**CENTRE FOR INFRASTRUCTURE PERFORMANCE AND RELIABILITY**

**RESEARCH REPORT**

---

# Cost-Benefit Analysis of Aviation Security:
## Installed Physical Secondary Barriers (IPSB), Federal Air Marshal Service (FAMS), and Federal Flight Deck Officer (FFDO) Program

*Mark G. Stewart and John Mueller*

**Research Report No. 281.12.2011**

**December 2011**

**ISBN No. 9780 9871 1435 8**

---

THE UNIVERSITY OF
NEWCASTLE
AUSTRALIA

# COST-BENEFIT ANALYSIS OF AVIATION SECURITY:

## INSTALLED PHYSICAL SECONDARY BARRIERS (IPSB), FEDERAL AIR MARSHAL SERVICE (FAMS), AND FEDERAL FLIGHT DECK OFFICER (FFDO) PROGRAM

Mark G. Stewart
Australian Research Council Professorial Fellow
Professor and Director, Centre for Infrastructure Performance and Reliability
The University of Newcastle
New South Wales, 2308, Australia
Honorary Research Fellow, Mershon Center for International Security Studies, Ohio State University.
phone: +61 2 49216027 email: mark.stewart@newcastle.edu.au

John Mueller
Senior Research Scientist, Mershon Center for International Security Studies
Ohio State University
Columbus, Ohio 43201, United States
Cato Senior Fellow, Cato Institute
Washington, DC, United States
phone: +1 614 2476007 email: bbbb@osu.edu

**ABSTRACT**
The Transportation Security Administration (TSA) and international regulators seek security measures to help reduce the likelihood of a direct replication of 9/11, in which commercial passenger airliners were commandeered by small bands of terrorists, kept under control for some time, and then crashed into specific targets. This paper compares, for the U.S. case, the costs and benefits of three specific security measures designed for that purpose, assessing risk reduction, losses, and security costs in the context of the full set of security layers. These three measures are Installed Physical Secondary Barriers (IPSB) to restrict access to the hardened cockpit door during door transitions, the Federal Air Marshal Service (FAMS), and the Federal Flight Deck Officer (FFDO) program. Since the FAMS costs $1.2 billion per year, and its effectiveness is in serious doubt, a alternate policy measure considered is to double the budget of the FFDO program to $44 million per year, install IPSBs in all U.S. aircraft at a cost of $13.5 million per year, and reduce funding for FAMS by 75% to $300 million per year. A break-even cost-benefit analysis then finds the minimum probability of an otherwise successful attack required for the benefit of security measures to equal their cost. It was found that the IPSB is cost-effective if the annual attack probability exceeds 0.5% or 1 attack every 200 years. The FFDO program is cost-effective if the annual attack probability exceeds 2.8%. On the other hand, more than four attacks per year need to be deterred, foiled, prevented or disrupted for FAMS to be cost-effective. Thus, even when assumptions are in place that considerably bias the analysis toward the opposite conclusion, the expensive FAMS very substantially fails a cost-benefit assessment. Moreover, insofar as FAMS does reduce risk, almost all of that benefit can be obtained with a mix of inexpensive measures: IPSB and FFDOs. A policy that includes IPSBs, an increased budget for FFDOs, and a reduced budget for FAMS may well be optimal.

# 1. INTRODUCTION

We seek to evaluate the costs and benefits of those security measures that are designed to prevent a direct replication of 9/11, in which commercial passenger airliners were commandeered by small bands of terrorists, kept under control for some time, and then crashed into specific targets. We will incorporate a general consideration of all airline security measures into our analysis, but to deal with the potential for a replication of 9/11, we focus in particular on the cost-effectiveness of three from the in-flight security list: (1) air marshals and other law enforcement officers (Federal Air Marshal Service or FAMS), (2) Federal Flight Deck Officers (FFDOs) which allows pilots and crew members to carry firearms to defend the flight deck, and (3) Installed Physical Secondary Barriers (IPSB) which restrict access to the hardened cockpit door during door transitions. Since the FAMS costs $1.2 billion per year, and their effectiveness is in serious doubt (Stewart and Mueller 2008), an alternate policy measure considered is to double the budget of the FFDO program to $44 million per year, install IPSBs in all U.S. aircraft at a cost of $13.5 million per year, and reduce funding for FAMS by 75% to $300 million per year.

The need for risk and cost-benefit assessment for homeland security programs, and those supported by the Department of Homeland Security (DHS) in particular, is well made by many in government, industry and academe (e.g., Friedman 2010, Hahn 2008, Poole 2008). The U.S. National Research Council (NRC 2010), after a 15 month study period, was critical of the DHS, and their primary conclusion was: 'the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested' and 'only low confidence should be placed in most of the risk analyses conducted by DHS'.

To compare costs and benefits requires the quantification of threat probability, risk reduction, losses, and costs of security measures. This is a challenging task, but necessary for any risk assessment, and the quantification of security risks is increasingly being addressed (e.g., Twisdale et al. 1994, Low and Hao 2002, Stewart et al. 2006, Stewart and Netherton 2008, Dillon et al. 2009, Cox 2009), as well as recent life-cycle and cost-benefit analyses for infrastructure protective measures (Little 2007, Willis and LaTourette 2008, von Winterfeldt and O'Sullivan 2006, Stewart 2008, 2010, 2011). Much of this work can be categorised as 'probabilistic terrorism risk assessment' (Willis et al. 2007).

Stewart and Mueller (2008) found that U.S. Federal Air Marshal Service which costs over $1.2 billion per year fails to be cost-effective, but that hardening cockpit doors is very cost-effective. However, this study considered cost per life saved as the decision-support criterion, which may be misleading since the consequences of terrorist attacks includes considerable damage to infrastructure, loss of business, tourism and GDP, and other indirect losses that amounted to up to $200 billion in the 9/11 attacks (Mueller and Stewart 2011a,b). More recently, Stewart and Mueller (2011) conduced a systems reliability analysis and more detailed cost-benefit assessment of Advanced Imaging Technologies (AIT) that are full-body scanners to inspect a passenger's body for concealed weapons, explosives, and other prohibited items. Since there is uncertainty and variability of parameters, three alternate probability (uncertainty) models were used to characterise risk reduction and losses. Monte-Carlo simulation methods were used to propagate these uncertainties in the calculation of benefits, and the minimum attack probability necessary for AITs to be cost-effective was calculated. It was found that the attack probability needs to exceed 160-330% per year (or 1.6 to 3.3 attacks per year) to be 90% certain that AITs are cost-effective. It therefore appears that many homeland security measures would fail a cost-benefit analysis using standard expected

value methods of analysis as recommended by the U.S. Office of Management and Budget (OMB 1992); a detailed assessment of threats and vulnerabilities leads to similar conclusions (Mueller 2010).

For many engineering systems the hazard (or threat) rate is known or predicted 'a priori', but for terrorism the threat is from an intelligent adversary who will adapt to changing circumstances to maximise likelihood of success (however, see Kenney 2010). Some statistical approaches exist for terrorist threat prediction (e.g., Pate-Cornell and Guikema 2002, Dillon et al 2009, Cox 2009), however, these rely heavily on expert judgments from security experts, game theory, etc. so the inherent uncertainties can still be high. For this reason, a practical approach is a 'break even' cost-benefit analysis that finds the minimum probability of a successful attack required for the benefit of security measures to equal their cost. In other words, the threat probability is the output of the cost-benefit analysis and it is the prerogative of the decision-maker, based on expert advice about the anticipated threat probability, to decide whether or not a security measure is cost-effective. If the threat probability is known with confidence, then the 'break-even' approach can be recast another way by calculating the minimum risk reduction required for a security measure to be cost-effective. While this approach is not without challenges (Farrow and Shapiro 2009), 'break-even' cost-benefit analyses are increasingly being used for homeland security applications (e.g., Ellig et al. 2006, Willis and LaTourette 2008, Winterfeldt and O'Sullivan 2006, Akhtar et al. 2010). Hence, we will undertake a 'break even' cost-benefit analysis in this paper.

This paper focuses on aviation security in the U.S. However, Australia, United Kingdom, Canada and many other countries also have air marshals with similar cost and effectiveness issues as the U.S. Hence, the present paper will provide useful guidance to U.S. and international aviation security regulators.

## 2. RISK AND COST-BENEFIT METHODOLOGY

An advantage of a probabilistic risk assessment is that it can include a risk-cost-benefit analysis that considers tradeoffs between risks and costs. An appropriate decision analysis compares the marginal costs of security measures with the marginal benefits in terms of fatalities and damages averted. The decision problem is to maximise the net benefit (equal to benefits minus the cost) or net present value:

$$\text{Net Benefit} = p_{attack} \times C_{loss} \times \Delta R - C_{security} \quad (1)$$

where

1. $p_{attack}$: The *probability of a successful attack* is the likelihood a successful terrorist attack will take place if the security measure were not in place.
2. $C_{loss}$: The *losses sustained in the successful attack* include the fatalities and other damage - both direct and indirect - that will accrue as a result of a successful terrorist attack, taking into account the value and vulnerability of people and infrastructure as well as any psychological and political effects.
3. $\Delta R$: The *reduction in risk* is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack.
4. $C_{security}$ *:costs* of providing the risk-reducing security that are required to attain the benefit.

