*Journal of Policing, Intelligence and Counter Terrorism,* 2014
Vol. 9, No. 2, 98–116, http://dx.doi.org/10.1080/18335330.2014.940816



# A risk and cost–benefit analysis of police counter-terrorism operations at Australian airports

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

[a]*Centre for Infrastructure Performance and Reliability, University of Newcastle, Callaghan, Australia;* [b]*Mershon Center for International Security Studies, Ohio State University, Columbus, USA*

Recent events have highlighted the vulnerabilities of airports and aircraft to terrorist attack, and has led to an increased police presence at many airports. Airport policing is designed to protect airport terminals and aircraft from terrorist attack. This paper assesses the risks and cost-effectiveness of Australian Federal Police (AFP) airport counter-terrorism (CT) policing at Australian airports. The risk reduction of AFP policing, losses from a successful attack, threat likelihood, and cost of AFP policing are quantified. The benefit-to-cost ratio is then calculated for various threat probabilities. A 'break-even' analysis calculates the minimum threat probability or risk reduction needed for AFP airport CT policing to be cost-effective. Airport CT policing begins to become cost-effective if it reduces risk by approximately 25 percent and if the probability of one attack at any airport in Australia exceeds 5 percent per year. These conditions do not seem prevail, but it does not follow that zero spending on airport CT policing is the preferred policy option. Moreover, the co-benefits of airport CT policing—such as reduction in crime and reassurance to the traveling public—may be considerable, and could dramatically improving the cost-effectiveness of the measure.

**Keywords:** airport security; policing; risk; terrorism



## Introduction

In the wake of the 9/11 attacks, counter-terrorism (CT) become a major focus of governments worldwide. For example, the USA increased expenditures on domestic CT by more than $100 billion per year (Mueller & Stewart, 2011a, 2011b), and many countries introduced stronger anti-terrorism legislation (e.g., Tulich, 2012; Walker, 2012). The events of 11 September 2001 and the more recent attempts to bomb US-bound flights in 2001, 2006, and 2009 have led to much research on aviation security. The focus of these efforts has mainly been on airplanes since "any attack guarantees maximum publicity" (George & Whatford, 2007). However, Elias (2010) notes that an airport has "unique vulnerabilities because it is unsecured". There is little information about whether airport security satisfies a cost–benefit assessment, or how airport policing can be made more effective. The Australian Office of Best Practice Regulation, US Office of Management and Budget, and other regulatory agencies strongly recommend risk and cost–benefit assessments of major programs. A risk and cost–benefit assessment quantifies risk reduction of security measures,

*Corresponding author. Email: mark.stewart@newcastle.edu.au

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 (hardened cockpit doors, air marshals) we have considered cost per life saved as the sole decision-support criterion (Stewart & Mueller, 2008), and we later conducted a systems reliability analysis with additional layers of security (full-body scanners, secondary barriers to the cockpit, armed flight deck officers, airport infrastructure protection, etc.) and a more detailed cost–benefit assessment that included other losses from a terrorist attack (Stewart & Mueller, 2011, 2013a, 2013b, 2014; see also Jackson et al., 2012). Utility theory can be used to factor risk aversion into the decision process (e.g., Stewart, Ellingwood, & Mueller, 2011). For a literature review of probabilistic terrorism risk assessment, see Stewart and Mueller (2013a).

As Donkin and Bronitt (2013) note, "measuring performance in the context of CT policing is challenging but not impossible" and "governments rarely justify the adoption or evaluate the effects of new CT initiatives by reference to scientifically informed research". However, they point to the innovative model of performance measurement for drug law enforcement developed by the Australian Institute of Criminology (AIC); see Willis, Anderson, and Homel (2011). The AIC has also developed a guide to cost–benefit analysis for crime prevention and criminal justice research (Dossetor, 2011). The framework described by Dossetor (2011) is well suited to crime prevention where there is an ample statistical database of crime, its prevention and its cost. Terrorism is mostly a low probability—low consequence event, although sometimes, of course, the consequences are high. It has much in common with nuclear power, commercial aviation, environmental protection, and other highly reliable systems subject to human factors and extreme events. In this case, predictive models of hazard, vulnerability, resilience, and loss need to be developed, often in the absence of large statistical databases (e.g., Stewart & Melchers, 1997).

Police at many airports around the world are provided from local, state, or federal law enforcement agencies (e.g., Rekiel & de Wit, 2013). Australia is no exception (e.g., McFarlane, 2007; Prenzler, Lowden, & Sarre, 2010), with the Australian Federal Police (AFP) providing over 600 officers for the policing of ten major airports in Australia. A significant responsibility of these officers is CT policing designed to protect airport terminals and aircraft from terrorist attack. This paper seeks to assess the risks and cost-effectiveness of AFP airport CT policing. It first describes the threats that airports and aircraft are exposed to, and the loss likelihood, and losses sustained in a successful attack are then inferred from empirical data and modeling, as is the cost of AFP airport CT policing. The net benefit or net present value (NPV) is then calculated for various threat probabilities and risk reductions, and a 'break-even' analysis then calculates the minimum threat probability or risk reduction needed for AFP airport CT policing to be cost-effective. A sensitivity analysis is conducted to assess the effect of changes in relative threat likelihood, risk reduction, vulnerability, and consequences on break-even risk reductions.

Note that the results presented herein are preliminary, and based on our 'best estimates' using publicly sourced material. Thus, all data should be seen as illustrative rather than definitive, and are used as a 'proof-of-concept' of how a

risk and cost–benefit analysis can be applied to the challenging area of policing resource allocation. Although the application here is to Australian airports, the approach can be used more broadly. Note that this paper is an expanded version of a Working Paper published by the ARC Centre of Excellence in Policing and Security in 2013 (Stewart & Mueller, 2013c).

## Cost–benefit analysis of airport CT policing

The standard definition of risk adopted by the US Department of Homeland Security (NRC, 2010) and risk analyses for many applications (e.g., Stewart & Melchers, 1997) is:

$$(\text{Risk}) = (\text{Threat}) \times (\text{Vulnerabilty}) \times (\text{Consequences}) \tag{1}$$

where

- Threat means annual probability there will be a terrorist attempt.
- Vulnerability means probability of loss (that the explosive will be successfully detonated or the gun will fire leading to damage and loss of life) given the attempt.
- Consequences means loss or consequence if the attack is successful in causing damage. This includes not only economic costs and lives lost, but indirect and intangible losses as well.

Security measures seek to reduce risk by reducing the threat, vulnerability, and/or consequences of a terrorist attack. For any security measure, the risk reduction can vary from 0–100 percent (or even a negative number for an ill-suited security measure).

