Working paper

CEPS ARC Centre of Excellence in Policing and Security

October 2013
>Issue 2

The terrorist attacks of 11 September 2001 highlighted the vulnerabilities of airports and aircraft. Further attacks in 2002, 2007 and 2009, have led to major government reforms in passenger processing and airport access. The security of Australian airports has also followed this trend, with an increased police presence. However, limited consideration has been given to the costs of these measures, compared to benefit. This Working Paper identifies the factors to be considered in such cost-benefit analyses and the authors outline their preliminary findings. The scope for further research is highlighted, particularly in relation to risk analysis and cost.

R. Delaforce

Dr Ruth Delaforce
Editor
CEPS Adjunct Fellow

Cost-Benefit Analysis of Australian Federal Police Counter-Terrorism Operations at Australian Airports

Professor Mark G. Stewart and Professor John Mueller

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 2002, 2006 and 2009. 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, U.S. Office of Management and Budget, and other regulatory agencies strongly recommend risk and cost-benefit assessments of major programmes. 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. This Working Paper seeks to assess the risks and cost-effectiveness of Australian Federal Police (AFP) airport counter-terrorism (CT) policing designed to protect airport terminals and aircraft from terrorist attack.

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.

2. AUSTRALIAN FEDERAL POLICE AND AVIATION SECURITY

The AFP has primary responsibility for policing and security at Australia's 10 major airports, namely Cairns, Brisbane, Gold Coast, Sydney, Canberra, Melbourne, Hobart, Adelaide, Perth, and Darwin. The 2009 Beale Review describes the full complement of operational uniformed and non-uniformed Unified Policing Model staffing as at 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 counter-terrorism (CT) comprises the Counter-Terrorism First Response (CTFR) and 50% of the Joint Airport Intelligence Groups (JAIG) - this totals 460 staff or 59% of police staffing at airports.

Recommendations from both the Aviation White Paper (2010) and the Beale Review (2009) have led the AFP to transition from a Unified Policing Model (UPM) to the 'All-In' Model of Aviation policing and security. The 'All-In' model allows the airport uniform police and CFTR to transition into a homogenised, fully-sworn AFP police officer workforce. The Senate Standing Committee on Legal and Constitutional Affairs hearing on 24 May 2012 noted that, following full implementation of the 'All-In' model, the final number of AFP officers would be 657, at an estimated direct (salaries) cost of approximately $80 million per year . This does not include the national canine program. It is also noted that, in December 2011, the AFP withdrew from Alice Springs Airport.

The cost estimate of $80 million per year also does not include the cost of unsworn staff, and equipment, facilities, depreciation and other operating costs. The AFP's 2012 budget is $1.289 billion, its personnel complement being 4,157 AFP and protective service officers, and 2,386 unsworn staff. If aviation security deploys 657 AFP officers, then this constitutes 15.8% of the total number of AFP 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 2010-11 Federal Budget that includes $759.4 million over 4 years for continuation of the Unified Policing Model 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 in 2011.

Following full implementation of the 'All-In' model, the final number of AFP officers is 657, a reduction from the 2009 estimate of 780 (see Table 1). It is not clear whether this reduction is equally shared between community and counter-terrorism policing. We will assume that the proportion of AFP airport policing officers with the specific task of counter-terrorism is 50%. The cost of airport CT policing at 10 airports in Australia is 50% of $185 million, or approximately $90 million per year.

	Description	Staffing
Airport Police Commanders	Responsible for the unified command and control of policing at the eleven 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
Counter-Terrorism 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, target serious and organised 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 Unified Policing Model 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 counterterrorism awareness training and other security activities

Table 1. Police Staffing Levels at 11 Airports in Australia (adapted from Beale 2009).

3. COST-BENEFIT ANALYSIS

The standard definition of risk is:

(Risk) = (Threat) X (Vulnerability) X (Consequences)

where

- Threat - annual probability there will be a terrorist attempt
- Vulnerability - 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 - loss or consequence (economic costs, number of people harmed) if the attack is successful in causing damage.