A security measure is viewed as cost-effective or efficient if the net benefit exceeds zero (OBPR 2010). There are many risk acceptance criteria and these depend on the type of risk being quantified (life safety, economic, environmental, social), the preferences of the interested parties and the decision maker, and the quality of the information available. Risk acceptance criteria based on annual fatality risk or failure probability may also be used (e.g., Stewart 2010, 2011).

Terrorism is a frightening threat that affects our willingness to accept risk, a willingness that is influenced by psychological, social, cultural, and institutional processes. Moreover, events involving high consequences can cause losses to an individual that they cannot bear, such as bankruptcy or the loss of life. On the other hand, governments, large corporations, and other self-insured institutions can absorb such losses more readily and so governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making (e.g., Sunstein 2002, Ellingwood 2006). This is confirmed by the U.S. Office of Management and Budget (OMB) which requires cost-benefit analyses to use expected values (an unbiased estimate), and where possible, to use probability distributions of benefits, costs, and net benefits (OMB 1992). However, Eqn. (1) can be generalised for expected utility incorporating risk aversion (e.g. Stewart et al. 2011). The issue of risk aversion is an important one as this seems to dominate counter-terrorism (CT) and other decisions (Jordaan 2005, Mueller 2006), but also arises from uncertainty of CT effectiveness (and threats).

In the process:

- we present our analysis in a fully transparent manner: readers who wish to challenge or vary our analysis and assumptions are provided with the information and data to do so.
- in coming up with numerical estimates and calculations, we generally pick ones that bias the consideration in favour of finding the homeland security measure under discussion to be cost-effective.
- we decidedly do *not* argue that there will be no further terrorist attacks; rather, we focus on the net benefit of security measures and apply 'break even' cost-benefit analyses to assess how high the likelihood of a terrorist attack must be for security measures to be cost-effective.
- we are aware that not every consideration can be adequately quantified (something that holds as well, of course, for other decision areas that excite political and emotional concerns), but we try nonetheless to keep non-quantifiable considerations in mind.
- although we understand that people are often risk-averse when considering issues like terrorism, we believe that governments expending tax money in a responsible manner need to be neutral when assessing risks, something that entails focusing primarily on mean estimates in risk and cost-benefit calculations, not primarily on worst-case or pessimistic ones.

## 3. THE 'LAYERS OF SECURITY' APPROACH

The TSA has arrayed '21 Layers of Security' to 'strengthen security through a layered approach' – see Figure 1. This is designed to provide defence-in-depth protection of the travelling public and of the United States transportation system.

Of these 21 layers, 15 are 'pre-boarding security' (i.e., deterrence and apprehension of terrorists prior to boarding aircraft):

1. Intelligence
2. International Partnerships
3. Customs and Border Protection
4. Joint terrorism task force
5. No-fly list and passenger pre-screening
6. Crew vetting
7. Visible Intermodal Protection Response (VIPR) Teams
8. Canines
9. Behavioural detection officers
10. Travel document checker
11. Checkpoint/transportation security officers
12. Checked baggage
13. Transportation security inspectors
14. Random employee screening
15. Bomb appraisal officers

The remaining six layers of security provide 'in-flight security':

16. Federal Air Marshal Service
17. Federal Flight Deck Officers
18. Trained flight crew
19. Law enforcement officers
20. Hardened cockpit door
21. Passengers

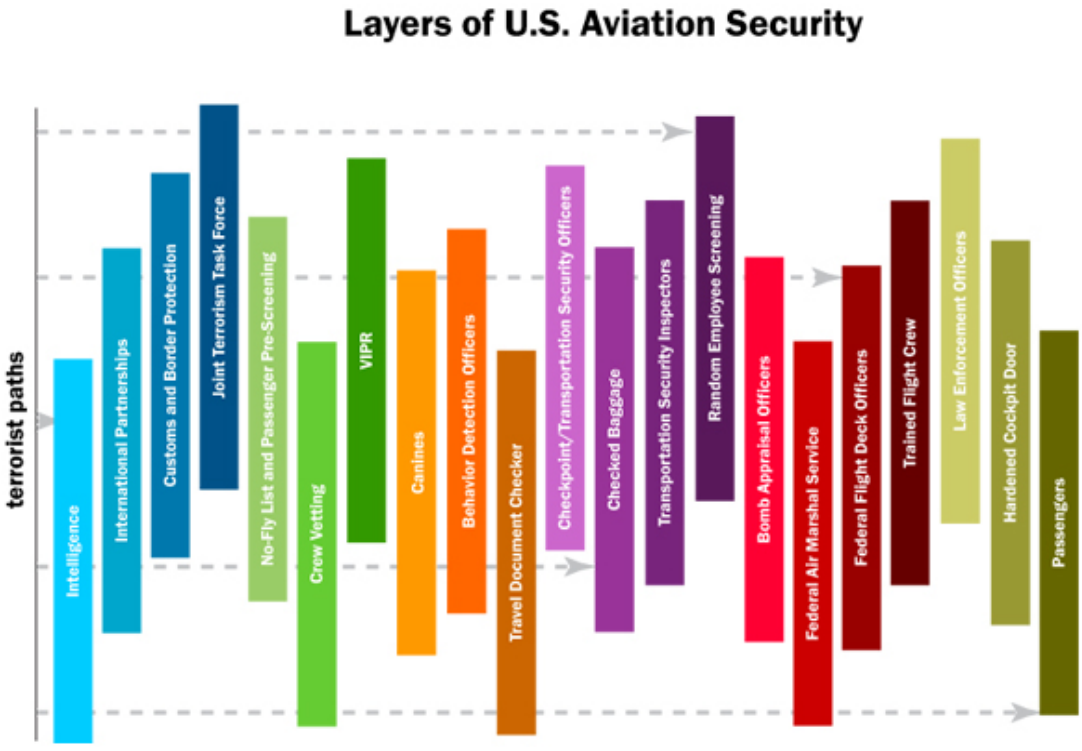


Figure 1. TSA's 21 Layers of Security.

We are concerned with the costs and benefits of measures that seek to prevent exact duplications of 9/11 in which commercial passenger airlines are commandeered, kept under control for some time, and then crashed into specific targets. For such a hijacking to succeed requires that all stages of the planning, recruiting and implementation of the plot succeed. We

will focus on three steps linked to aviation security:

1. success in boarding aircraft undetected
2. success in hijacking an aircraft
3. success in entering cockpit, commandeering the aircraft, and crashing it into a designated target

The security measures in place to foil, deter or disrupt these three steps are:

1. success in boarding aircraft undetected - 11 of the 15 pre-boarding layers of security apply: intelligence, international partnerships, Customs and Border Protection, joint terrorism task force, no-fly list and passenger pre-screening, behavioural detection officers, travel document checker, checkpoint/transportation security officers (TSO), transportation security inspectors, crew vetting, and random employee screening.
2. success in hijacking an aircraft - trained flight crew, passenger resistance, air marshals, and on-board law enforcement officers
3. success in entering cockpit and commandeering the aircraft - armed flight crew (FFDO), hardened cockpit door, and IPSB.

We begin assessing risk reduction by developing a simple systems model of existing aviation security measures. Figure 2 shows a reliability block diagram used to represent the system of foiling, deterring or disrupting a terrorist hijacking on a commercial airplane. If a terrorist attack is foiled by any one of these layers of security, then this is viewed as a series system. Note that we include a new 'layer of security' - Installed Physical Secondary Barriers (IPSB).

