatalities from an airport attack is 'unrealistically high', but we adopt this figure to be slightly conservative, and since most losses arise from indirect causes, and not from fatalities or injuries. Physical damage might average $100 million, and $1 billion in the extreme. Flight disruptions and relocation of check-in counters, etc. might total several billion dollars as a plausible upper bound. The additional costs of social and business disruptions, loss of tourism, and the like, might total $5–10 billion. A mean total loss of $10 billion is reasonable, with plausible lower and upper bounds of $500 million (assuming direct losses only) and $50 billion (assuming zero growth in global passenger numbers for a year valued at $30 billion and $10 billion in other indirect losses), respectively.
2. A curbside car bomb containing several hundred kilograms of explosives would result in fewer fatalities and less physical damage, but the indirect losses would still be substantial. The total cost in this case might total $7.5 billion, with plausible lower and upper bounds of $500 million and $40 billion, respectively. Note that the TSAs RMAT estimates indirect losses of only $11.1 billion for an attack on aircraft, and less for other threats (such as airports) (Morral et al., 2012).
3. The vulnerability analysis by Weisz (2012) also concluded that a 45 kg (100 pound) luggage bomb detonated near a check-in counter would wreak considerably less structural damage with approximately 30 fatalities. The 2011 suicide bombing of the arrivals area of Moscow's Domodedovo airport that killed 37 was reportedly accomplished with an IED of 2–5 kg. While some flights were diverted to other airports in Moscow immediately following the attack, Domodedovo airport remained open, and damage to airport infrastructure was minimal. While fatalities and physical damage would be less than with a large truck bomb, the public averseness to travel would be similar resulting in social and business disruptions, loss of tourism, etc. but these losses may be lower than for a large truck bomb but similar for a curbside car bomb. The losses sustained from the 2005 London and 2004 Madrid bombings which killed 52 and 191 commuters, respectively amounted to no more than $5 billion in direct and indirect losses (including loss of life, loss of tourism, business interruption, etc.) (Mueller and Stewart, 2011a). Mean loss is thus $5 billion. This estimate assumes the Madrid and London bombings have relevance – though a coordinated set of multiple bombings in the centre of a city is likely to inflict far greater indirect costs than a single explosion at an isolated airport. Plausible lower and upper bounds are $500 million and $30 billion, respectively.
4. The attack in Mumbai in 2008 bears some resemblance to the public grounds shooting threat. Two attackers targeted a crowded Mumbai railway station killing over 50 people, and injuring a hundred others, and more were killed in nearby hotels and restaurants by other terrorists. As with other threat scenarios, losses resulting from loss of life and physical damage are minor when compared to indirect losses. The mean cost in this case might total $2 billion, with plausible lower and upper bounds of $500 million and $20 billion, respectively.

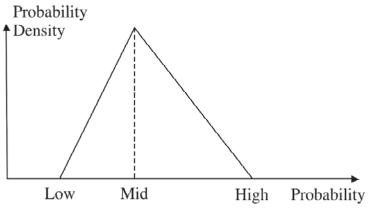
Table 4 summarises low, mid, and high estimates of loss (L) assuming a 'successful' attack. A triangular probability distribution is used to represent uncertainty of losses. It should be kept in mind that airports sprawl and are only two or three stories high, and therefore damage to a portion is not likely to be nearly as significant as damage to a taller or more compact structure. Moreover, if a bomb does go off at an airport, the consequences would probably be comparatively easier to deal with: passengers could readily be routed around the damaged area, for example, and the impact on the essential function of the airport would be comparatively modest (Mueller and Stewart, 2011a). This suggests that the losses proposed above might be skewed more to the lower bound – or even below it. However, public fear and averseness to air travel could sometimes increase these losses to those approaching the high (upper bound) estimates.

3.5. Attack probability

Since the cost and risk reduction data is for a large U.S. airport (LAX), we will calculate attack probabilities for large airports. A 'large' airport may be one with over five million passengers per year: for example, Glasgow international airport handles 6.5 million passengers per year. Using this criterion, there are 75, 70,

Table 4
Loss L in Billions of Dollars.

	Low	Mid	High
1. large truck bomb	0.5	10	50
2. curbside car bomb	0.5	7.5	40
3. luggage bomb	0.5	5	30
4. public grounds shooting attack	0.5	2	20



and 32 large airports in Europe, Asia-Pacific and the U.S., respectively.