This is consistent with the conceptual framework adopted by the U.S. Department of Homeland Security (NRC 2010) and risk analyses for many applications (e.g., Stewart and Melchers 1997). Security measures should result in risk reduction that may arise from a combination of reduced likelihood of threat, vulnerability or consequences. For any security measure the risk reduction can vary from 0% to 100% (or even a negative number for an ill-suited security measure). A security measure is cost-effective when the benefit outweighs the costs of providing the security measure - i.e., the benefit-to-cost ratio exceeds one.

$$\text{Benefit-to-Cost Ratio} = \frac{\text{Benefit}}{\text{Cost}}$$

$$= \frac{\text{(Risk) X (Reduction in Risk Generated by the Security Measure) + (Co-Benefits)}}{\text{(Cost of Security Measure)}}$$

The *reduction in risk* is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack. The *benefit* of a security measure is the sum of the losses averted due to the security measure and, any expected co-benefit from the security measure not directly related to mitigating vulnerability or threat (such as reduction in crime, improved passenger experience, etc). This benefit is then compared to the cost of the security measure which should include opportunity costs. A security measure is cost-effective if the benefit exceeds the cost.

In essence, this process requires the evaluation of six readily-understandable considerations:

1. Threat - likelihood of a terrorist attack
2. Vulnerability - likelihood that a threat results in a 'successful' attack
3. Consequences - consequences of a successful terrorist 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

The Australian Office of Best Practice Regulation (OBPR), U.S. Office of Management and Budget (OMB) and other regulatory agencies strongly recommend risk-neutral attitudes in their decision-making as described by the above equations (e.g., OBPR 2010, OMB 1992, Faber and Stewart 2003, Sunstein 2002, Stewart et al. 2011). This entails using mean or average estimates for risk and cost-benefit calculations, and not worst-case or pessimistic estimates.

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 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, 2012). In most cases, target selection for perpetrators may not be random, but this would essentially be the case for people trying to anticipate and counter 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 be cost-effective.

3.1 Threats

We consider six threats to airports and aircraft:

- Airports:
  1. large Vehicle-Borne Improvised Explosive Devices (VBIEDs) in non-screened (public) place
  2. small Improvised Explosive Devices (IEDs) 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 boards 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 (Stevens et al. 2004, Elias 2010). Other threats to airport facilities or aircraft seem unlikely (Stevens et al. 2004).

In the fourteen year period 1998-2011, the Global Terrorism Database[1] recorded 20 attacks on airports, large and small, in the U.S., Canada, Australia, and Europe. Most of these hurt no one 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 and the shooting of two people at the El Al ticket counter at Los Angeles International Airport in 2002 (Campbell 2002, Townsend et al 2007).

Over the same period there were 31 attacks on aircraft. In total, attacks on aviation account for only 0.5% of all terrorist attacks, and attacks on airports comprise less than half of these. This experience led the 2007 U.S. National Strategy for Aviation Security to observe that 'reported threats to aviation infrastructure (including) airports and air navigation facilities … are relatively few' (p 11). A study of the 53 cases that have come to light since 9/11 in which Islamist terrorists planned, or in many cases vaguely imagined, doing damage in the United States finds only one in which an airport facility was on the target list (Mueller 2013). It should also be noted that, since 9/11, only one attack consisting of two explosions has occurred in the United States (Boston 2013) and - except for the four bombs on the Underground in London in 2005 - none in the United Kingdom (Mueller and Stewart 2011b). 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 far better places to detonate a bomb or undertake an armed attack.

We assume that attacks on airports constitute 40% of all threats, and 60% for attacks on aircraft. Since there are three threat scenarios for airports then the relative threat likelihood for threats 1, 2 and 3 is 13.3% (40% divided by three), and the relative threat likelihood for threats to aircraft is 20% for threats 4, 5 and 6 (60% divided by three). In other words, if there is a threat against airports or aircraft, then, for example, there will be a 20% likelihood that the threat is a suicide bomber attempting to board an aircraft.

3.2 Vulnerability

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.

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% (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. The probability of successful attacks using IEDs increases to 65% for terrorists or insurgents in the Middle East (Grant and Stewart 2012).

We assume that, for a small IED where there is less device complexity and placement issues, vulnerability is 30% (threat 2). This reduces to 15% 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.

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 vulnerability of 90%.

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%, which is consistent with small IEDs associated with threat 2.

5. There is a very high likelihood that a suicide bomber will be foiled once on the aircraft – as happened with both the 'shoe' and the 'underwear' bombers. Moreover, an air explosion might well fail to cause the airliner to crash (Stewart and Mueller 2011b). Nonetheless, we assume that (Stewart and Mueller 2011):

- 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 high 75% chance of IED detonating successfully.