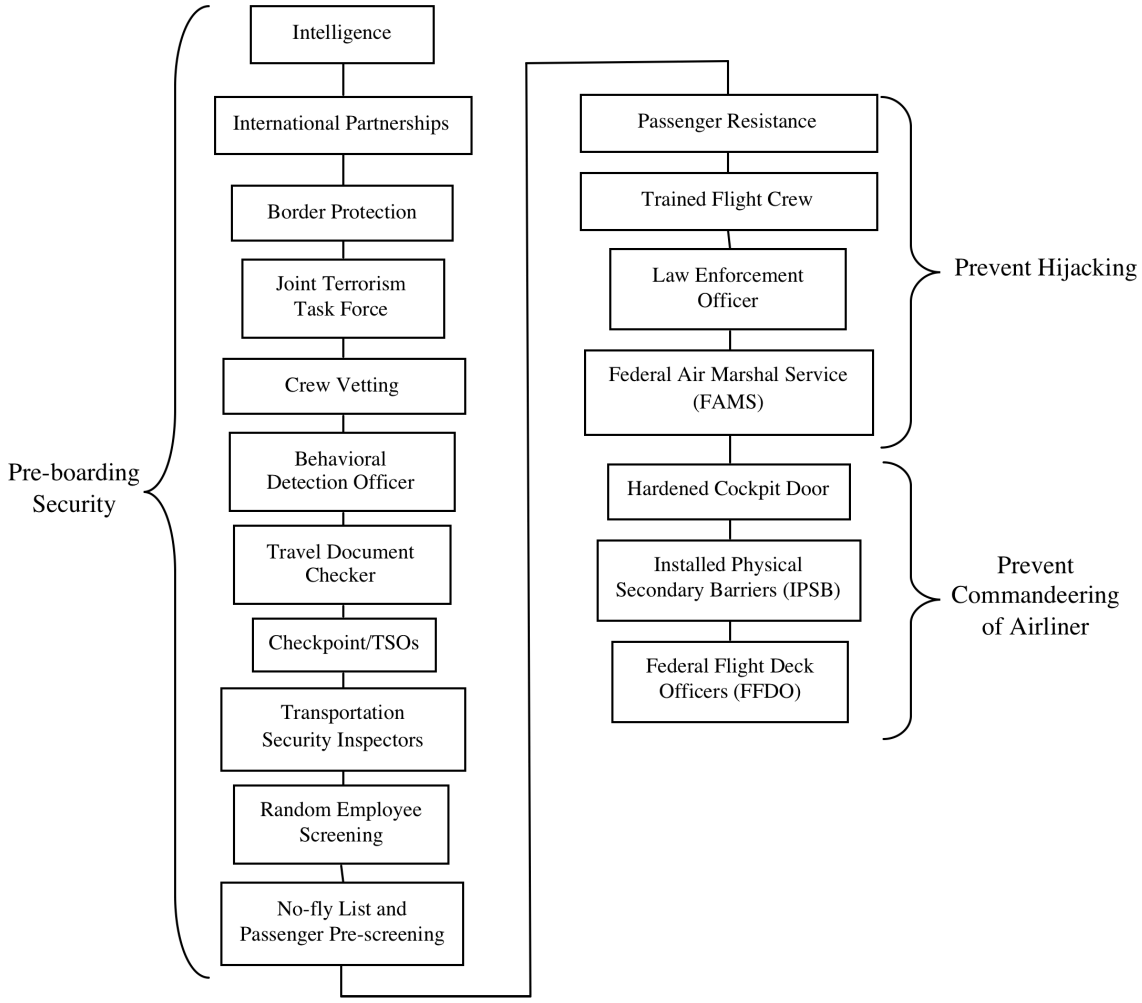


Figure 2. Reliability Block Diagram for Aviation Security Measures.

If any one of these security measures are effective, or the capabilities of the terrorist are lacking, the terrorist hijacker will not be successful. We do not include all 'layers' of TSA security such as checked baggage or canines, only those likely to stop a replication of a 9/11 type attack. Also, we do not deal with efforts to prevent other air mishaps like such as attempts to blow up of an airliner without hijacking it or to shoot it down with a missile. Such threats cannot be deterred or confidently prevented by hardened cockpit doors or air marshals or secondary barriers to the cockpit, and are outside the scope of this cost-benefit analysis focusing as it does on preventing a direct replication of a 9/11 type of attack.

Assuming a series system where each event probability is statistically independent, the probability that a terrorist hijacking plot will be foiled, disrupted or deterred is

$$\Pr(\text{hijacking foiled}) = 1 - \left\{ \begin{array}{l} \prod_{i=1}^{N} 1 - \Pr(\text{detection for pre-boarding security measure i}) \\ \times \left[1 - \Pr(\text{foiled by passenger resistance})\right] \\ \times \left[1 - \Pr(\text{foiled by flight crew})\right] \\ \times \left[1 - \Pr(\text{foiled by law enforcement officer})\right] \\ \times \left[1 - \Pr(\text{foiled by hardened cockpit door})\right] \\ \times \left[1 - \Pr(\text{foiled by IPSB})\right] \\ \times \left[1 - \Pr(\text{foiled by FAMS})\right] \\ \times \left[1 - \Pr(\text{foiled by FFDO})\right] \end{array} \right\} \quad (2)$$

It might be noted that there are at least two potential 'layers of security' that might be added to this consideration.

One concerns the general incompetence of terrorists particularly in complicated plots. Their success on 9/11 was considerably graced by luck, and there were many points at which it could have gone awry. Indeed, 9/11 increasingly seems to be an aberration, not a harbinger. Thus, since that time no terrorist in the United States has been able successfully to detonate even a simple bomb and, except for the London bombings of 2005, neither has any in the United Kingdom. Most (though not all) terrorist efforts seem to be characterised mainly by poor tradecraft and muddled vision (Kenney 2010, Mueller 2011).

Another concerns anti-aircraft defensive measures put into place after 9/11. If a pilot were able to transmit to air controllers even the scrappiest of information that the plane was under a violent hijacking attempt, anti-aircraft measures would be immediately scrambled to shoot down or ground the captured airliner before it could reach an intended target. Even if the flight crew were disabled, the cabin crew could communicate with the outside and, as the experience with the fourth plane on 9/11 demonstrates, so could the passengers.

Of particular consideration in our analysis is an examination of the possibility that a team of hijackers could seize control of the flight deck by forcing their way in during those brief and fleeting moments when the door is opened during flight. Once in the cockpit, the hardened cockpit doors would then help defend the attackers. An important study finds that such an undertaking could be accomplished in a matter or seconds - though its scenario posits a team

of attackers that is "highly-trained, armed, athletic," qualities that, as noted, characterise very few potential terrorists (RTCA 2011).

# 4. COST-BENEFIT ASSESSMENT OF AVIATION SECURITY

## 4.1 Costs and Characteristics of the In-Flight Security Measures

### *4.1.1 Passenger Resistance*

An important form of in-flight defence is crew and passenger resistance. One reason for the extent of the losses of 9/11 was the reluctance of crew and passengers to confront and resist the hijackers. This is understandable, as most previous hijackings ended peacefully or with minimal loss of life, and the main response to a hijacking was to 'get the plane on the ground so negotiations can begin' (Schneier 2006). Indeed, only a few months earlier, three terrorists had commandeered a Russian airliner, demanding that it be flown to Saudi Arabia, at which point they were overcome by local security forces with almost no loss of life (Kramer 2004).

The 9/11 suicide attacks on the World Trade Center and Pentagon radically changed this perception. As demonstrated on the fourth plane, where passengers had news of what had happened on the first three, passengers and crew will now fight back, particularly if there is any indication that the terrorists' intent is to enter the cockpit (or to explode the airliner). As pilot Patrick Smith puts it forcefully:

> Conventional wisdom says the terrorists exploited a weakness in airport security by smuggling aboard box-cutters. What they actually exploited was a weakness in our mindset - a set of presumptions based on the decades-long track record of hijackings. In years past, a takeover meant hostage negotiations and standoffs; crews were trained in the concept of 'passive resistance.' All of that changed forever the instant American Airlines Flight 11 collided with the north tower. What weapons the 19 men possessed mattered little; the success of their plan relied fundamentally on the element of surprise. And in this respect, their scheme was all but guaranteed not to fail. For several reasons - particularly the awareness of passengers and crew - just the opposite is true today. Any hijacker would face a planeload of angry and frightened people ready to fight back. Say what you want of terrorists, they cannot afford to waste time and resources on schemes with a high probability of failure. And thus the September 11th template is all but useless to potential hijackers. (Smith 2007)

Similarly, Thomas Kean, chair of the 9/11 Commission, believes that the 'best defense is always still going to be the flying public.' (Comments at the presentation of 'Assessing the Terrorist Threat' report, Bipartisan Policy Center, Washington, DC, September 10, 2010; see also Mueller 2006.)

There is now clearly a new paradigm, and crew and passengers will no longer be passive. Thus, an attempted hijacking of an Australian domestic flight in 2003 was foiled as flight attendants and passengers restrained a man attempting to enter the cockpit 'armed' with two wooden stakes, an aerosol can, and a lighter (Murphy and Hudson 2003). Beyond hijacking, passenger and crew reactions were also effective in subduing the shoe bomber of 2001 and the underwear bomber of 2009.

Yet the issue may not be quite so clear-cut. Most reported incidents of fighting back have occurred when the terrorist was acting alone, not the coordinated resistance needed to

overwhelm a team of hijackers spread throughout an aircraft, or hijackers already in control of the flight deck with a hardened cockpit door to protect them from passengers and crew - and a team of hijackers is what would be required for a 9/11 type of attack to be repeated. As noted, the time required for hijackers to take over the flight deck (during a door transition) might be a matter of seconds, and this would likely be much less than passengers need to assess the situation, realise the dire threat, communicate with other passengers, and process other information needed for them to summon the courage to assault armed and dangerous terrorists. The fact that passengers are required to be buckled into their seats during door transitions (RTCA 2011) further lowers this likelihood.