According to the Global Terrorism Database, in the 14 year period 1998–2011 there were five bombing and shooting attacks on large airport terminals in Europe (one every 2 or 3 years), the same number of attacks in the Asia-Pacific area, and one in the U.S. If we assume there are 70–75 large airports in Europe and in the Asia-Pacific area, the probability an individual airport will be attacked is approximately 0.5% per year for each area. In the U.S. the attack probability is considerably lower at approximately 0.2% per year. Of the 11 attacks, most failed to inflict any casualties or significant damage at all; that is, the yearly likelihood an individual airport will be *successfully* attacked is lower by more than a half.

It is important to note that this assumes terrorists only desire to attack large airports. However, there are thousands of smaller passenger airports, and it is not clear that there is a great deal of comparative advantage to the terrorist in attacking large ones. In addition, enhanced security measures at large airports might have the effect of diverting terrorists to the smaller ones. Even if only the 100 largest of these smaller airports were to be included in the count for each area, the probability an individual airport will be attacked would be greatly reduced.

We use historical data here and it can be argued that they do not necessarily provide a reliable guide to the future. However, in this case there needs to be some explanation as to why the capacity of terrorists to commit damage will increase in the future and why terrorists will become more likely to target airports than they have in the past. To date, there is little evidence that terrorists are becoming any more destructive, particularly in the West, and fears about large, sophisticated attacks have been replaced by ones concerning smaller conspiracies and one-off attackers (Mueller and Stewart (2011a,b)).

4. Results

4.1. Fatality risks

According to the Global Terrorism Database, in the period 1998–2011 attacks on airport terminals in Europe inflicted 37 fatalities, and 24 fatalities resulted from attacks to airport terminals in the Asia-Pacific area (note that these statistics cover all airports, not just ‘large’ ones). In the same period there was one attack at a U.S. airport (LAX) where a gunmen killed two people at the El Al ticket counter in 2002.

The annual fatality risk is approximately 4.6×10^{-9} for the Asia-Pacific region, 2.6×10^{-9} for Europe, and 4.4×10^{-10} for the U.S. These are extremely low risks, and are considered “acceptable” based on a fair degree of agreement about acceptable risk in which an annual fatality risk of 1×10^{-6} is generally considered ‘acceptable’ (Stewart and Melchers, 1997). However, terrorism is a hazard where risk acceptability is not only a matter of fatality risks: there are in addition direct economic consequences as well as indirect ones, both of which could be significant as discussed in Section 3.4.

4.2. Cost-benefit assessment

The net present value (NPV) and benefit-to-cost ratio (BCR) for each security measure are calculated from Eqns. (3) and (4) where $\Pr(L|T)$ and L are triangular distributed random variables, ΔR is a uniformly distributed random variable, and we assume co-benefits $\Delta B = 0$. Monte-Carlo simulation methods are used to estimate the mean NPV and BCR, and probability that a security measure is cost-effective $\Pr(\text{NPV} > 0)$ or $\Pr(\text{BCR} > 1)$, for annual attack probabilities from 0.01% (one attack every 10,000 years) to 100% (one attack every year). Note the attack probability is the annual probability of attack per airport and that the threat has not been thwarted by other security or police agencies (or the public). Also note that $\Pr(\text{NPV} > 0) = \Pr(\text{BCR} > 1)$. Since the analysis considered only the costs and benefits for the following year, discounting of costs and benefits was not required. However, for a longer time period or differing economic lives, results may be sensitive to discount rates used (Boardman et al., 2011) as is the relationship between discount rates and risk aversion (Snell, 2011). These issues are beyond the scope of the present paper.

Table 5 shows the mean BCR for various attack probabilities assuming terrorist only will attack large airports. A mean BCR is cost-effective when it exceeds one. Adding curbside blast protection has the highest mean BCR and is therefore likely to be the most cost-effective security measure. Note that, as discussed earlier, the likelihood of any sort of an attack (whether a failure or a success) on a large airport is less than 0.5% per airport per year. If the annual attack probability is 0.5% per airport per year, Table 5 shows that the mean BCR exceeds one only for adding skycaps, check-in personnel and more TSA lines (security measure 2), enhanced training of police (3), adding curbside blast deflection (5), and eliminate lane closest to terminals (6). The security measure with the highest BCR is adding curbside blast deflection and shatterproof glass with a mean BCR of 2.55 for an attack probability of 0.5%. This means that $1 of cost buys $2.55 of benefits. Clearly, as the attack probability decreases, the benefit reduces, thus reducing net benefit. If the annual attack probability is under 0.2% per airport per year (the rate of attacks for large airports in the U.S.), then none of the enhanced security measures are cost-effective.