1 The Global Terrorism Database is developed by the U.S. National Consortium for the Study of Terrorism and Responses to Terrorism (START). It contains country-by-country information for more than 80,000 terrorist incidents that have taken place throughout the world between 1970 and 2011. See http://www.start.umd.edu/gtd/

- Aircraft resilience - a 75% chance of an airliner crashing if a bomb is successfully detonated.

Hence, under these generous assumptions, the probability than an airliner will be downed by a suicide bomber (assuming they enter the aircraft undetected) is 0.5 × 0.75 × 0.75 = 28.1% which we will round up to 30%.

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) show that the probability that existing security measures will deter or detect terrorists prior to boarding is a high 70-90%, 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 reduces the remaining risk by 80%. In total, with existing security measures, the probability that hijackers could board an airliner undetected and then successfully commandeer the aircraft and crash it into a specific target is only about 20%.

3.3 Consequences

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 9/11 attack on the Pentagon caused up to $10 billion in losses including physical damage, loss of life and indirect losses such as social and business disruptions (Mueller and Stewart 2011a, 2011b).

The September 11, 2001, attack directly resulted in the deaths of nearly 3,000 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 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 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 it should be noted that losses from 9/11 were also magnified due to a later 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 might result in no global growth in revenue/passengers for one year (ie. equivalent to a 5% 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 1988 Lockerbie tragedy notable among them - but the response by the flying public has not been nearly so extreme as in the aftermath of 9/11. While 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, which has been attributed mainly to the 60 percent increase in fuel prices. By the following year, passenger traffic had increased by 3.9 percent (IATA 2010).

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% compared to 2010, and international passengers increased by 13.2% 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.

1. 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 United States - a large truck bomb containing 1,800 kg of TNT detonated 11 m from the front wall of Dulles International Airport near Washington D.C. would wreak 'immense destruction'. Nearly all windows facing the blast would be destroyed, and little of the structure would be left standing, thereby causing the entire roof to collapse; estimated fatalities being 306, or many with severe injuries. By way of comparison, this scenario is similar to the 1995 Oklahoma City bombing that killed 165 people, the 1998 U.S. Embassy attack in Kenya that killed 213 people, and the 2008 truck bombing of the Islamabad Marriott Hotel that resulted in 54 deaths. 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 result in more than 30 fatalities (LaTourrette et al. 2006).

   Assuming an on-ground explosion would cause an average of 50 fatalities, and based on the value of a single life (VSL) being $6.5 million (Robinson et al. 2010), an economic loss of 50 fatalities totals $325 million. Morral et al. (2012) conclude that 50 fatalities from an airport attack is 'unrealistically high,' but we adopt this figure to be slightly 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, and so on, 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 billion to $10 billion. A mean total loss of $10 billion is reasonable.

2. Weisz (2012) concluded that a smaller 45 kg (100 pound) luggage bomb detonated near a check-in counter would also destroy nearly all the windows at Dulles International Airport, but inflict considerably less structural damage overall, with approximately 10% of the fatalities caused by a large truck bomb; this would represent about 30 fatalities or severe injuries valued at $200 million. The 2011 suicide bombing at Moscow's Domodedovo airport that killed 37, reportedly accomplished with an IED of 2-5 kilograms, 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 compared to 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 and Stewart 2011b). However, 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.

It should be noted that airports sprawl, are only two or three stories high and therefore damage to a portion is unlikely to be nearly as significant as damage to a taller or more compact structure. Moreover, if a bomb does explode 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 impact on the essential function of the airport would be comparatively modest (Mueller and 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.

3. The attacks 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.

4. and 5. If we take a VSL of $6.5 million, then the economic loss caused by 300 fatalities on a downed airliner is approximately $2 billion. Added to this is the cost of a large commercial airliner, of $200 million to $250 million. If we also include forensic and air transport crash investigations, the direct economic loss of a luggage bomb or suicide bomber is approximately $2.5 billion. 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.

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 Pentagon attack 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.

3.4 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 risk reduction already supplied by the remaining security layers. For example, a 2006 London plot to put bombs on several transatlantic airliners was thwarted by police and intelligence work long before the plot was set into motion, as was a 2007 plot to ignite fuel lines serving JFK airport (Mueller 2013).