In addition, it has been argued that passengers are susceptible to the "bystander effect" - a phenomenon where the greater the number of people present the less the likelihood of someone intervening to help someone in distress (RTCA 2011). However, this hardly applies to the airline hijacking case because the effect is built on the idea that bystanders are not, themselves, in danger if they fail to intervene. Also, when the costs of intervening are high, when the situation is seen to be dangerous, and when the perpetrator is present, there is often little or no bystander effect (Fischer et al. 2011). The people in the first three planes on 9/11 did not intervene in part because they didn't think they were necessarily in personal danger. This condition clearly changed for the fourth plane, and so did passenger behaviour. Airline hijacking now seems to be one of mutual disaster, and decades of research indicates that the most common response in disasters is for people to work to cope and to cooperate - help each other - even if that entails some personal risk and danger (Fischhoff 2005).

The 2011 RTCA report on flight deck security procedures concludes that "passengers are not considered a predictably reliable option for preventing an attempted violent or sudden breach of the flight deck" and so "did not include the possibility of passenger intervention as a mitigating measure" (RTCA 2011). Although the "bystander effect" does not really support this conclusion, the fact that a door transition attack could take place in seconds does.

Although passengers may provide at most only a small deterrent effect to a door-transition hijacking because of their limited ability to disrupt the actual physical attack, they would still be able to alert outsiders by voice or text messaging, something that hijackers could have a hope of preventing only if they had infiltrated an improbably large number of ruthless teammates into the cabin to keep watch. As noted, under current, post-9/11 circumstances, messages to the outside would quickly trigger air interceptors that would prevent the hijacked plane from reaching a target. If they successfully made it into the flight deck, the hijackers could still crash the plane of course, but if that were their goal, it could be accomplished with far simpler (if still difficult) methods such as smuggling a bomb aboard.

### *4.1.2 Trained Flight Crew*

The training of flight attendants includes no instructions in the use of force. However, the TSA Crew Member Self Defense Training (CMSDT) Program provides one-day training programs at a cost of $3 million per year (CAPA 2011). However, reportedly less than 1% of flight attendants have undertaken this course (Wilber 2007). Nonetheless, many airlines have instituted procedures during door transition (such as galley trolleys to block access to the flight deck) - these are referred to as 'human secondary barriers' (RTCA 2011). Test trials, using highly trained attackers and defenders, found that using blocking crew members without additional equipment (IPSB) did "not produce satisfactory results" (RTCA 2011). The flight deck is clearly vulnerable to flight deck intrusions during door transition due to

lack of training and the very short reaction times needed to defeat an attacker in easy reach of the cockpit door.

### *4.1.3 Hardened Cockpit Doors*

The FAA required operators of more than 6,000 planes to install hardened cockpit doors by 9 April 2003 in order to protect cockpits from intrusion and small-arms fire or fragmentation devices. The FAA also required foreign airlines serving the United States to harden their cockpit doors. The FAA mandated that 'The doors will be designed to resist intrusion by a person who attempts to enter using physical force. This includes the door, its means of attachment to the surrounding structure, and the attachment structure to the bulkhead'. It also requires that the cockpit doors remain locked and cockpit access controlled (FAA 2002). The purchase and installation cost of each hardened cockpit door is typically $30,000 to $50,000. The total cost to airlines is estimated as $300-$500 million over a 10-year period, including the cost of increased fuel consumption due to the heavier doors (FAA 2003). This cost will decrease over time as door installation costs for new aircraft will be less than for existing aircraft. While the effectiveness of these doors in restricting cockpit access to a determined hijacker may be questioned (Lott 2004), there is little doubt that hardened cockpit doors will deter and delay a hijackers attempt to enter the cockpit. A best estimate annual cost of hardening cockpit doors for U.S. aircraft is $40 million.

Hardened cockpit doors may be useful in preventing a direct replication of 9/11, but they contribute little to the prevention or mitigation of other kinds of terrorist acts on airplanes such as detonation of explosives. Also, as noted, if attackers are somehow able to get into the flight deck during a door transition, the doors become a security device that could protect the attackers.

### *4.1.4 Installed Physical Secondary Barriers (IPSB)*

A secondary barrier to the cockpit could further enhance security - this is 'a lightweight device that is easy to deploy and stow, installed between the passenger cabin and the cockpit door that blocks access to the flight deck whenever the reinforced door is opened in flight.' (ALPA 2007) - see Figure 3. The barrier is normally stowed when the cockpit door is closed and locked. However, on many flights the flight deck door cannot remain closed for the entire duration of the flight, as access is required for rest periods, toilet breaks, and meals. During the time of opening and closing ('door transition'), the protective benefits of a hardened cockpit door to protect the flight deck area is reduced at least against highly skilled and light-footed hijackers (RTCA 2010). While some airlines have instituted procedures during door transition (such as galley trolleys to block access to the flight deck), they are not fool-proof. This has led the Airline Pilots Association (ALPA) to conclude that 'the reinforced flight deck door does not provide a complete solution for securing the flight deck' (ALPA 2007). Hence, in 2004 United Airlines installed on its entire fleet of 500 passenger aircraft Installed Physical Secondary Barriers (IPSB) that crew members must deploy prior to opening the flight deck door (AT 2004, ALPA 2007). Additionally, Boeing and Airbus have designed installed physical secondary barriers as options on certain models of their next generation aircraft (RTCA 2010). Further security is provided by the fact that a cabin crew member is generally required to be at the scene when the secondary barrier is put into place, something that adds another complication for would-be hijackers - and at little or no cost.

Figure 3. Fully Deployed Installed Physical Secondary Barrier (ALPA 2007).

The cost of an IPSB for a single aircraft is approximately $25,000 in 2004 (AT 2004) - when adjusted for inflation this is approximately $30,000 in 2011 dollars. Since there are approximately 6,000 commercial aircraft in the U.S., this equates to $180 million. If we round this up to $200 million, and this cost is annualised over 20 year design life of an aircraft with a 3% discount rate, this equates to a present value cost of $13.5 million per year.

As with hardened cockpit doors, secondary barriers may be useful in preventing a direct replication of 9/11, but they contribute little to the prevention or mitigation of other kinds of terrorist acts on airplanes such as detonation of explosives.

### *4.1.5 Federal Air Marshal Service (FAMS) and Law Enforcement Officers*

A significant chunk of TSA's budget is spent on the Federal Air Marshal Service. There are now some 2,500 to 4,000 air marshals, up from 33 before 9/11 (Meckler and Carey 2007). In 2010, federal officials stated that there were more than 3,200 air marshals available for deployment (ABC 2010). The FY2011 budget for the service is $950 million (DHS 2010). In addition, airlines are expected to provide free seats to air marshals, and these are generally in first class to allow observation of the cockpit door. The Air Transport Association estimates that this costs airlines $220 million per year in lost revenue (Poe 2005). A best estimate of the annual cost to government and airlines for the Federal Air Marshal Service, then, is $1.2 billion.

Air marshals ride on no more than 10 percent of flights in the United States, and some estimates are even lower, concluding that air marshals fly on less than 5 percent (Hudson 2004, 2005; Griffin 2008). However, Thomas Quinn, former director of the Federal Air Marshal Service, has dismissed such reports and, while declining to give specifics, insists his

agents cover 'more than 5 percent' of some 28,000 daily commercial flights in the United States (Meeks 2004). These are often high-risk flights, based on intelligence reports (Kearney 2005). Exactly how that risk has been determined is difficult to fathom, particularly since air marshals have had almost nothing to do over the years. They have several dozen arrests since 2001, but none of these has been related to terrorism (Meckler and Carey 2007; Griffin 2010). Their chief, or at rate most publicised, achievement thus far seems to have been to kill an apparently deranged and menacing, but innocent and unarmed, passenger during a Florida airport altercation on the ground in 2005 (Mueller 2006).

Additional law enforcement officers may be on some flights for reasons other than countering terrorism, such as escorting prisoners or protecting VIPs. However, their numbers will not significantly boost the percentage of flights that have an armed officer on board.

The presence of air marshals or other law enforcement officers is likely to have a deterrent effect, but this is ameliorated by the low percentage of flights that they can cover. It might even be argued that some crew and passengers may be reluctant to be the first to confront a hijacker if they believe an air marshal is on board, a hesitation that could conceivably give attempted hijackers the time they need to execute their plans. Hence, the anticipated presence of air marshals may be counter-productive in some cases.

The goal of the air marshals is primarily to prevent a replication of 9/11 - a reason for putting them in the first class section upfront. Conceivably, they could be helpful in other terrorist situations - for example, if a passenger tried to blow up the airliner - but their added value over crew and passenger resistance is likely to be rather small because they are present on only a rather small percentage of flights and because they are likely to be seated far from where a potential bomber is located. In addition, if a door-transition attack (by highly trained, armed, and athletic attackers) can take place in seconds, it is not at all clear that air marshals could act fast enough to waylay the attempt.

### *4.1.6 Federal Flight Deck Officers (FFDO)*

Flight crews have shown interest in the Federal Flight Deck Officer (FFDO) program, which allows pilots and crew members who volunteer to transport and carry firearms to defend the flight deck of aircraft against acts of criminal violence or air piracy. The FFDO program is managed by the FAMS, and provides the 'last line of defense' of the flight deck, and has dramatically increased in size since its inception in 2003 (Moak 2011). It is estimated that in 2008 10% of pilots in the U.S. were FFDOs which will grow to 16.1 percent, or nearly 15,000, pilots by 2011 (Frank 2008), and that FFDOs provide five more times coverage than the FAMS (Flagg 2011). If there are 2,500 to 4,000 FAMS, and roughly 15,000 FFDOs, then Flagg's estimate of FFDOs providing five more times coverage than FAMS is realistic.