A security measure is cost-effective when the benefit of the measure outweighs the costs of providing the security measure—i.e., the benefit exceeds the cost. The NPV or net benefit is:

$$\begin{aligned}&\text{Net Present Value} = \text{Benefit} - \text{Cost}\\&= (\text{Risk}) \times (\text{Risk Reduction}) + (\text{Co}-\text{Benefits}) - (\text{Cost of Security Measure})\end{aligned} \tag{2}$$

A security measure is cost-effective if the NPV > 0. A complementary decision metric is benefit-to-cost ratio (BCR) equal to benefit divided by cost. Maximizing NPV (but not BCR) will lead to optimal outcomes when prioritizing the cost-effectiveness of various security measures (e.g., Hall, Brown, Nicholls, Pidgeon, & Watson, 2012; OMB, 1992). In terms of risk communication, the concept of a BCR has some appeal to policy-makers. However, prioritizing security measures based on maximizing BCR may lead to sub-optimal outcomes as a high BCR can be achieved if the cost is small, but NPV may be lower than other security measures (OBPR, 2010; OMB, 1992). 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, 2010).

Either way, if a security measure has NPV > 0, then clearly BCR > 1.

Equations (1) and (2) are consistent with international risk management standards such as ISO 31000-2009. This approach has also been applied to assessing the cost-effectiveness of a range of homeland security measures (e.g., Jackson et al., 2012; Jacobson, Karnani, Kobza, & Ritchie, 2006; Poole, 2008; Willis & LaTourette, 2008), as well as the Federal Bureau of Investigation (FBI) and other policing (Mueller & Stewart, 2011a, in press). The specifics of each analysis may vary, as do theories which are dependent on data quality and availability (e.g., Prunckun, 2011). However, the overall objective to maximize NPV remains the same. This is the objective of many decision problems, such as those related to natural hazards mitigation and climate change adaptation (e.g., Hall et al., 2012; Stewart, Wang, & Willgoose, in press).

This process requires the evaluation of six readily understandable considerations; the first three are the components of risk as laid out in Equation (1):

(1) Threat—likelihood of a terrorist attack
(2) Vulnerability—likelihood that the attempted attack is 'successful'
(3) Consequences—consequences of a successful attack
(4) Risk reduction—degree to which the proposed security measure is likely to reduce either the consequences, vulnerability, or the likelihood of a terrorist attack
(5) Co-benefits—benefits of security measure not related to risk reduction
(6) Cost—cost of the proposed security measure, including opportunity costs.

Equation (2) can be expanded to consider multiple threats, hazards and losses, discounting of costs and benefits, interaction between threats and risk reduction, risk aversion (utility theory), etc. The degree of sophistication depends on data and model availability, and detailed systems reliability modeling techniques can be utilized, such as for the effectiveness of multiple layers of aviation security (e.g., Stewart & Mueller, 2013b, 2014). However, indicative results are instructive as a 'first pass' at the problem. This is the approach used in the present paper.

We recognize that perceptions of risk and risk averseness are commonly cited as reasons to overinvest in homeland security measures. Mueller and Stewart (2011b) 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 Australian Office of Best Practice Regulation, US Office of Management and Budget, and other regulatory agencies that strongly recommend risk-neutral attitudes in their decision-making as described by the above equations (e.g., Faber & Stewart, 2003; OBPR, 2010; OMB, 1992; Stewart, 2011; Sunstein, 2002). This entails using mean or average estimates for risk and cost–benefit calculations, and not worst-case or pessimistic estimates.

A key challenge is the prediction of threat probability. A scenario-based approach assesses benefits by simply assuming that threat probability is 100 percent—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 threat probability, particularly in a dynamic threat environment where the threat may arise from an intelligent adversary who will adapt to changing circumstances to maximize 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 & Stewart, 2011a, 2011b, 2012). 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 threat probability or risk reduction needed for a security measure to begin to be cost-effective.

### *Threats*

We consider six specific threat scenarios to airports and aircraft:

Airports:

(1) large vehicle-borne improvised explosive device (VBIED) in non-screened (public) place
(2) small improvised explosive device (IED) in non-screened (public) place
(3) shooting in screened and non-screened areas.

Aircraft:

(4) IED in checked luggage
(5) suicide bomber boards aircraft
(6) hijackers board aircraft (replication of 9/11 type attack).

These threats have been called 'major vulnerabilities' or 'major' threats that can kill a large number of people (Elias, 2010; Stevens et al., 2004). Other threats to airport facilities or aircraft seem unlikely (Stevens et al., 2004).

In the 14-year period 1998–2011, the Global Terrorism Database (GTD) (www.start.umd.edu/gtd/) recorded 20 attempted attacks on airports, large and small, in the USA, Canada, Australia and Europe. Most of these failed to hurt anyone and did no significant damage. In total these incidents resulted in the deaths of 64 people, 37 of them in a single suicide explosion in the baggage claim section at Moscow's Domodedovo airport in 2011. Notable among the other attacks were an attempted, but failed, bombing of the Glasgow international airport in 2007, the shooting of two people at the El Al ticket counter at Los Angeles International Airport (LAX) in 2002, and (later than the database period) the shooting of a Transportation Security Administration officer at LAX in 2013.

Over the same period there were 31 attempted attacks on aircraft. In total, attacks on aviation account for only 0.5 percent of all terrorist attacks, and attacks on airports comprise less than half of these. This experience led the 2007 US National Strategy for Aviation Security to observe that "reported threats to aviation

infrastructure, including airports and air navigation facilities are relatively few". A study of the 54 cases that have come to light since 9/11 in which Islamist terrorists planned, or in many cases vaguely imagined, doing damage in the USA finds only three in which an airport facility was on the target list (Mueller, 2014). There have thus been less than four attacks per year on airports and aircraft in the USA, Canada, Australia, and Europe (which contain well over half of the 43,000 airports in the world), and most of these were failures or inflicted minimal damage. In any given year, each of these airports has something like one chance in five thousand (0.02 percent) of suffering any sort of terrorist attack effort. If we consider only large airports, the threat probability increases to something approaching 0.5 percent per airport per year (Stewart & Mueller, 2014). This suggests that 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 better places to detonate a bomb or undertake an armed attack.

On the other hand, the low frequency may arise because airports, and particularly aircraft, have been made secure by the expensive and extensive security measures in place. The target may have become so hardened that terrorists have been deterred from attacking them—though the actual gain to public safety may be somewhat limited because the terrorists may then simply seek out other lucrative, but less secured, targets among the huge number possible. The goal in this paper, however, is to assess whether adding airport police to the security mix already in place improves airport and airplane security enough to justify the cost of doing so.