Table 6 shows the mean NPV (measured in $ millions) for various attack probabilities. The trends are similar to that observed from Table 5 where NPV is highest (most cost-effective) for adding curbside blast deflection and shatterproof glass with a mean NPV of $5.53 million for an attack probability of 0.5%. In this case, this security measure has the highest BCR and highest NPV. However, for a higher attack probability (1%) adding curbside blast deflection and shatterproof glass has the highest BCR of 5.09, but NPV is second highest at $14.7 million. The highest NPV occurs for adding skycaps, check-in personnel and more TSA lines (security measure

Table 5
Mean benefit-to-cost ratio (BCR).

Security measure	Annual attack probability per airport (%) absent additional airport security measures				
	0.1%	0.2%[a]	0.5%[b]	1.0%	10%
1. Add permanent vehicle search checkpoints with bomb detection capability	0.09	0.19	0.49	0.97	9.66
2. Add skycaps, check-in personnel, and more TSA lines	0.42	0.84	2.10	4.21	42.10
3. Enhanced training of airport police to SWAT standards	0.33	0.65	1.63	3.27	32.74
4. Direct all vehicles to remote lots	0.03	0.06	0.16	0.31	3.14
5. Add curbside blast deflection and shatterproof glass	0.51	1.02	2.55	5.09	50.91
6. Eliminate lane closest to terminals	0.21	0.42	1.04	2.08	20.82
7. Add additional support columns for upper level roadway	0.05	0.10	0.24	0.49	4.85
8. Search all luggage entering terminals	0.02	0.03	0.09	0.17	1.73
9. Add 30 handheld bomb sniffers	0.04	0.07	0.18	0.37	3.71
10. Add 30 bomb sniffing dogs	0.02	0.05	0.13	0.25	2.54

[a] Rate of attack in U.S. in the period (1998–2011).
[b] Rate of attack in Europe and Asia-Pacific in same period.

2) at $15.6 million, with BCR still a high 4.21. Hence, if the annual attack probability exceeds 1%, the optimal security measure would be security measure 2 as it has the highest NPV.

The probability that NPV > 0 or BCR > 1 is shown in Fig. 1 for the four security measures most likely to be cost-effective (i.e., those with highest NPV or BCR), and the one with a low NPV and BCR (security measure 8). With reference to Fig. 1, it is clear that if attack probability is less than 0.1% per year then there is near zero likelihood that any of the security measures are cost-effective and so 90–100% likelihood of a net loss. On the other hand, if attack probabilities exceed 100% or one attack per year then all security measures are certain to be cost-effective (i.e. $\Pr(\text{BCR} > 1) = 100\%$).

The decision problem can be recast as a break-even analysis. The minimum attack probability for security measures to be cost effective is selected such that there is 50% probability that the benefit will equal the cost (see Table 7). As expected, break-even probabilities are less than observed attack probabilities of 0.2–0.5% only for adding skycaps, check-in personnel, and more TSA lines (security measure 2), enhanced training of airport police to SWAT standards (3), and add curbside blast deflection and shatterproof glass (5). All other security measures require considerably higher attack probabilities than those currently being observed for them to be cost-effective. However, a decision-maker may wish the likelihood of cost-effectiveness to be higher before investing millions of dollars in security measures – to say 90% so there is more certainty about a net benefit and small likelihood of a net loss. Table 7 also shows the minimum attack probabilities needed for there to be a 90% chance that security measures are cost-effective. In this case, the threshold attack probabilities more than double when compared to the break-even analysis. The results are not overly sensitive to the probabilistic models used.

Clearly, due to the uncertainties inherent in such an analysis, a sensitivity analysis is recommended. Doubling the cost of physical damages or loss of life has a negligible effect on NPV or BCR, which illustrates that in this situation the expected losses are dominated by indirect losses. Many of the assessed security measures would only begin to be cost-effective if the current rate of attack at airports in the U.S., Europe, and the Asia-Pacific increases by a factor of 10–20. Thus, input parameters can be doubled or halved and this would not change the fundamental findings herein that many airport security measures fail a cost-benefit assessment.