The FY2011 budget for the FFDO program is approximately $22 million. The cost of each Federal Air Marshal is around $3,300 per flight, compared to FFDOs costing approximately $15 per flight (Flagg 2011) For its modest cost, and higher coverage than the FAMS, Lee Moak, President of the Airline Pilots Association International, describes that the "FFDO program has been acknowledged by industry and government to be an extremely successful and cost-effective layer of aviation security" (Moak 2011). Moak goes on to request that the "FFDO program is in need of a significant increase in funding", and the Coalition of Airline Pilots Associations recommends doubling the FFDO budget over five years (CAPA 2011).

## 4.2 Losses Sustained in a Successful Attack

The loss of an aircraft and follow-on economic costs and social disruption might be considerable. A 2007 RAND study reported that the direct loss of an airliner with 300 passengers is about $1 billion assuming a value of life of only $2-2.5 million (Chow et al 2005). The scenario hypothesised in the RAND study was the downing of an airliner by a shoulder fired missile, and this could cause a shutdown of U.S. airspace for a week that might lead to an economic loss of $3 billion during the shutdown period, and losses in the following months would lead to a total economic loss of more than $15 billion assuming a 15% drop in air travel in the 6 months following the attack.

To establish something of an upper bound for the losses inflicted by conventional terrorist attacks, it may be best to begin with an estimate of the aggregate costs, as expressed in economic terms, inflicted by the terrorist attack that has been by far the most destructive in history, that of September 11, 2001. That attack directly resulted in the deaths of nearly 3,000 people with an associated loss of approximately $20 billion. In addition 9/11 caused, of course, great direct physical damage, amounting to approximately $30 billion in 2010 dollars, including rescue and clean-up costs (Bram et al. 2002). Indirect costs were even more substantial. Thus, the International Monetary Fund estimates that the 9/11 attacks cost the U.S. economy up to 0.7% in lost GDP ($100 billion in 2010 dollars, adjusting for inflation) in that year alone, while others estimate that associated business costs and loss of tourism cost the US economy $190 billion over 3 years (Hook 2008). A comprehensive 2009 study by the National Center for Risk and Economic Analysis of Terrorist Events found that the impact on the U.S. economy of the 9/11 attacks range from 0.3% to 1% of GDP (Blomberg and Rose 2009). An upper bound estimate of the losses of 9/11 might approach $200 billion.

However, this is the total cost for four aircraft hijackings, not one. Most of the losses arose from the devastating attacks on the World Trade Center by two separate aircraft, so for a single aircraft we divide this figure by two, generating a loss of $100 billion for a hijacked aircraft that is subsequently flown into a significant building or target. This is a high, upper-bound estimate because it would obviously be difficult for terrorists to again inflict such a huge loss of life and treasure as was accomplished with the attacks on the World Trade Center. Somewhat more plausible, actually, would be an attack like that on the Pentagon on 9/11. In that case, the damage bill came to $700 million, while compensating the families of the 184 victims up to $1.2 billion if we use $6.5 million as the value of life. With the additional costs of social and business disruptions, loss of tourism, and the like, the total cost in this case might total $10 billion.

The magnitude of the effects of terrorism on GDP is highly variable, but as economist Paul Krugman suggests, ‘on an economy-wide basis - except for small economies like that of Israel - the costs of behavioural responses to terrorism at current levels are probably fairly small, almost surely less than 1 percent of GDP’ (Krugman 2004). An exhaustive review of international terrorism losses by Sandler and Enders (2005) concludes that ‘For most economies, the economic consequences of terrorism are generally very modest and of a short-term nature’. As they point out,

- Large diversified economies are able to withstand terrorism and do not display adverse macroeconomic influences. Recovery is rapid even from a large-scale terrorist attack.
- Developed countries can use monetary and fiscal policies to offset adverse economic impacts of large-scale attacks. Well-developed institutions also cushion the consequences.

- The immediate costs of most terrorist attacks are localized, thereby causing a substitution of economic activity away from a vulnerable sector to relatively safe areas. Prices can then reallocate capital and labour quickly.

The last point is an important one. When expenditures are either transferred somewhere else or deferred temporarily, money will still be spent one way or the other. There will be loss of economic activity to the affected areas, but other areas or sectors of the economy will benefit with increased economic activity. For example, after 9/11 Hawaii experienced a boom in domestic visitors generating an extra $550 million in 2004 alone because more Americans decided to take vacations closer to home than travel internationally (Bonham et al. 2006). If there is an attack on a subway, more people will catch a bus or take a taxi. So there will be winners and losers, not just losers as we often assume when discussing economic 'losses' from terrorism. None of this is to dismiss the tragic and life-changing losses faced by the victims. But when we step back and look at the bigger picture the overall losses and damages to society may not be as great as they may first appear.

The $10 billion in losses from the 9/11 attack on the Pentagon, or the $15 billion proposed by the RAND study (assuming the aircraft missed its target) would be a plausible lower value of economic loss - we shall select $10 billion. Moreover, $100 billion in losses, mainly due to loss of GDP, and equivalent to the 9/11 losses from a single aircraft, is a plausible upper bound on losses. A mean loss of $50 billion is thus reasonable.

### 4.3 Reduction in Risk Due to the Security Measure

The risk reduction ($\Delta R$) is the additional risk reduction achieved by the presence of IPSB, FAMS, and/or FFDOs when compared to the overall risk reductions achieved by the presence, absence and/or effectiveness of all other security measures. For any security measure the risk reduction can vary from 0% to 100%. If a combination of security measures will foil every threat then the sum of risk reductions is 100%. This soon becomes a multidimensional decision problem with many possible interactions between security measures, threat scenarios, threat probabilities, risk reduction and losses. Fault trees and logic diagrams, together with systems engineering and reliability approaches, will aid in assessing these and other complex interactions involving threats, vulnerabilities and consequences (e.g., (Stewart and Melchers 1997, Biringer et al. 2007). This is the approach used herein.

For these purposes, we assume:

- The probability that a terrorist is detected by any one of the 11 TSA layers of pre-boarding security is a very low 10%. This is quite conservative. For example, the layer 'checkpoint/security layer' which involved passenger and carry-on items screening by metal detectors, X-ray machines and/or Advanced Imaging Technology (AIT) full-body scanners will have high probability of deterring terrorists or detecting weapons concealed on the passenger or their carry-on items for use in a hijacking attempt. This is perhaps the most effective of all pre-boarding security measures. The extra and more vigilant intelligence, immigration and passport control, airport screening, and other pre-boarding security measures implemented since 9/11 should result in an increased likelihood of detection and apprehension of terrorists. Increased public awareness is also of significant benefit to aviation security. Added to this are the much enhanced preventative policing and investigatory efforts that have caught potential terrorists including, in the U.K. in 2006, some planning to blow up airliners. Moreover, terrorist incompetence will increase detection rates for most of these barriers.

- Passengers have a very low chance (5%) of foiling a terrorist attempting to hijack and commandeer an aircraft. As discussed earlier, it could well be argued that the largest deterrent to an attempted hijacking is crew and passenger resistance - particularly when their ability to contact the outside is considered. Thus, one could readily justify (far) more than a 5% chance that passengers would foil or deter an attempted hijacking.
- Flight crew have a low 10% chance of foiling a terrorist attempting to hijack and commandeer an aircraft. There are standard operating procedures in place to minimise the vulnerability of the flight deck during door transitions, but the flight deck is vulnerable to flight deck intrusions during door transition due to lack of training and to the very short reaction times needed to defeat an attacker.
- On-board law enforcement officer has a negligible 1% chance of foiling a terrorist attempting to hijack an aircraft (due to very low probability of being on a hijacked flight).
- Hardened cockpit door is effective (75%) in preventing entry to the cockpit. This is likely to underestimate the actual likelihood, but we select a lower value in recognition that the flight deck may be vulnerable during 'door transitions'.

Since there are uncertainties with quantifying these probabilities, sensitivity analyses are conducted to assess the robustness of the results.

The probability of a hijacking being foiled, deterred or disrupted without the IPSBs, FFDOs or FAMS is

$$\Pr(\text{hijacking foiled}) = 1-(1-0.1)^{11}(1-0.05)(1-0.10)(1-0.01)(1-0.75) = 93.4\% \quad (3)$$

This likelihood of foiling a hijacking will be higher, and so potential for risk reduction is decreased, if any of the 11 TSA layers of pre-boarding security have detection rates higher than 10%. This is highly likely for passenger and carry-on items screening by metal detectors, X-ray machines and/or Advanced Imaging Technology (AIT) full-body scanners which have high probability of deterring or detecting weapons concealed on the passenger or in their carry-on items. Moreover, terrorist incompetence can generally be expected to increase detection rates.