The GTD shows that attacks on airports constitute 40 percent of all threats, and 60 percent for attacks on aircraft. Since there are three threat scenarios for airports, the relative threat likelihood for threats 1, 2, and 3 is 13.3 percent (40 percent divided by three), and the relative threat likelihood for threats to aircraft is 20 percent for threats 4, 5, and 6 (60 percent divided by three). In other words, if there is a threat against airports or aircraft, then there is, for example, 20 percent likelihood that the threat is a suicide bomber attempting to board an aircraft. It should be stressed that these are *relative* threats. That is, if the yearly likelihood of a terrorist attack effort on an airport or on an airplane at the airport is one in five thousand, 40 percent of all such threats will be directed at the airports and 60 percent at aircraft.

### *Vulnerability*

The vulnerability is the likelihood that a threat results in a 'successful' attack—i.e., detonation of IED, hijacking, or shooting—and that the desired damaging effect is achieved. The vulnerabilities for the six threats are now discussed and quantified.

Threats 1 and 2: In principle, an IED is relatively simple to design and manufacture if done by well-trained personnel, resulting in reliabilities in excess of 90 percent (Grant & Stewart, 2012). However, the probability of an IED creating a damaging effect (casualties) reduces to 19 percent for terrorists in Western countries where there is less opportunity for IED operational skills to be acquired (Grant & 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. The probability of successful attacks using IEDs increases to 65 percent for terrorists or insurgents in the Middle East (Grant & Stewart, 2012). It should also be noted that, since 9/11, terrorists in the USA have been able to detonate bombs in

only one case (in Boston in 2013) and the same holds for the UK (the bombings of London transport on 7 July 2005).

We assume that for a small IED, where there is less device complexity and placement issues, vulnerability is 30 percent (threat 2). This reduces to 15 percent for complex and large IEDs (threat 1) where placement and timing is more crucial to achieve maximum damaging effects and where both pose substantial difficulties for terrorists. Since, as noted, terrorists seem to have great difficulty detonating even simple bombs, these estimates are likely quite generous overestimates of the capacities of actual terrorists.

Threat 3: A shooting attack is much easier to accomplish because guns and ammunition are generally easier to acquire and detonate than bombs. Hence, a well-trained and coordinated shooting has a high chance of doing some damage (e.g., Mumbai 2008) leading to a high vulnerability of 90 percent.

Threat 4: An IED in checked luggage poses similar challenges as threats 1 and 2. The fabrication of a small, compact IED suitable for concealed placement in luggage is a challenging task, as is its remote detonation. We assume the probability of IED success is 30 percent, and this is consistent with small IEDs associated with threat 2.

Threat 5. There is a likelihood that a suicide bomber will be foiled once on the aircraft—as happened with both the shoe and the underwear bomber. Moreover, an air explosion might well fail to cause the airliner to crash (Mueller & Stewart, 2011b). Modeling by Stewart and Mueller (2011) showed:

- Passengers and trained flight crew have a low 50/50 chance of foiling a terrorist attempting to assemble or detonate an IED.
- Imperfect bomb-making training results in a high 75 percent chance of an IED detonating successfully.
- Aircraft resilience—a 75 percent chance of an airliner crashing if a bomb is successfully detonated.

Hence, the probability than an airliner will be downed by a suicide bomber (assuming they enter the aircraft undetected) is $0.5 \times 0.75 \times 0.75 = 28.1$ percent which we will round up to 30 percent. For more details of this system reliability modeling, see Stewart and Mueller (2011).

Threat 6: The likelihood that a commercial passenger airliner will be commandeered by small bands of terrorists, kept under control for some time, and then crashed into specific targets is small. Stewart and Mueller (2013a, 2013b) developed a system reliability tool to estimate that the probability that existing security measures will deter or foil terrorists prior to boarding is a high 70–90 percent, and that measures on the aircraft to foil, prevent, or deter the hijackers (air marshals, flight crew, passengers, hardened cockpit door) and anti-aircraft measures reduce the remaining risk by 80 percent. In total, with all existing security measures, the probability hijackers could board an airliner undetected and then successfully commandeer the aircraft and crash it into a specific target is well under 10 percent.

### *Consequences*

Losses for the six threats are now described.

Threat 1: A large truck bomb containing 1800 kg of TNT detonated 11 meters 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 Rudy Weisz (2012) working from studies conducted by the Defense Threat Reduction Agency's VAPO program in the USA. Nearly all windows facing the blast would be destroyed, and little of the structure left standing, causing the entire roof to collapse—causing 306 fatalities or severe injuries. In another study, blast pressure modeling from a 400 kg VBIED detonated in the passenger drop-off area of a generic airport predicted approximately 250 fatalities (Lord, Nunes-Vaz, Filinkov, & Crane, 2010). By way of comparison, these scenarios are similar to the 1995 Oklahoma City bombing that killed 165 people, the US 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 percent of bomb attacks had more than 30 fatalities (LaTourrette, Howell, Mosher, & MacDonald, 2006). Assuming an average of 50 fatalities from an on-ground explosion, and based on the value of a single life (VSL) being $6.5 million (Robinson, Hammitt, Aldy, Krupnick, & Baxter, 2010), an economic loss of 50 fatalities comes to $325 million. Morral et al. (2012) conclude that 50 fatalities from an airport attack is 'unrealistically high', but we adopt this figure to be conservative. Moreover, most losses arise from indirect causes, not from fatalities or injuries, and therefore the results are not very sensitive to assumptions about the average numbers of fatalities. Physical damage might average $100 million. 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.

Threat 2: Weisz (2012) concluded that a smaller 45 kg (100 pound) luggage bomb detonated near a check-in counter would also destroy nearly all windows at Dulles international airport, but would inflict considerably less structural damage overall and approximately 10 percent of the fatalities caused by a large truck bomb—that would be about 30 fatalities or severe injuries valued at $200 million. Lord et al. (2010) predicted approximately 100 fatalities from a 36 kg IED detonated in the check-in area of a generic airport. The 2011 suicide bombing at Moscow's Domodedovo airport that killed 37, accomplished with an IED reportedly of 2–5 kg, did cause some flights to be diverted to other airports in Moscow immediately following the attack. However, Domodedovo airport still 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. We will assume a mean loss of $5 billon. For reference, the losses sustained from the 2005 London and the 2004 Madrid bombings which killed 52 and 191 commuters, respectively (where IED size was relatively small), amounted to no more than $5 billion in direct and indirect losses (including loss of life, loss of tourism, business interruption, etc.) (Mueller & Stewart, 2011b). However, a coordinated set of multiple bombings in the center of a city is likely to inflict far greater indirect costs than a single explosion at an isolated airport.