4.3. Cost and benefit relevance of the passenger experience

Security measure 3, adding more skycaps and check-in personnel and more TSA lines is one of the more cost-effective under our assumptions as it mitigates against most threats. This measure will also improve the passenger experience by reducing queues and waiting times, with the result that the co-benefit ΔB in Eqns. (3) and (4) will exceed zero dollars.

Treverton et al. (2008) reported that TSA security increased delays by 19.5 min in 2004, and that passengers value their time at about $40 per hour (in 2012 dollars). Clearly, the longer a passenger waits to be screened the more they are likely to be unsatisfied (Gkritza et al., 2006), and waiting in security lines is an important indicator of passenger experience. Holguin-Veras et al. (2012)

Table 6
Mean net present value (NPV) in $ millions.

Security measure	Annual attack probability per airport (%) Absent additional airport Security measures				
	0.1%	0.2%[a]	0.5%[b]	1.0%	10%
1. Add permanent vehicle search checkpoints with bomb detection capability	−$12.6	−$11.3	−$7.12	−$0.27	$122
2. Add skycaps, check-in personnel, and more TSA lines	−$2.92	−$0.93	$5.33	$15.6	$202
3. Enhanced training of airport police to SWAT standards	−$1.69	−$1.56	$1.56	$5.55	$80.5
4. Direct all vehicles to remote lots	−$58.1	−$56.2	−$50.4	−$40.8	$129
5. Add curbside blast deflection and shatterproof glass	−$1.66	$0.05	$5.53	$14.7	$175
6. Eliminate lane closest to terminals	−$1.96	−$1.47	$0.16	$2.83	$50.1
7. Add additional support columns for upper level roadway	−$5.70	−$5.41	−$4.49	−$3.02	$23.5
8. Search all luggage entering terminals	−$21.6	−$21.2	−$20.1	−$18.2	$16.0
9. Add 30 handheld bomb sniffers	−$3.37	−$3.25	−$2.88	−$2.24	$9.20
10. Add 30 bomb sniffing dogs	−$4.87	−$4.75	−$4.37	−$3.75	$7.70

[a] Rate of attack in U.S. in the period (1998–2011).
[b] Rate of attack in Europe and Asia-Pacific in same period.

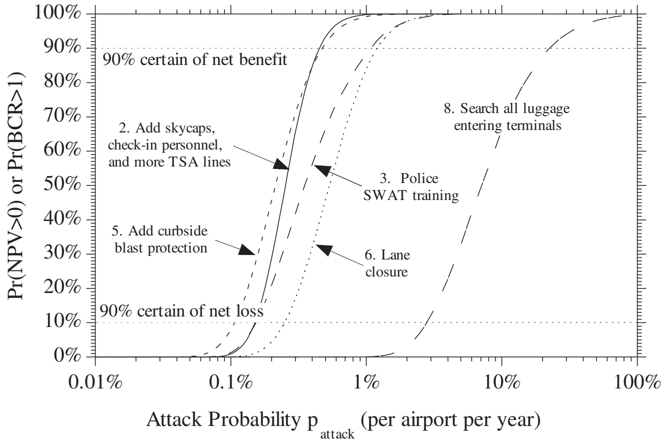


Fig. 1. Probability of cost effectiveness Pr(NPV > 0) or Pr(BCR > 1), for various attack probabilities.

found 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). Hence, an improved passenger experience will also increase revenues to airlines.

The number of passengers departing LAX in 2011 was 30.9 million, or 4.3% of all enplanements in the U.S. If waiting times at check-in and TSA lines can be reduced by a total of a modest five minutes, then this equates to savings at LAX alone of (i) $103 million per year in value of passenger time, and (ii) $64 million in increased airline revenues. The total savings at LAX is a co-benefit rounded down to ΔB = $150 million per year. Since the costs of providing additional skycaps, check-in personnel, and more TSA lines at LAX is only $5 million, then the NPV is at least $145 million even for zero attack likelihood. Moreover, if the attack probability is 0.2%, BCR increases from 0.84 with $\Delta B = 0$ (see Table 5) to 30.83 with ΔB = $150 million per year, and NPV increases to $149.1 million. Clearly, considering the co-benefits of an enhanced passenger experience adds to the benefits of some security measures, dramatically improving their cost-effectiveness.