Schneier (2006) concludes that the only two effective antiterrorism countermeasures implemented after 9/11 were strengthening cockpit doors and passengers learning they need to fight back, and Athol Yates, Executive Director of the Australian Homeland Security Research Centre says that air marshals are of 'questionable' security value, and that 'hardening the cockpit doors and changing the protocols for hijacking has made it harder for terrorists to get weapons on board an aircraft and take control of it' (Maley 2008). It could be argued that these two measures alone reduce the risk of a hijacking to near zero percent. Hence, Eqn. (3) biases the calculations in favour of finding IPSB, FFDOs or FAMS to be cost-effective. That is, an estimate that in total all security measures besides IPSB, FFDOs and FAMS reduce the risk of a successful hijacking by 93.4% is probably quite low.

Information about risk reductions may also be inferred from expert opinions, scenario analysis, and statistical analysis of prior performance data, as well as system and reliability modelling. Nonetheless, the systems approach to modelling effectiveness of aviation security measures described herein is instructive.

As noted, the Airline Pilots Association (International) requests that the 'FFDO program is in need of a significant increase in funding', and the Coalition of Airline Pilots Associations recommends doubling the FFDO budget over five years (CAPA 2011). A policy scenario

might involve doubling the budget, and effectiveness, of the FFDO program, while at the same time reducing funding to FAMS by 75% leaving roughly 500 to 1,000 air marshals available for deployment. This would enable FAMS to target 'high risk' flights in those (apparently exceedingly rare) instances in which there is a credible threat. While there are a myriad of possible policy changes, this is a suggested policy scenario with the potential to reduce expenditure considerably with negligible decrease in risk reduction. Risk reductions are thus calculated for the following scenarios:

1. IPSB only (no FAMS or FFDO)
2. FAMS only (no IPSB or FFDO)
3. FFDO only (no FAMS or IPSB)
4. IPSB+25%FAMS+200%FFDO

### *4.3.1 IPSB only (no FAMS or FFDO)*

If an IPSB is installed, and if we assume it is equally effective as hardened cockpit doors at preventing a hijacking at 75%, the probability a hijacking will be foiled, deterred or disrupted with all the security measures in place except for FFDOs and FAMS increases to

$$\Pr(\text{hijacking foiled}) = 1-(1-0.1)^{11}(1-0.05)(1-0.10)(1-0.01)(1-0.75)(1-0.75) = 98.3\% \quad (4)$$

The additional risk reduction in this case by IPSB is $\Delta R$=98.3-93.4=5.1%.

Risk reduction is an uncertain variable. Using the figures above, the best case scenario is that IPSB are 100% effective in eliminating this remaining risk then the best case risk reduction is $\Delta R$=6.6%. If IPSB is half as effective as assumed above (37.5%), risk reduction is reduced to 2.5%. If passengers and crew are deemed to have zero likelihood of deterring or foiling hijackers, then risk reduction is increased to 5.8%. If detection rates for the 11 TSA layers of pre-boarding security are halved to only 5%, then risk reduction increases to 9.0%. If the hardened cockpit door is half as effective as assumed above (37.5%), then risk reduction increases to 12.5%. Lower and upper bound risk reductions is thus taken as 2.5% and 12.5%, respectively.

### *4.3.2 FAMS only (no IPSB or FFDO)*

If air marshals are on a flight, we expect them to be near 100% effective in foiling a hijacking. This is conditional on air marshals being on the aircraft, however, whereas the probability of air marshals being on the hijacked flight is only near 5%. On the other hand, air marshals are more likely to be on 'high-risk' flights based on intelligence reports, and it follows that the probability of an air marshal being on a flight is higher if terrorists might also be on the flight. However, experience from Australian air marshals is that 'following increases in screening at airports and the installation of bullet-proof cockpit doors, there is little intelligence indicating which flights are at risk', and so now air marshals only 'have random assignments or fly to protect VIPs' (Kearney 2005). Nonetheless, to be conservative it is assumed that the probability of air marshals being on a plane is 10% to account for their increased likelihood of being present on higher risk flights. Hence: Pr(foiled by FAMS)=0.1×100%=10%.

It follows that the probability of a hijacking being foiled, deterred or disrupted with all the security measures in place except for IPSB and FFDO increases to

$$\Pr(\text{hijacking foiled}) = 1-(1-0.1)^{11}(1-0.05)(1-0.10)(1-0.01)(1-0.75)(1-0.1) = 94.0\% \quad (5)$$

The additional risk reduction caused by FAMS is ΔR=94.0-93.4=0.6%.

A lower bound estimate may be based on air marshals being on only 5% of flights, hence Pr(foiled by FAMS)=0.05×100%=5% and ΔR=0.3%. If it is believed that air marshals are on 'high risk' flights or have a higher deterrent capability, then Pr(foiled by FAMS) may increase to 0.25×100%=25%, resulting in ΔR=1.7%. If passengers and crew are deemed to have zero likelihood of deterring or foiling hijackers, and detection rates for the 11 TSA layers of pre-boarding security are halved to only 5%, then risk reduction increases to 1.4%. If the hardened cockpit door is half as effective as assumed above (37.5%), then risk reduction increases to 1.7%. Lower and upper bound risk reductions is thus taken as 0.3% and 2%, respectively.

### *4.3.3 FFDO only (no FAMS or IPSB)*

If FFDOs are in every cockpit, then we expect them to be near 100% effective in foiling a hijacking. This is conditional on an FFDO being on the flight deck. The probability of air marshals being on a hijacked flight is only near 5%, and since FFDOs provide five times more coverage than the FAMS (Flagg 2011), then the probability of FFDOs being on a plane is 25%. Hence: Pr(foiled by FFDO)=0.25×100%=25%.

It follows that the probability of a hijacking being foiled, deterred or disrupted with all the security measures in place except for IPSB and FAMS increases to

$$\Pr(\text{hijacking foiled}) = 1-(1-0.1)^{11}(1-0.05)(1-0.10)(1-0.01)(1-0.75)(1-0.25) = 95.0\% \quad (5)$$

The additional risk reduction caused by FFDOs is ΔR=95.0-93.4=1.6%.

A lower bound estimate may be based on FFDOs being on only 10% of flights, hence Pr(foiled by FFDO)=0.10×100%=10% and ΔR=0.6%. If passengers and crew are deemed to have zero likelihood of deterring or foiling hijackers, and detection rates for the 11 TSA layers of pre-boarding security are halved to only 5%, then risk reduction increases to 3.5%. If the hardened cockpit door is half as effective as assumed above (37.5%), then risk reduction increases to 4.2%. Lower and upper bound risk reductions is thus taken as 0.5% and 5%, respectively.

### *4.3.4 IPSB + 25% FAMS + 200% FFDOs*

If the budget of the FFDO program is doubled to $44 million per year, then the number of FFDOs would double leading to the probability of FFDOs being on a plane as 50%. Hence: Pr(foiled by FFDO)=0.50×100%=50%. Concurrent with this increase in the FFDO program, the funding for FAMS would be reduced 75% to $300 million per year, with a proportional reduction in Pr(foiled by FAMS) from 10% to 2.5%.

The probability of a hijacking being foiled, deterred or disrupted with this new scenario increases to

$$\begin{aligned}&\Pr(\text{hijacking foiled})\\ &= 1-(1-0.1)^{11}(1-0.05)(1-0.10)(1-0.01)(1-0.75)(1-0.75)(1-0.025)(1-0.5) = 99.2\%\end{aligned} \quad (6)$$

The additional risk reduction caused by this policy scenario is ΔR=99.2-93.4=5.8%.

By way of comparison, if the FAMS was not reduced by 75%, but maintained at its present level, then risk reduction increases negligibly by 0.1% to 5.9%. Hence, reducing the cost of FAMS by $900 million will reduce risk reduction by a meagre 0.1%. This observation alone provides strong evidence that the FAMS is not cost-effective.

If IPSB is half as effective as assumed above (37.5%), risk reduction is reduced to 4.6%. If passengers and crew are deemed to have zero likelihood of deterring or foiling hijackers, and detection rates for the 11 TSA layers of pre-boarding security are halved to only 5%, then risk reduction increases to 12.4%. If the hardened cockpit door is half as effective as assumed above (37.5%), then risk reduction increases to 14.6%. Lower and upper bound risk reductions is thus taken as 4.5% and 15%, respectively.

## 4.4 Break-Even Sensitivity Analysis

The analysis will use an expected value cost-benefit analysis using single-point estimates. In principle, a probabilistic analysis could be attempted, such as that described by Stewart and Mueller (2011) for the cost-benefit assessment of AITs where risk reduction and losses were treated as random variables. However, in this case, the information required to accurately assess detection rates for TSA security measures are scarce, so a sensitivity analysis will be conducted using a range of parameter values likely to represent the best and worse cases of risk reduction and losses.