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 & Stewart, 2011b). This suggests that the losses proposed above might be skewed more to lower values, but public fear and averseness to air travel may increase these losses.

Threat 3: The attacks in Mumbai in 2008 bear 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.

Threats 4 and 5: A 2005 RAND study hypothesized 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 attack on the Pentagon on 9/11 caused up to $10 billion in losses counting physical damage, loss of life and indirect losses such as social and business disruptions (Mueller & Stewart, 2011a, 2011b).

The 11 September 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 US economy of the 9/11 attacks ranged from $50 to $150 billion in 2010–2011 dollars (e.g., Mueller & Stewart, 2011b). 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, Moore II, Pak, & Richardson, 2007; IATA, 2011). These losses were mainly due to a 1–5 percent 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 due to the recession.

IATA revenue projections to 2020 show approximately 5 percent 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 traveling public, and might result in no global growth in revenue/passengers for one year (i.e., equivalent to a 5 percent revenue or passenger decrease for one year)—this is a loss of at least $30 billion.

This is an extreme case, however. 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 has not been nearly so extreme as in the aftermath of 9/11. And after two Russian airliners were blown up by suicidal Chechen female terrorists in 2004, that country's airline industry seems 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 traffic had increased by 3.9 percent (IATA, 2010).

And 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. The suicide bomb attack at Moscow's Domodedovo airport also had little impact on Russian airlines; indeed Russian airlines increased passenger numbers in 2011 by 12.6 percent compared to 2010, and international passengers increased by 13.2 percent over the same period (Borondina, 2012). Hence, $30 billion in airline losses is very much an upper value of consequences of a terrorist attack at an airport.

If we take a VSL of $6.5 million, the economic loss caused by 300 fatalities on a downed airliner is approximately $2 billion. If we add the cost of a large commercial airliner of $200–$250 million, the direct economic loss of a luggage bomb or suicide bomber is approximately $2.5 billion if we also include forensic and air transport crash investigations. Death rates lower than 300 will reduce direct losses considerably of course. The economic consequences of a luggage bomb or suicide bomber would likely be less than the shocking events of 9/11, so we will assume that a reasonable medium loss is $25 billion.

Threat 6: If hijackers succeed in commandeering an airliner and crashing it into a target then loss will be considerable. The $10 billion in losses from the 9/11 attack on the Pentagon would be a plausible lower value of economic loss, and $100 billion in losses and equivalent to the 9/11 losses from a single aircraft is a plausible upper bound. A medium loss of $50 billion is thus reasonable.



### *Risk reduction*

Risk reduction is the probability that airport CT policing will deter, prevent, disrupt, or protect against the threat. Because there are many layers of security at airports and in aircraft, the effect of one layer, such as airport CT policing, may be small when compared to the reduction of risk already supplied by the remaining layers of security. For example, a London plot to put bombs on several transatlantic airliners in 2006 was thwarted by police and intelligence work long before the plot was set into motion, as was a plot to ignite fuel lines serving JFK airport in 2007 (Mueller, 2014).

Airport CT policing will have the highest risk reduction for a shooting attack—mainly by reducing its consequences—because police can respond quickly to minimize casualties. VBIED or IED threats are more difficult to prevent or ameliorate than a shooting attack. A visible police presence may have a deterrent effect, but it is unlikely to prevent or disrupt such an attack. Good intelligence would boost such risk reduction.

Airport CT policing is less likely to be effective against attacks on aircraft: hijackings or suicide bombers. However, if the terrorists are detected during passenger screening, prompt action by police is essential to avoid premature detonation of an IED. Again, good intelligence should boost the risk reduction.

To illustrate the cost–benefit analysis, we will consider the sensitivity of NPV calculations to risk reductions from 10 to 100 percent, and the break-even risk reduction needed for airport CT policing to be cost-effective. Expert opinions, 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 & Mueller, 2011, 2013a, 2013b 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, considering a range of risk reductions provides a basis to assess the influence and sensitivity of policy options on risk reduction and the cost-effectiveness of security measures.

### *Co-benefits of airport CT policing*

The co-benefits of CT policing—such as reduction in crime and reassurance to the traveling public—can be substantial. The cost of crime has been estimated to

range from $2000 (theft) to $85,000 (serious assault) to $9,000,000 for homicide (Heaton, 2010). For example, if each CT police officer deters or disrupts one assault, theft or other criminal act once per year at $15,000 per crime averted, then for 300–350 airport CT police officers this gives a co-benefit of approximately $5 million per year.

Data on the effect that visible airport policing has on passengers are scarce. However, a visible police presence may act to reassure the traveling public—although one study (Grosskopf, 2006) concludes that visible security measures directed at terrorism can have the opposite effect of alarming people. If a visible police presence does prove overall to reassure passengers that air travel is safer, this may lead to higher passenger numbers and more revenue for airport operators and airlines. If we assume that airport CT policing contributes to a very modest passenger growth of 0.1 of 1 percent, then, based on Qantas and Virgin Australia revenues of $19.6 billion in 2012, this corresponds to an increase of $19.6 million in revenues for Qantas and Virgin Australia. Other airlines would also benefit, as would airport operators. A co-benefit of $19.6 million is thus an underestimate.

The total co-benefit is therefore the sum of $5 million and $19.6 million, or $24.6 million which we round to $25 million per year.

### *Cost of AFP airport CT policing*

The AFP has seen their budget increase by more than three and a half times (in real terms) from expenditure in 1998–1999 due to the expanded role for the AFP in both CT and peacekeeping operations (Donkin & Bronitt, 2013). The AFP has primary responsibility for policing and security at Australia's ten major airports: Cairns, Brisbane, Gold Coast, Sydney, Canberra, Melbourne, Hobart, Adelaide, Perth, and Darwin. The Australian Government 2009 Beale Review (Beale, 2009) describes the full complement of operational uniformed and non-uniformed Unified Policing Model (UPM) staffing at Australian airports as of 29 May 2009 (see Table 1). AFP airport CT policing is designed to protect airport terminals and aircraft from terrorist attack. The number of AFP or state police at airports with the specific task of CT comprises the CTFR and some 50 percent of the Joint Airport Intelligence Groups (JAIG)—this totals 460 staff or 59 percent of police staffing at airports.