Airport CT policing will have the highest risk reduction for a shooting attack - mainly by reducing its consequences - because police can respond quickly to minimise 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, i.e. hijackings or suicide bombers. However, if the terrorists are detected during passenger screening, prompt police action 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 assume that CT policing reduces risk identically for all six threats. We will also generously assume a risk reduction of ΔR=50% for each threat. That is, we will assume, for each of the six threats, that airport CT policing will reduce by 50% whatever residual risk remains after all other security measures have had their risk-reducing effect. This is likely to be 50% of a rather small number for Threats 4, 5 and 6, and 50% of a larger one for Threats 1, 2, and 3.

We have relied on 'best guess' risk reductions. However, 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 (see Stewart and 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, the risk reductions noted in Table 2 provides a basis to assess the influence and sensitivity of policy options on risk reduction and the cost-effectiveness of security measures.

3.5 Co-Benefits of Airport CT Policing

The co-benefits of CT policing - such as reduction in crime and reassurance to the travelling public - can be substantial. The cost of crime ranges from $2,000 (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 is scarce, although a visible police presence may act to reassure the travelling public. However, one study (Grosskopf 2006) concludes that visible security measures directed at terrorism can have the opposite effect, by 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% 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. Therefore, a co-benefit of $19.6 million is an under-estimate. 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.

4. RESULTS

Our best estimates of the risk analysis input parameters are given in Table 2. We also include the following as inputs:

- Cost of Security Measure = $90 million per year
- Co-Benefits = $25 million per year

Threat	Relative Threat Likelihood	Vulnerability	Risk Reduction from Airport CT Policing	Consequences ($ billion)
1. large VBIED	13.3%	15%	50%	10
2. small IED in public place	13.3%	30%	50%	5
3. shooting	13.3%	90%	50%	2
4. IED in checked luggage	20.0%	30%	50%	25
5. suicide bomber boards aircraft	20.0%	30%	50%	25
6. hijackers boards aircraft	20.0%	20%	50%	50

Table 2. "Best Estimates" for Input Parameters.

Table 3 shows the benefit-to-cost ratio (BCR) generated for airport CT policing and a range of annual threat probabilities. 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 BCR exceeds one.
and security measures (as well as by public awareness and response, etc.).

If the annual threat probability at all airports in Australia is less than 1% (or one in a hundred) the BCR for airport CT policing is significantly less than one, and the security measure consequently fails to be cost-effective by a considerable margin. However, a threat probability of 50% (or one attack every two years) would yield a BCR of 15.8 and airport CT policing would be cost-effective under that condition, and $1 of cost would buy $15.80 in benefits. Table 3 shows that airport CT policing would also be cost-effective when the annual threat probability exceeds 5% or one attack every 20 years - that is, it would have to be solely responsible for deterring, foiling, or protecting against one threat every twenty years for the security measures to be cost-effective. It also needs to be kept in mind 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.).

Annual Threat Probability Annual Probability of a Successful or Unsuccessful Attack at any Australian Airport in the Absence of Airport CT Policing	Benefit-to-Cost Ratio
0.1 percent	0.31
1 percent	0.59
5 percent	1.83
10 percent	3.39
25 percent	8.06
50 percent	15.8
100 percent[1]	31.4
200 percent	62.5

1 one attack per year

Table 3. Benefit-to-Cost Ratio for Airport CT Policing.

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

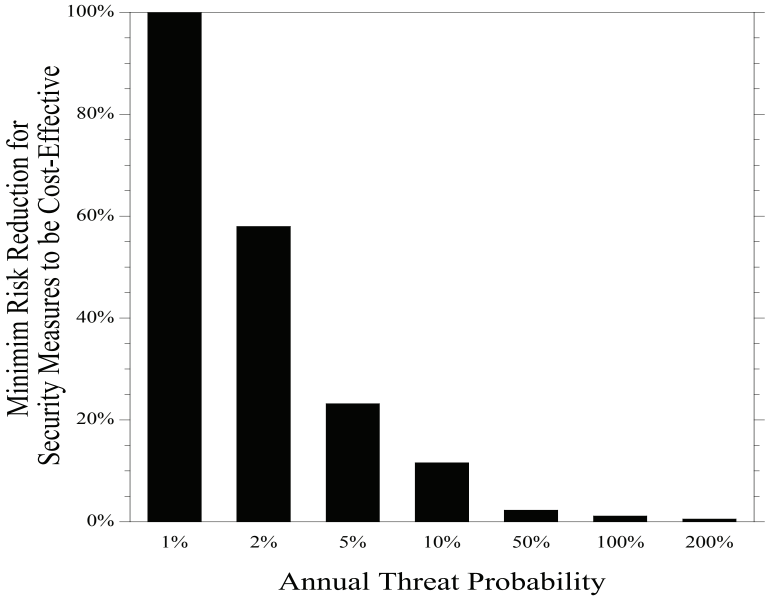

Figure 1. Minimum Risk Reduction Required for Airport CT Policing to be Cost-Effective.