### *4.4.1 IPSB only (no FAMS or FFDO)*

An expected value cost-benefit analysis is one that uses mean values. In this case, the issue under consideration is: What does the yearly probability of an otherwise successful $50 billion attack where hijackers commandeer an airliner and crash it into a building have to be to justify spending $13.5 million per year to reduce the total risk of this possibility by 5.1%? The minimum attack probability for IPSB to be cost-effective is thus 0.5% per year. This is calculated following Eqn. (1) as $13.5 million divided by $50 billion in losses divided by 5.1% risk reduction (see Table 1). Thus, a mean rate of attack of less than one attack every two hundred years would fail an expected value cost-benefit analysis.

This result is derived from analyses applying assumptions biased toward finding the security measure to be cost effective: each pre-boarding security protective measure has only a 10% likelihood of being successful, passengers and crew have only a 5-10% chance of foiling a hijacking attempt, and the hardened cockpit door is only 75% effective. The analysis also assumes a successful attack will cause an average $50 billion in damage, a rather high estimate according to some accountings.

The break-even analysis is applied to a range of risk reductions and losses in Table 1. It is seen that, for the lowest combination of risk reduction and losses, the attack probability needs to exceed 5.4% per year for the IPSB to be cost-effective, and less than 2.7% or one in 40 per year for all other likely combinations of risk reduction and losses. These are relatively low threshold attack probabilities, which suggests that the IPSB is an effective and cost efficient security measure.

| Additional Risk Reduction Caused by IPSB (ΔR) | Losses from a Successful Terrorist Attack ($C_{loss}$) | | | |
|---|---|---|---|---|
| | $10 billion | $50 billion | $100 billion | $200 billion |
| 2.5% | 5.4% | 1.1% | 0.5% | 0.3% |
| 5.1% | 2.7% | 0.5% | 0.3% | 0.1% |
| 12.5% | 1.1% | 0.2% | 0.1% | 0.05% |

Table 1. Minimum Annual Attack Probability for IPSB to be Cost-Effective.

### *4.4.2 FAMS only (no IPSB or FFDO)*

If the FAMS reduces the risk by 0.6% at a cost of $1.2 billion per year, the yearly probability of an otherwise successful $50 billion attack where hijackers commandeer an airliner and crash it into a building has to exceed 400% per year for the FAMS to pass a cost-benefit assessment (see Table 2). Thus, a mean rate of attack of less than four attacks per year would fail an expected value cost-benefit analysis.

The break-even analysis is applied to a range of risk reductions and losses in Table 2. In this case, more than one attack every two years is needed to justify the FAMS even when we more than triple the risk reduction and double the losses. Such high attack probabilities are not being observed, which strongly suggests that the FAMS fails a cost-benefit assessment.

| Additional Risk Reduction Caused by FAMS (ΔR) | Losses from a Successful Terrorist Attack ($C_{loss}$) | | | |
|---|---|---|---|---|
| | $10 billion | $50 billion | $100 billion | $200 billion |
| 0.3% | 4,000% | 800% | 400% | 200% |
| 0.6% | 2,000% | 400%[1] | 200% | 100% |
| 2.0% | 600% | 120% | 60% | 30% |

[1] 4.0 attacks per year

Table 2. Minimum Annual Attack Probability for FAMS to be Cost-Effective.

### *4.4.3 FFDO only (no FAMS or IPSB)*

If the FFDO program reduces the risk by 1.6% at a cost of $22 million per year, the yearly probability of an otherwise successful $50 billion attack where hijackers commandeer an airliner and crash it into a building has to exceed 2.8% per year for the FFDOs to pass a cost-benefit assessment (see Table 3). Thus, a mean rate of attack of less than one attack every 35 years would fail an expected value cost-benefit analysis.

The break-even analysis is applied to a range of risk reductions and losses in Table 3. It is seen that, for the lowest combination of risk reduction and losses, the attack probability needs to exceed 44% per year for the FFDO program to be cost-effective, and less than 13.8% or one in seven per year for all other likely combinations of risk reduction and losses. These are relatively low threshold attack probabilities, which suggests that the FFDO program is an effective and cost efficient security measure.

| Additional Risk Reduction Caused by FFDOs (ΔR) | Losses from a Successful Terrorist Attack ($C_{loss}$) | | | |
|---|---|---|---|---|
| | $10 billion | $50 billion | $100 billion | $200 billion |
| 0.5% | 44.0% | 8.8% | 4.4% | 2.2% |
| 1.6% | 13.8% | 2.8% | 1.4% | 0.7% |
| 5.0% | 4.4% | 0.9% | 0.4% | 0.2% |

Table 3. Minimum Annual Attack Probability for FFDOs to be Cost-Effective.

### *4.4.4 IPSB + 25% FAMS + 200% FFDOs*

The results above show that although the FAMS does reduce risk, almost all of that benefit can be obtained with very inexpensive measures: the installation of physical secondary barriers (IPSB) and Federal Flight Deck Officers (FFDOs). Hence, a policy scenario that reduces reliance on FAMS, and increases the role of FFDOs may be optimal. The policy scenario where the budget of the FFDO program is doubled and funding for FAMS cut by 75% is now examined. This policy scenario will reduce the risk by 5.8% at a cost of $357.5 million per year. In this case, the yearly probability of an otherwise successful $50 billion attack where hijackers commandeer an airliner and crash it into a building has to exceed 12.3% per year or one attack every eight years for this policy scenario to pass a cost-benefit assessment (see Table 4).

The break-even analysis is applied to a range of risk reductions and losses in Table 4. The highest attack probability is 79.4% for the combination of lowest risk reduction and lowest losses. For all other combination of risk reduction and losses the attack probability needs to exceed one attack every two years for this policy scenario to be cost-effective.

| Additional Risk Reduction (ΔR) | Losses from a Successful Terrorist Attack ($C_{loss}$) | | | |
|---|---|---|---|---|
| | $10 billion | $50 billion | $100 billion | $200 billion |
| 4.5% | 79.4% | 15.9% | 7.9% | 4.0% |
| 5.8% | 61.6% | 12.3% | 6.2% | 3.1% |
| 15.0% | 23.8% | 4.8% | 2.4% | 1.2% |

Table 4. Minimum Annual Attack Probability for Policy Scenario 4 ( IPSB + 25% FAMS + 200% FFDOs) to be Cost-Effective.

### *4.4.5 Summary of Results*

Table 5 summarises the risk reduction, cost and minimum annual attack probability for each security measure to be cost effective, for losses sustained in a successful attack of $50 billion.

| Security Measure | Additional Risk Reduction (ΔR) | Cost ($ million) | Minimum Annual Attack Probability for Security Measure(s) to be Cost-Effective for Losses of $50 Billion |
|---|---|---|---|
| IPSB only (no FAMS or FFDO) | 5.1% | 13.5 | 0.5% |
| FAMS only (no IPSB or FFDO) | 0.6% | 1,200 | 400%[1] |
| FFDO only (no FAMS or IPSB) | 1.6% | 22.0 | 2.8% |
| IPSB + 25% FAMS + 200% FFDOs | 5.8% | 357.5 | 12.3% |

[1] 4.0 attacks per year

Table 5. Summary of Results.

### 4.5 Discussion

While we have tried to err on the generous side - i.e. towards approving the cost-effectiveness of the FAMS, FFDOs or IPSB - we recognise that the probability estimates for effectiveness of security measures are uncertain and subjective. If the effectiveness of passengers and crew are doubled to 10% and 20% respectively, a low likelihood by some, then risk reduction is $\Delta R$=4.2%, $\Delta R$=0.6%, and $\Delta R$=1.4% for IPSB, FAMS and FFDOs, respectively. These risk reductions are still within the range depicted in Tables 1 to 3. Moreover, if opportunity costs are considered then this would increase the threshold attack probabilities.

It may be argued that many security measures may provide a type of 'security theatre' that will make travellers feel safer which in itself is beneficial. We have ignored any possible security theatre benefits - likely, however, to be small as there is little evidence that FAMS, FFDOs or IPSB by themselves will make travellers feel much safer. However, this is an area for further research.

The present paper has shown the utility of systems and reliability modelling for cost-benefit analysis for homeland security expenditure. The results suggest that the threat likelihood needs to be exceedingly high for FAMS to be cost-effective. But we recognise that the preliminary cost-benefit analysis conducted herein will not necessarily give a definitive answer to whether FAMS, FFDOs or IPSB are cost-effective. A more detailed and comprehensive study is required to properly model the complex interactions and interdependencies in aviation security. This paper provides a starting point for this type of analysis. The assumptions and quantifications made here can be queried, and alternate hypotheses can be tested in a manner which over time will minimise subjectivity and parameter uncertainty inherent in an analysis for which there are little accurate data. This should lead to more widespread understanding and agreement about the relative cost-effectiveness of aviation and other counter terrorism security measures.

## 5. CONCLUSIONS

We have generally underestimated the likely risk reduction supplied by existing security measures. However, even with these assumptions in place, it appears that the expensive Federal Air Marshal Service very substantially fails a cost-benefit assessment. Moreover, insofar as FAMS does reduce risk, almost all of that benefit can be obtained with a very inexpensive mix of security measures: the installation of physical secondary barriers (IPSB)

to entering the cockpit for those brief and fleeting moments when the cockpit door is opened during flight, and doubling the budget of the Federal Flight Deck Officer program. Overall, a policy that includes IPSBs, an increased budget for FFDOs, and a reduced budget for FAMS may well be optimal.