The 2005 Wheeler Review "comprehensively discredited many aspects of Australia's aviation security" and "Airport policing was described by him as 'often inadequate and dysfunctional' with rivalries, lack of coordination of policing agencies and lack of information sharing including between public and private sectors" (Prenzler et al., 2010). The Wheeler Report recommended an overhaul of the airport policing system and the development of a UPM at Australia's 11 major airports (Prenzler et al., 2010; Wheeler, 2005). Recommendations from both the Aviation White Paper (DITRDLC, 2009) and the Beale Review have led the AFP to transition from the UPM to the 'All-In' model of aviation policing and security which allows the airport uniform police and CT and first response to become a homogenized, fully-sworn AFP police officer workforce (e.g., Prenzler et al., 2010). The 2014 Australian Auditor-General report on policing at Australian airports reported that, at 15 November 2013, there were 618 sworn AFP officers at Australian airports, at a direct (salaries) cost of $74.1 million per year (ANAF, 2014).

Table 1. Police staffing levels at 11 airports in Australia in 2009.

| | Description | Staffing |
|---|---|---|
| Airport police commanders | Responsible for the unified command and control of policing at the 11 major airports. | 11 |
| Airport uniform police | Perform general policing duties at airports. Their visible presence also contributes to crime prevention and deterrence efforts. The UPM draws heavily from state and territory police jurisdictions. | 225 |
| CT and first response | Focuses on the deterrence, prevention and response to acts of terrorism and/or unlawful interference to aircraft (hijacking). Sixty-three CTFR members have also been trained to conduct preliminary bomb assessments. | 445 |
| Joint airport investigation teams | Comprising AFP, state/territory police and Australian Customs and Border Protection Service (ACBPS) personnel, targeting serious and organized crime across the aviation network. | 51 |
| Joint airport intelligence groups | Coexist with the JAITs and are jointly staffed by AFP, state/territory police and ACBPS analysts to provide dedicated intelligence support to the UPM. | 31 |
| Police aviation liaison officers | Primary communication conduits between the UPM and the wider aviation industry. These members also provide support to the special processing of dignitaries through airports. | 17 |
| Total | | 780 |

Note: The UPM also includes a national canine program delivering an explosive and firearm detection capability to all designated airports. Regional Rapid Deployment Teams (RRDT), based at Brisbane, Melbourne, Perth, and Sydney, deliver CT awareness training and other security activities.
Source: Adapted from Beale (2009).

The cost of $74.1 million per year also does not include the cost of unsworn staff, and equipment, facilities, depreciation, and other operating costs. The 2014 budget of the AFP is $1.4 billion, and the AFP has 4300 AFP and protective service officers, and 2600 un-sworn staff. If aviation security deploys 618 AFP officers, then this constitutes 15 percent of the AFP total number of police officers—a pro-rata analysis suggests that aviation security has a budget of approximately $200 million per year. This is confirmed by forward estimates for the 2010–2011 Federal Budget that includes $759.4 million over four years for continuation of the UPM for 11 airports (AG, 2010; Yates, 2010)—or $189.85 million per year. We will round this down to $185 million as a result of the AFP withdrawal from Alice Springs Airport that occurred in 2011.

The current number of AFP officers following full implementation of the 'All-In' model is 618, a reduction from the 2009 estimate of 780 (see Table 1). It is not clear whether this reduction is equally shared between community and CT policing. To be conservative, we will round down the proportion of AFP airport policing officers with the specific task of CT from 59 to 50 percent. The cost of airport CT policing at ten airports in Australia is 50 percent of $185 million or approximately $90 million per year.

## Results

The analysis will apply an expected value cost–benefit analysis using single-point estimates and mean values. In principle, a probabilistic analysis could be attempted, such as that described by Stewart and Mueller (2011, 2013b, 2014) for the cost–benefit assessment of in-flight security measures and full-body scanners where risk reduction, vulnerabilities, and losses were treated as random variables. However, in this case, the information required to accurately assess risk reductions is scarce, so a break-even analysis will be conducted using a range of parameter values likely to represent the best and worst cases of threat probabilities and losses. Also note that some results are rounded so as not to imply a precision higher than the precision of input parameters.

Our best estimates of input parameters for the risk analysis are given in Table 2 using open-source empirical data for estimates of vulnerability and consequences. We also include the following as inputs: co-benefits of $25 million per year; cost of security measure of $90 million per year.

Table 3 shows the NPV (or net benefit) for a range of annual threat probabilities and risk reductions. Note that in this case the threat probability is the probability of attack at any large airport in Australia that has AFP airport CT police, and that the threat has not been thwarted by other security or police agencies (or the public). A security measure is cost-effective when NPV is a positive value. An annual threat probability of 100 percent represents one attempted attack per year. Risk reduction is the probability that airport CT policing will deter, prevent, disrupt, or protect against the threat.

If the annual probability of a terrorist attack, successful or not, on one of the ten airports in Australia with CT policing is less than 1 percent (or one in a hundred), there is no net benefit for airport CT policing even if risk reduction is a perfect 100 percent. The security measure consequently fails to be cost-effective. Based on open-sourced data on threats to Australian airports or aircraft, the actual likelihood of a terrorist attack attempt at an Australian airport is zero, or close to it. However, if we lump the country in with the USA, Canada, Europe, and the Asia-Pacific area, the history-based annual threat likelihood rises to 5 percent that any one of the ten major airports in Australia will be attacked (i.e., 0.5 percent per airport per year

Table 2. Best estimates for input parameters.

| Threat | Relative threat likelihood (%) | Vulnerability (%) | Consequences if successful ($ billion) |
|---|---|---|---|
| 1. Large VBIED | 13.3 | 15 | 10 |
| 2. Small IED in public place | 13.3 | 30 | 5 |
| 3. Shooting | 13.3 | 90 | 2 |
| 4. IED in checked luggage | 20.0 | 30 | 25 |
| 5. Suicide bomber boards aircraft | 20.0 | 30 | 25 |
| 6. Hijacker boards aircraft | 20.0 | 20 | 50 |

Table 3. Net benefit (NPV) in millions of dollars for AFP airport CT policing costing $90 million per year.

| Annual probability of attack in the absence of airport CT policing (%) | Risk reduction from airport CT policing | | | | |
|---|---|---|---|---|---|
| | 25% | 50% | 75% | 90% | 100% |
| 0.01 | −$65 | −$65 | −$65 | −$64 | −$64 |
| 0.1 | −$64 | −$62 | −$61 | −$60 | −$59 |
| 1 | −$51 | −$37 | −$23 | −$14 | −$9 |
| 5 | $5 | $76 | $146 | $189 | $217 |
| 10 | $76 | $217 | $358 | $443 | $499 |
| 50 | $640 | $1345 | $2050 | $2473 | $2755 |
| 100[a] | $1345 | $2755 | $4165 | $5011 | $5575 |
| 200 | $2755 | $5575 | $8395 | $10,087 | $11,215 |