Table 7
Threshold attack probabilities.

Security measure	Minimum attack probability for enhanced security expenditures on protecting an airport terminal to be 50% sure of being cost-effective.	Minimum attack probability for enhanced security expenditures on protecting an airport terminal to be 90% sure of being cost-effective.
1. Add permanent vehicle search checkpoints with bomb detection capability	1.20%	2.30%
2. Add skycaps, check-in personnel, and more TSA lines	0.25%	0.42%
3. Enhanced training of airport police to SWAT standards	0.35%	1.10%
4. Direct all vehicles to remote lots	3.50%	7.11%
5. Add curbside blast deflection and shatterproof glass	0.22%	0.43%
6. Eliminate lane closest to terminals	0.53%	1.21%
7. Add additional support columns for upper roadway	2.60%	7.35%
8. Search all luggage entering terminals	7.02%	20.00%
9. Add 30 handheld bomb sniffers	3.72%	13.10%
10. Add 30 bomb sniffing dogs	5.25%	17.70%

On the other hand, eliminating the lane closest to an airport terminal can result in significant costs because this is likely to lead to greater traffic congestion and inconvenience. If we assume that this will delay a passenger entering the terminal by only 5 min, using the cost data above, the cost is $103 million per year in value of passenger time, not to mention the lost time of friends and family who may be accompanying the passenger. In this case, $C_{security}$ is now the sum of direct and opportunity costs or $2.5 million + $103 million which we round to $C_{security}$ = $105 million per year. Since the costs of security increase more than 40 fold, BCR will decrease by 40 fold leading to very low values indeed. For example, a break-even analysis shows that the attack probability would have to exceed 50%, or one attack on the individual airport every two years, before eliminating the lane closest to an airport terminal would be cost-effective. This compares to only 0.53% if opportunity costs are ignored (see Table 6). Opportunity costs obviously can dramatically reduce the cost-effectiveness of some security measures.

5. Conclusions

The risk and cost-benefit decision framework described herein illustrates the key concepts and data requirements. This provides a starting point for this type of risk analysis – and to flesh out some of the issues, including data requirements becoming more challenging as the systems model increases in detail and complexity. Our analysis considered each security measure in isolation, whereas policy options might prefer a mix of security measures. In this case, security measures may also not be perfectly substitutional; for example, removing one layer of security may alter the systems model and/or risk reduction of other layers of security. A more detailed and comprehensive study is required to properly model the complex interactions and interdependencies in airport security.

The protection of airport terminals and associated facilities such as car parks at LAX from terrorist attack was used to illustrate the cost-effectiveness of protective and counter-terrorism measures. This analysis considered threat likelihood, cost of security measures, and random variability of hazard likelihood, risk reduction and losses to compare the costs and benefits of security measures to decide the optimal security measures to airports. Monte-Carlo simulation methods were used to propagate hazard likelihood, risk reduction and loss uncertainties in the calculation of net present value and benefit-to-cost ratio that also allows probability of cost-effectiveness to be calculated.

It was found that attack probabilities had to be much higher than currently observed rates of attack to justify protective measures. This was the general result even though the analysis was substantially biased toward coming to the opposite conclusion. Thus, we assumed a terrorist attack would inflict considerable direct and indirect damage, that attacks would only target large airports thereby exaggerating their likelihood per target because the many smaller airports were not included in the target count, and were very generous in our estimates about how much the security measures would reduce risk. We also underestimated the costs of the security measures by ignoring any costs entailed in inconveniencing travellers or deterring them from flying.

In fact, it may be worthwhile to consider whether airports are actually very attractive terrorist targets. If the goal of the terrorist is to kill people and inflict physical damage, there are many other places to detonate a bomb or undertake an armed attack. In addition, although the blowing up of an airliner may have considerable negative consequences for the airline and travel industry, an isolated attack at an airport is unlikely to be anywhere near as damaging. Moreover, if the analysis suggests that enhancement of airport security is highly questionable, it may well be time to consider if many of the security arrangements already in place to protect airports are excessive.

Acknowledgements

Mark Stewart appreciates the financial support of the Australian Research Council.

References

Boardman, A.E., Greenberg, D.H., Vining, A.R., Weimer, D.L., 2011. Cost-Benefit Analysis: Concepts and Practice. Pearson, Boston.