The co-benefit of CT airport policing may well exceed $25 million per year, particularly if CT airport policing is able to utilise number plate recognition capability, passenger photograph identification and other measures to apprehend people with outstanding criminal issues. If a security measure also enhances the passenger experience, there would be an additional co-benefit, dramatically improving the measure's cost-effectiveness.

5. CONCLUSIONS AND FURTHER WORK

This Working 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, and are 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 is cost-effective if it reduces risk by approximately 25% and that the probability of an attack at any airport in Australia exceeds 5% per year. The co-benefits of airport CT policing - such as reduction in crime and reassurance to the travelling public - can be considerable, and will dramatically improve the cost-effectiveness of airport CT policing. Further work should focus on more comprehensive threat scenarios; the layers of airport security, interactions and interdependencies; analysis of operational data on effectiveness of airport CT policing; and improved cost data, including co-benefits. The scope could 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 by the use of other security measures, for example, number plate recognition capability and passenger photograph identification ID.

REFERENCES

Australian Government 2010. *Budget Paper No. 2. Budget Measures 2010-2011, Part 2: Expense Measures.* Canberrra: Australian Government.

Borondina P (10 February 2012). 'Russian Airlines Passenger Traffic Up 12.6%, Load Factor Down in 2011.' *Air Transport World.*

Beale R (30 June 2009). *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.

Campbell D (5 July 2002). 'El Al Guard Kills US Airport Gunman.' *The Guardian.*

Chow J, J Chiesa, P Dreyer, M Eisman, TW Karasik, J Kvitky, S Lingel, D Ochmanek & C Shirley (2005). *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat.* Santa Monica, Ca: RAND Corporation.

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

Faber MH & MG Stewart (2003). 'Risk Assessment for Civil Engineering Facilities: Critical Overview and Discussion.' *Reliability Engineering and System Safety,* 80(2),173-184.

Gordon, P., Moore II J.E., Pak, J.Y. and Richardson, H.W. (2007), The Economic Impacts of a Terrorist Attack on the U.S. Commercial Aviation System, *Risk Analysis*, 27(3), 505-512.

Grant M & MG Stewart (2012). 'A Systems Model for Probabilistic Risk Assessment of Improvised Explosive Device Attack.' *International Journal of Intelligent Defence Support Systems,* 5(1), 75-93.

Grosskopf KR (2006). 'Evaluating the Societal Response to Antiterrorism Measures.' *Journal of Homeland Security and Emergency Management,* 3(2).

Heaton P (2010). *Hidden in Plain Sight: What Cost-of-Crime Research Can Tell Us About Investing in Police*. Santa Monica, Ca: RAND Corporation.

IATA (2012). *2012 Annual Review*. Geneva: International Air Transport Association.

IATA (2011). *The Impact of September 11 2001 on Aviation.* Geneva: International Air Transport Association.

IATA (2 March 2010). *Facts and Figures,* International Air Transport Association, Pressroom.

LaTourrette T, DR Howell, DE Mosher & J MacDonald (2006). *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options.* Santa Monica, Ca: RAND Corporation.

Morral, AR, CC Price, DS Oritz, B Wilson, T LaTourrette, BW Mobley, S McKay & HH Willis (2012). *Modeling Terrorism Risk to the Air Transportation System*. Santa Monica, Ca: RAND Corporation.

Mueller J & MG Stewart (2012). 'The Terrorism Delusion: America's Overwrought Response to September 11.' *International Security,* 37(1): 81-110.

Mueller J & MG Stewart (2011a). 'The Price is Not Right: The U.S. spends too much money to fight terrorism.' *Playboy,* 58(10), 149-150.

Mueller J & MG Stewart (2011b). *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security.* New York: Oxford University Press.

Mueller J. (2013). *Terrorism Since 9/11: The American Cases.* http://politicalscience.osu.edu/faculty/jmueller/since.html

National Research Council of the National Academies (2010). *Review of the Department of Homeland Security's Approach to Risk Analysis*. Washington DC: National Academies Press.