[a]Denotes one attack per year. A value of –$65 denotes no benefit.

multiplied by ten airports). If risk reduction is 50 percent, an annual threat probability of 5 percent yields an NPV of $76 million per year, and the BCR is 1.84. At that level, airport CT policing for the ten airports would be cost-effective, and $1 of cost would buy $1.84 in benefits. The net benefit increases with increasing risk reduction and threat likelihood. Airport CT policing for the ten airports would begin to be cost-effective if minimum risk reduction is 25 percent and when the annual threat probability exceeds 5 percent or one attack every 20 years. It should be kept in mind in all this that many threats against the aviation industry would be deterred, foiled, or prevented by other (non-airport) police and security measures (as well as by public awareness and response, etc.).

Figure 1 shows the break-even (minimum) risk reduction for airport CT policing to be cost-effective as a function of the annual threat probability. Clearly, if that threat probability is 5 percent per year, risk reduction must exceed 23 percent for airport CT policing to begin to be cost-effective. If the annual threat probability is less than 1 percent, risk reduction would need to exceed 100 percent, which is not feasible, and so airport CT policing would not be cost-effective under that condition.

As discussed above, there is uncertainty with many of the input parameters. It follows from Equation (2) that net benefit is proportional to risk reduction, loss, and vulnerability. Hence, a doubling of either of these parameters will nearly double net benefit. The relative threat likelihoods given in Table 2 may also be uncertain. For example, if it is believed that airport policing is aimed at airport threats only, then the relative threat likelihood for threats 1, 2, and 3 would be 33.33 percent, and 0 percent for other (aircraft) threats. On the other hand, if airport policing is in place to deal mainly with threats to aircraft, then the relative threat likelihood for threats 4, 5, and 6 would be 33.33 percent. Figure 2 shows the minimum risk reduction for the airport CT policing to be cost-effective for these scenarios. If airport threats are considered, then Figure 2 shows that the break-even risk reduction increases from 23 to 81 percent, for a 5 percent annual threat probability. However, threats to aircraft reduce the break-even risk reductions by no more than 20 percent. Clearly, the benefits of risk reduction to threats against aircraft are higher than for threats against airports, mostly because of the higher losses that would result from a successful attack against an aircraft.

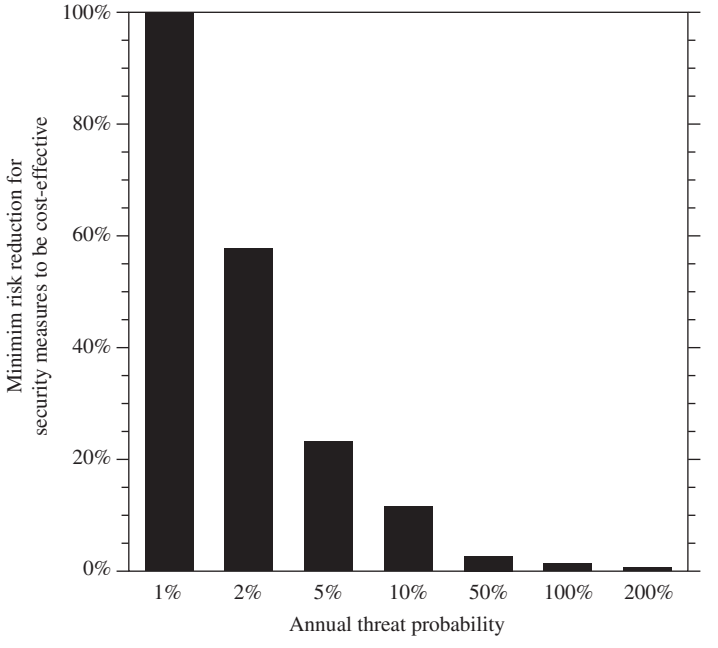


Figure 1. Minimum (break-even) risk reduction required for airport CT policing to be cost-effective.

The observation that airport CT policing may not be cost-effective under some combinations of risk reduction and threat probability informs us that spending $90 million to achieve such a risk reduction would not be cost-effective. It does not follow that zero spending on airport CT policing is thus cost-effective, or the preferred policy option. Security measures that are at once effective and relatively inexpensive are generally the first to be implemented—for example, one erects warning signs on a potentially dangerous curve in the road before rebuilding the highway. So the first dollars spent on CT measures are likely to be worthwhile, even if the last is not. It follows that reduced spending, even if it reduces the risk reduction, may increase the marginal level of cost-effectiveness. For example, if CT and First Response (CTFR) personnel are reduced by 25 percent to 335 personnel (see Table 1), then the AFP airport policing budget would also decrease by close to 25 percent to $67.5 million per year. The break-even risk reduction with full ($90 million) expenditure is 58 percent for a 2 percent threat probability (see Figure 1). However, the break-even risk reduction reduces nearly threefold to 20 percent if cost of security reduces by only 25 percent to $67.5 million. In this case, a break-even risk reduction of 20 percent may be easier to achieve (or justify) even though the cost of the security measure is less. Or put another way, increasing risk reduction threefold from 20 to 58 percent may be challenging to achieve for an additional outlay of only $22.5 million. Clearly, there are various policy options available with differing costs and risk reductions. The risk and cost–benefit framework described herein provides one approach to weighing the costs and benefits of each policy option.

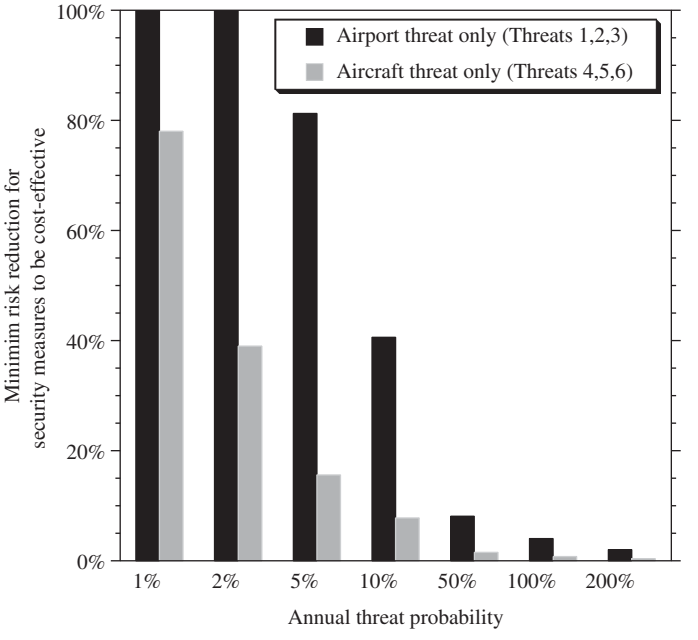


Figure 2. Effect of relative threat likelihood on minimum risk reductions for airport CT policing to be cost-effective.