Borondina, P., 2012. Russian airlines passenger traffic up 12.6%, load factor down in 2011. Air Trans. World, 10 February 2010.

Chow, J., Chiesa, J., Dreyer, P., Eisman, M., Karasik, T.W., Kvitky, J., Lingel, S., Ochmanek, D., Shirley, C., 2005. Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat. RAND Corporation, Santa Monica, CA.

Elias, B., 2010. Airport and Aviation Security: U.S. Policy and Strategy in the Age of Global Terrorism. CRC Press, Boca Raton.

Ellingwood, B.R., 2006. Mitigating risk from abnormal loads and progressive collapse. J. Perform. Constr. Facil. 20 (4), 315–323.

GAO, 2011. Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11. U.S. Government Accountability Office, Washington, D.C.

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.

Gordon, P., Moore II, J.E., Pak, J.Y., Richardson, H.W., 2007. The economic impacts of a terrorist attack on the U.S. Commercial Aviation System. Risk Anal. 27 (3), 505–512.

Grant, M., Stewart, M.G., 2012. A systems model for probabilistic risk assessment of improvised explosive device attack. Int. J. Intell. Def. Support Syst. 5 (1), 75–93.

Grosskopf, K.R., 2006. Evaluating the societal response to antiterrorism measures. J. Homel. Secur. Emerg. Manag. 3 (2).

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, 2010. Facts and Figures. International Air Transport Association, Pressroom. March 2, 2010.

IATA, 2011. The Impact of September 11 2001 on Aviation. International Air Transport Association, Geneva.

IATA, 2012. 2012 Annual Review. International Air Transport Association, Geneva.

Jackson, B.A., LaTourrette, T., Chan, E.W., Lundberg, R., Morral, A.R., Frelinger, D.R., 2012. Efficient Aviation Security. RAND, Santa Monica, CA.

Kaplan, S., Garrick, B.J., 1981. On the quantitative definition of risk. Risk Anal. 1 (1), 11–27.

LaTourrette, T., Howell, D.R., Mosher, D.E., MacDonald, J., 2006. Reducing Terrorism Risk at Shopping Centers an Analysis of Potential Security Options. RAND Corporation, Santa Monica, CA.

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, Santa Monica, CA.

Mosteller, F., Youtz, C., 1990. Quantifying probabilistic expressions. Stat. Sci. 5 (1), 2–12.

Mueller, J., Stewart, M.G., 2011a. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security. Oxford University Press, New York.

Mueller, J., Stewart, M.G., 2011b. The price is not right: the U.S. spends too much money to fight terrorism. Playboy 58 (10), 149–150.

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

Mueller, J., 2013. Terrorism Since 9/11: the American Cases. http://politicalscience.osu.edu/faculty/jmueller/since.html.

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, D.C.

OBPR, 2009. Best Practice Regulation Guidance Note: Decision Rules in Regulatory Cost-Benefit Analysis. Office of Best Practice Regulation, Australian Government, Canberra. April 2009.

OMB, 1992. Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs (Revised), Circular No. A-94, October 29, 1992. Office of Management and Budget, Washington, DC.

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).

Rogers, M., 2012. Rebuilding TSA into a smarter, leaner organization. In: A Majority Staff Report – Subcommittee on Transportation Security Committee on Homeland Security, 112th Congress, September 2012.

Snell, M., 2011. Cost-Benefit Analysis: a Practical Guide. Thomas Telford, London.

Stevens, D., Schell, T., Hamilton, T., Mesic, R., Brown, M.S., et al., 2004. Near-Term Options for Improving Security at Los Angles International Airport. RAND Corporation, Santa Monica.

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., 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), 30.

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., 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 Anal. Manag. 32 (3), 615–633.

Sunstein, C.R., 2002. The Cost-Benefit State: the Future of Regulatory Protection. ABA Publishing, American Bar Association, Chicago.

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.

TSA, 2011. Recommended Security Guidelines for Airport Planning, Design and Construction. Transportation Security Administration, Washington, D.C.. May 2011.

Weisz, R.G., 2012. America's Lack of Airport Security. In: 2012 Critical Infrastructure Symposium, Arlington, Virginia.

Zycher, B., 2003. A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures. RAND Corporation, Santa Monica, CA.