National Consortium for the Study of Terrorism and Responses to Terrorism (October 2012). *Global Terrorism Database.* University of Maryland, Ca. [http://www.start.umd.edu/gtd/].

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

Office of Best Practice Regulation (June 2010). *Best Practice Regulation Handbook*, Canberra: Australian Government.

Robinson LA, JK Hammitt, JE Aldy, A Krupnick & J Baxter (2010). 'Valuing the Risk of Death from Terrorist Attacks.' *Journal of Homeland Security and Emergency Management,* 7(1).

Stewart MG & RE Melchers (1997). *Probabilistic Risk Assessment of Engineering Systems.* London: Chapman & Hall.

Stewart MG & J Mueller (2013a). 'Terrorism Risks and Cost-Benefit Analysis of Aviation Security.' *Risk Analysis,* 33(5): 893-908.

Stewart MG & J Mueller (2013b). 'Aviation Security, Risk Assessment, and Risk Aversion for Public Decision-Making.' *Journal of Policy Analysis and Management*, 32(3): 615-633.

Stewart MG & J Mueller (2011). 'Cost-Benefit Analysis of Advanced Imaging Technology Fully Body Scanners for Airline Passenger Security Screening.' *Journal of Homeland Security and Emergency Management*, 8(1): 30.

Stewart MG, BR Ellingwood & J Mueller (2011). 'Homeland Security: A Case Study in Risk Aversion for Public Decision-Making.' *International Journal of Risk Assessment and Management*, 15(5/6): 367-386.

Stevens D, T Schell, T Hamilton, R Mesic, MS Brown, EW Chan, M Eisman, EV Larson, M Schaffer, J Gibson & E Harris (2004), *Near-Term Options for Improving Security at Los Angeles International Airport,* Santa Monica, Ca: RAND Corporation.

Sunstein CR (2002). *The Cost-Benefit State: The Future of Regulatory Protection.* Chicago: American Bar Association Publishing.

Townsend M, J Revill & P Kelbie (1 July 2007). 'Terror Threat "Critical" As Glasgow Attacked.' *The Guardian.*

United States Government (26 March 2007). *National Strategy For Aviation Security.* [http://www.fas.org/irp/offdocs/nspd/nspd-47.pdf].

Weisz RG (2012). 'America's Lack of Airport Security.' *2012 Critical Infrastructure Symposium*, Arlington, Virginia.

Yates A (13 May 2010). *Domestic & National Security Budget Analysis: 2010-11 Federal Budget*. Canberra: Australian Security Research Centre.

About the Authors

Mark G. Stewart is Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. He is the co-author of Probabilistic Risk Assessment of Engineering Systems (Chapman & Hall, 1997) and Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security (Oxford University Press, 2011), as well as more than 350 technical papers and reports. He has more than 25 years of experience in probabilistic risk and vulnerability assessment of infrastructure and security systems that are subject to man-made and natural hazards. Mark has received over $3 million in Australian Research Council (ARC) support in the past 10 years. Since 2004, Mark has received extensive ARC support to develop probabilistic risk-modeling techniques for infrastructure subject to military and terrorist explosive blasts and cost-benefit assessments of counter-terrorism protective measures for critical infrastructure. In 2011, he received a five-year Australian Professorial Fellowship from the ARC to continue and to extend that work.

John Mueller is Senior Fellow at the Cato Institute, and Professor and Senior Research Scientist at the Mershon Center for International Security Studies at Ohio State University, Columbus, Ohio. In addition to being co-author of Terror, Security, and Money, he is the author of over a dozen books. Three of these have won prizes: War, Presidents and Public Opinion (1973), Astaire Dancing: The Musical Films (1985), and The Remnants of War (2004). Other books include , Overblown (2006), Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda (2010), and War and Ideas (2011). He also edited the web book, Terrorism Since 9/11: The American Cases (2013). Mueller has published hundreds of articles in scholarly journals, general magazines, and newspapers, is a member of the American Academy of Arts and Sciences, and has been a John Simon Guggenheim Fellow.

ARC Centre of Excellence in Policing and Security

M10_3.01
Mt Gravatt Campus
170 Kessels Road
NATHAN QLD 4122
Ph: 07 3735 6903
Fax: 07 3735 1033

www.ceps.edu.au

ISSN 2200-4130 (Print)
2200-4149 (Online)

Australian Government
Australian Research Council

Griffith University · Australian National University · The University of Queensland Australia · Charles Sturt University