Moreover, the co-benefit of CT airport policing may well exceed $25 million per year, particularly if CT airport policing is able to utilize number plate recognition capability, photo ID of passengers, etc. to apprehend people with outstanding criminal issues. If a security measure also enhances the passenger experience more than we have assumed, there would be an additional co-benefit, dramatically improving the measure's cost-effectiveness.

## Conclusions and further work

This paper sets out the basic principles of risk and cost–benefit analysis. These principles are applied to airport CT policing provided by the AFP. The results are preliminary, and based on our 'best estimates' using publicly sourced material. This provides a starting point for this type of risk analysis. The preliminary results show the combinations of risk reduction and threat probability that allow airport CT policing to be cost-effective. For example, airport CT policing begins to become cost-effective if it reduces risk by approximately 25 percent and if the probability of an attack at any airport in Australia exceeds 5 percent per year. The co-benefits of airport CT policing—such as reduction in crime and reassurance to the traveling public—might be considerable, and could dramatically improve the cost-effectiveness of airport CT policing. Further work should focus on more comprehensive threat scenarios, the layers of airport security and their interactions and interdependencies, analysis of operational data on effectiveness of airport CT policing, and improved cost data including co-benefits. The scope can also be broadened to encompass all airport police, their rates of crime deterrence and prevention, and

propose how airport policing may be made more effective/efficient such as number plate recognition capability, photo ID of passengers, etc.

**Acknowledgments**

The support of the Australian Research Council is gratefully acknowledged. This paper is an expanded version of a Working Paper published by the ARC Centre of Excellence in Policing and Security (CEPS). The authors are grateful to Prof. Simon Bronitt, Dr Ruth Delaforce, and Dr Tim Legrand from CEPS for their reviews of the working paper manuscript.



**References**

ANAF. (2014). *Policing at Australian international airports*. The Auditor-general Audit Report No. 23, 2013–14 performance audit. Australian National Audit Office. Canberra: Australian Government.

Australian Government. (2010). *Budget paper no. 2. Budget measures 2010–2011. Part 2: Expense measures*. Canberra: Author.

Borondina, P. (2012, February 10). Russian airlines passenger traffic up 12.6%, load factor down in 2011. *Air Transport World*.

Beale, R. (2009, June 30). *New realities: National policing in the 21st century*. Federal Audit of Police Capabilities. Report to Minister for Home Affairs, the Hon, Brendan O'Connor MP.

Chow, J., Chiesa, J., Dreyer, P., Eisman, M., Karasik, T. W., Kvitky, J., … Shirley, C. (2005). *Protecting commercial aviation against the shoulder-fired missile threat*. Santa Monica, CA: RAND Corporation.

DITRDLC. (2009). *National aviation policy white paper: Flight path to the future*. Department of Infrastructure, Transport. Regional Development and Local Government. Canberra: Australian Government.

Donkin, S., & Bronitt, S. (2013). Critical perspectives on the evaluation of counter-terrorism strategies: Counting the costs of the 'war on terror' in Australia. In A. Masferrer & C. Walker (Eds.), *Counter-terrorism, human rights and the rule of law: Crossing legal boundaries in defence of the state* (pp. 169–188). Cheltenham: Edward Elgar.

Dossetor, K. (2011). *Cost-benefit analysis and its application to crime prevention and criminal justice research*. AIC Reports Technical and Background Paper 42. Canberra: Australian Institute of Criminology.

Elias, B. (2010). *Airport and aviation security: U.S. policy and strategy in the age of global terrorism*. Boca Raton: CRC Press.

Faber, M. H., & Stewart, M. G. (2003). Risk assessment for civil engineering facilities: Critical overview and discussion. *Reliability Engineering and System Safety*, *80*, 173–184. doi:10.1016/S0951-8320(03)00027-9

George, B., & Whatford, N. (2007). Regulation of transport security post 9/11. *Security Journal*, *20*, 158–170. doi:10.1057/palgrave.sj.8350062

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 Analysis*, *27*, 505–512. doi:10.1111/j.1539-6924.2007.00903.x

Grant, M., & Stewart, M. G. (2012). A systems model for probabilistic risk assessment of improvised explosive device attack. *International Journal of Intelligent Defence Support Systems*, *5*(1), 75–93. doi:10.1504/IJIDSS.2012.053664

Grosskopf, K. R. (2006). Evaluating the societal response to antiterrorism measures. *Journal of Homeland Security and Emergency Management*, *3*, 1547–7355. doi:10.2202/1547-7355.1170

Hall, J. W., Brown, S., Nicholls, R. J., Pidgeon, N. F., & Watson, R. T. (2012). Proportionate adaptation. *Nature Climate Change*, *2*, 833–834. doi:10.1038/nclimate1749

Heaton, P. (2010). *Hidden in plain sight: What cost-of-crime research can tell us about investing in police*. Santa Monica, CA: RAND Corporation.

International Air Transport Association. (2010, March 2). *Facts and figures*. Pressroom: Author.

International Air Transport Association. (2011). *The impact of September 11 2001 on aviation*. Geneva: Author.
International Air Transport Association. (2012). *2012 Annual review*. Geneva: Author.
International Standards Organization 31000. (2009). *Risk management — Principles and guidelines*. Geneva: Author.
Jackson, B. A., LaTourrette, T., Chan, E. W., Lundberg, R., Morral, A. R., & Frelinger, D. R. (2012). *Efficient aviation security*. Santa Monica, CA: RAND Corporation.
Jacobson, S. H., Karnani, T., Kobza, J. E., & Ritchie, L. (2006). A cost-benefit analysis of alternative device configurations for aviation checked baggage security screening. *Risk Analysis*, *26*, 297–310. doi:10.1111/j.1539-6924.2006.00736.x
LaTourrette, T., Howell, D. R., Mosher, D. E., & MacDonald, J. (2006). *Reducing terrorism risk at shopping centers: An analysis of potential security options*. Santa Monica, CA: RAND Corporation.
Lord, S., Nunes-Vaz, R., Filinkov, A., & Crane, G. (2010). Airport front-of-house vulnerabilities and mitigation options. *Journal of Transportation Security*, *3*, 149–177. doi:10.1007/s12198-010-0045-0
McFarlane, J. (2007). The thin blue line: The strategic role of the Australian Federal Police. *Security Challenges*, *3*(3), 91–108.
Morral, A. R., Price, C. C., Oritz, D. S., Wilson, B., LaTourrette, T., Mobley, B. W., … Willis, H. H. (2012). *Modeling terrorism risk to the air transportation system*. Santa Monica, CA: RAND Corporation.
Mueller, J. (2014). *Terrorism since 9/11: The American cases*. Retrieved from http://politicalscience.osu.edu/faculty/jmueller/since.html
Mueller, J., & Stewart, M. G. (2011a). The price is not right: The U.S. spends too much money to fight terrorism. *Playboy*, *58*, 149–150.
Mueller, J., & Stewart, M. G. (2011b). *Terror, security, and money: Balancing the risks, benefits, and costs of homeland security*. New York, NY: Oxford University Press.
Mueller, J., & Stewart, M. G. (2012). The terrorism delusion: America's overwrought response to September 11. *International Security*, *37*(1), 81–110. doi:10.1162/ISEC_a_00089
Mueller, J., & Stewart, M. G. (in press). Evaluating counterterrorism spending. *Journal of Economic Perspectives*.
NRC. (2010). *Review of the department of homeland security's approach to risk analysis*. National Research Council of the National Academies. Washington, DC: National Academies Press.
OBPR. (2010). *Best practice regulation handbook*. Office of Best Practice Regulation. Canberra: Australian Government.
Office of Management and Budget. (1992). Guidelines and discount rates for benefit-cost analysis of federal programs (revised), Circular No. A-94, October 29, 1992. Washington, DC: Author.
Poole, R. W. (2008, December 11–12). *Towards risk-based aviation security policy*. Discussion Paper No. 2008–23, OECD/ITF Round Table on Security, Risk Perception and Cost-benefit Analysis, International Transport Forum.
Prenzler, T., Lowden, C., & Sarre, R. (2010). Aviation security issues in Australia post-9/11. *Journal of Policing, Intelligence and Counter Terrorism*, *5*(2), 9–22. doi:10.1080/18335300.2010.9686946
Prunckun, H. (2011). A grounded theory of counterintelligence. *American Intelligence Journal*, *29*(2), 6–15.
Rekiel, J., & de Wit, J. (2013). The security system at European airports Tour d'Horizon. *Journal of Transportation Security*, *6*(2), 89–102. doi:10.1007/s12198-013-0105-3
Robinson, L. A., Hammitt, J. K., Aldy, J. E., Krupnick, A., & Baxter, J. (2010). Valuing the risk of death from terrorist attacks. *Journal of Homeland Security and Emergency Management*, *7*, 1547–7355. doi:10.2202/1547-7355.1626
Stewart, M. G., Ellingwood, B. R., & Mueller, J. (2011). Homeland security: A case study in risk aversion for public decision-making. *International Journal of Risk Assessment and Management*, *15*, 367–386. doi:10.1504/IJRAM.2011.043690
Stewart, M. G., & Melchers, R. E. (1997). *Probabilistic risk assessment of engineering systems*. London: Chapman & Hall.

Stewart, M. G., & Mueller, J. (2008). A risk and cost-benefit assessment of U.S. aviation security measures. *Journal of Transportation Security*, *1*(3), 143–159. doi:10.1007/s12198-008-0013-0

Stewart, M. G., & Mueller, J. (2011). Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. *Journal of Homeland Security and Emergency Management*, *8*(1), 30.

Stewart, M. G., & Mueller, J. (2013a). Terrorism risks and cost-benefit analysis of aviation security. *Risk Analysis*, *33*, 893–908. doi:10.1111/j.1539-6924.2012.01905.x

Stewart, M. G., & Mueller, J. (2013b). Aviation security, risk assessment, and risk aversion for public decision-making. *Journal of Policy Analysis and Management*, *32*, 615–633. doi:10.1002/pam.21704

Stewart, M. G., & Mueller, J. (2013c, October). *Cost-benefit analysis of Australian Federal Police counter-terrorism operations at Australian airports*. CEPS Working Paper, ARC Centre of Excellence in Policing and Security, Issue 2.

Stewart, M. G., & Mueller, J. (2014). Cost-benefit analysis of airport security: Are airports too safe? *Journal of Air Transport Management*, *32*, 615–633.

Stewart, M. G., Wang, X., & Willgoose, G. R. (in press). Direct and indirect cost and benefit assessment of climate adaptation strategies for housing for extreme wind events in Queensland. *Natural Hazards Review*.

Stevens, D., Schell, T., Hamilton, T., Mesic, R., Brown, M. S., Wei-Min Chan, E., … Harris, E. (2004). *Near-term options for improving security at Los Angeles International Airport*. Santa Monica, CA: RAND Corporation.

Sunstein, C. R. (2002). *The cost-benefit state: The future of regulatory protection*. Chicago, IL: American Bar Association.

Tulich, T. (2012). Prevention and pre-emption in Australia's domestic anti-terrorism legislation. *International Journal for Crime and Justice*, *1*(1), 52–64.

Walker, B. (2012). *Declassified annual report. Independent National Security Legislation Monitor*. Canberra: Australian Government.

Weisz, R. G. (2012). *America's lack of airport security. 2012 critical infrastructure symposium*. Arlington, TX: Virginia.

Wheeler, J. (2005). *An independent review of airport security and policing for the Government of Australia*. Airport Security and Policing Review. Canberra: Commonwealth of Australia.

Willis, H., & LaTourette, T. (2008). Using probabilistic terrorism risk-modeling for regulatory benefit-cost analysis: Application to the western hemisphere travel initiative in the land environment. *Risk Analysis*, *28*, 325–339. doi:10.1111/j.1539-6924.2008.01022.x

Willis, K., Anderson, J., & Homel, P. (2011). Measuring the effectiveness of drug law enforcement. *Trends and Issues in Crime and Criminal Justice*. Canberra: Australian Institute of Criminology, 406.

Yates, A. (2010, May 13). *Domestic & national security budget analysis: 2010–11 federal budget*. Canberra: Australian Security Research Centre.

Zycher, B. (2003). *A preliminary benefit/cost framework for counterterrorism public expenditures*. Santa Monica, CA: RAND Corporation.