## ACKNOWLEDGEMENTS

The first author appreciates the financial support of the Australian Research Council. The second author appreciates the financial support of a Distinguished Scholar Award at Ohio State University.

## REFERENCES

ABC (2010), Obama Orders Air Marshals Surge by Feb. 1: 'Race Against Time', *abc News*, Jan 6.

ALPA (2007), *Secondary Flight Deck Barriers and Flight Deck Access Procedures: A Call for Action*, ALPA White Paper, Airline Pilots Association International, Washington, D.C. , July.

AT (2004), United Airlines Installing Secondary Security Barrier for Cockpit Protection, *Aviation Today*, September 27.

Akhtar, J., Bjornskau, T. and Veisten, K. (2010), Assessing Security Measures Reducing Terrorist Risk: Inverse ex-post cost-benefit and cost-effectiveness analyses of Norwegian airports and seaports, *Journal of Transportation Security*, 3: 179-195.

Biringer, B.E., Matalucci, R.V. and O'Connor, S.L. (2007), *Security Risk Assessment and Management*, Wiley, New Jersey.

Blomberg, S.B. and Rose, A.Z. (2009), Editor's Introduction to the Economic Impacts of the September 11, 2001, Terrorist Attacks, *Peace Economics, Peace Science, and Public Policy*, 15(2):1-14.

Bonham, C., Edmonds, C. and Mak, J. (2006), The Impact of 9/11 and Other Terrible Global Events on Tourism in the United States and Hawaii, *Journal of Travel Research*, 45(1):99-110.

Bram, J., Orr, J. and Rapaport, C. (2002), Measuring The Effects of the September 11 Attack on New York City, *FRBNY Economic Policy Review*, November, 5-20.

CAPA (2011), Federal Flight Deck Officer (FFDO) Program, Coalition of Airline Pilots Associations, Washington, D.C., September 22.

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

Cox, L.A. (2009), Improving Risk-Based Decision-Making for Terrorism Applications, *Risk Analysis*, 29(3): 336-341.

Dillon, R.L., Liebe, R. and Bestafka, T. (2009), Risk-based Decision Making for Terrorism Applications, *Risk Analysis*, 29(3): 321-335.

DHS (2010), Budget-in-Brief Fiscal Year 2011, U.S. Department of Homeland Security, Washington, DC,

Ellig, J., Guiora, A, and McKenzie, K. (2006), *A Framework for Evaluating Counterterrorism Regulations*, Policy Resource No. 3, Mercatus Center, George Mason University, September.

Ellingwood, B.R. (2006), Mitigating Risk from Abnormal Loads and Progressive Collapse, *Journal of Performance of Constructed Facilities*, 20(4): 315-323.

FAA (2002), FAA Sets New Standards for Cockpit Doors. Federal Aviation Administration Office of Public Affairs Press Release, January 11, 2002.

FAA (2003), Airlines Meet FAA's Hardened Cockpit Door Deadline. Federal Aviation Administration Office of Public Affairs Press Release, April 2003.

Farrow, S. and Shapiro, S. (2009), The Benefit-Cost Analysis of Security Focused Regulations, *Journal of Homeland Security and Emergency Management*, 6(1):Article 25.

Fischhoff, B. (2005), A Hero in Every Seat. *New York Times*, August 7.

Fischer, P., Krueger, J.I., Greitemeyer, T., Vogrincic, C., Kastenmuller, A., Frey, D. et al. (2011), The Bystander-Effect: A Meta-Analytic Review on Bystander Intervention in Dangerous and Non-Dangerous Emergencies, *Psychological Bulletin*, 137(4): 517-537.

Flagg, M.W. (2011), Statement of Marcus W. Flagg, President Federal Flight Deck Officers Association before the Committee on Homeland Security and Government Affairs, November 1.

Frank, T. (2008), More than 10% of pilots allowed to fly armed, *USA Today*, April 1.

Friedman, B.H. (2010), Managing Fear: the Politics of Homeland Security, in *Terrorizing Ourselves: why U.S. counterterrorism policy is failing and how to fix it*, Benjamin H. Friedman, Jim Harper, and Christopher A. Preble (Eds.), Cato Institute, 2010.

Griffin, D. (2008), Sources: Air marshals missing from almost all flights, *CNN.com*, March 25, 2008.

Griffin, D. (2010), Four Arrests for $800M, *CNN.com*, February 4.

Hahn, R.W. (2008), *An Analysis of the 2008 Government Report On the Costs and Benefits of Federal Regulations*, Regulatory Analysis 08-04, AEI Center for Regulatory and Market Studies, December 2008, pp. 8-9.

Hook, S. (2008), Assessing Expenditure in Individual Agencies: the Case of the Australian Federal Police *in Risky business: Measuring the costs and benefits of counter-terrorism spending*, by Carl Ungerer, Henry Ergas, Scott Hook and Mark Stewart, Australian Strategic Policy Institute, November 18 2008.

Hudson, A. (2004), Air Marshals Cover Only a Few Flights. *Washington Times*, August 16.

Hudson, A. (2005), Flight Marshal Numbers Disputed, Agents Criticize Data 'Padding'. *Washington Times*, March 3.

Jordaan, I. (2005), *Decisions Under Uncertainty: Probabilistic Analysis for Engineering Decisions*, Cambridge University Press, Cambridge, U.K.

Kearney, S. (2005), Air Marshal's Role Now VIP Security, *The Australia*n, 9 December.

Kenney, M. (2010), 'Dumb' yet Deadly: Local Knowledge and Poor Tradecraft among

Islamist Militants in Britain and Spain, *Studies in Conflict and Terrorism*, 31:1-22.

Kramer, M. (2004), The Perils of Counterinsurgency: Russia's War in Chechnya. *International Security*, 29(3):5-63.

Krugman, P. (2004), *The Costs Of Terrorism: What Do We Know?*, Briefing Note, The Nexus of Terrorism & WMDs: Developing a Consensus*,* Princeton University, December 12-14.

Little, R.G. (2007), Cost-Effective Strategies to Address Urban Terrorism: A Risk Management Approach, in *The Economic Costs and Consequences of Terrorism*, H.W. Richardson, P. Gordon and J.E. Moore II (eds.), Edward Elgar Publishing, Cheltenham, UK, 98-115.

Lott, J.R. (2004), Marshals Are Good, But Armed Pilots are Better, *Wall Street Journal Europe*, January 2.

Low, H.Y. and Hao, H. (2002), Reliability Analysis of Direct Shear and Flexural Failure Modes of RC Slabs Under Explosive Loading, *Engineering Structure,* 24(2):189-198.

Maley, P. (2008), Overhaul Cuts Sky Marshals by a Third., *The Australian*, January 23.

Meckler, L. and Carey, S. (2007), Sky Patrol: U.S. Air Marshal Service Navigates Turbulent Times. *The Wall Street Journal*, February 9.

Meeks, B.N. (2004) For Air Marshals, Less Equals More, MSNBC, September 15.

Moak, L. (2011), Letter to House Subcommittee on Transportation Security, President of Airline Pilots Association International, July 12, 2011.

Mueller, J. (2006), *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. Free Press, New York.

Mueller, J. (2010), Assessing Measures Designed to Protect the Homeland, *Policy Studies Journal*, 38 (1): 1-21.

Mueller, J. (ed.) (2011), *Terrorism Since 9/11: The American Cases*. Mershon Center, Ohio State University, Columbus, Ohio.

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

Mueller, J. and Stewart, M.G. (2011b), The Price is Not Right: The U.S. spends too much money to fight terrorism, *Playboy*, 58(10), 149-150.

Murphy, P. and Hudson, P. (2003), Heroes Foil Qantas Hijack Attack, *The Age*, May 30.

NRC (2010), *Review of the Department of Homeland Security's Approach to Risk Analysis*, Committee to Review the Department of Homeland Security's Approach to Risk Analysis, National Research Council, National Academic Press, Washington D.C.

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

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

Pate-Cornell, E. and Guikema, S. (2002), Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Counter-measures, *Military Operations Research*, 7(4):5-23.

Poe, T. (2005), Department of Homeland Security Appropriations Act, 2006: Amendment No. 10. House of Representatives, May 17.

Poole, R.W. (2008), *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, 11-12 December.

RTCA (2010), Airplane Secondary Barriers and Alternative Flight Deck Security Procedures, Terms of Reference, *Radio Technical Commission for Aeronautics, Special Committee 221*, RTCA Paper No. 116-10/PMC-801, Washington, D.C., June 10.

RTCA (2011), Aircraft Secondary Barriers and Alternative Flight Deck Security Procedures, Final Report, *Radio Technical Commission for Aeronautics, Special Committee 221*, RTCA DO-329, Washington, D.C., September 28.

Sandler, T. and Enders, W. (2005), *Economic Consequences of Terrorism in Developed and Developing Countries: An Overview*, World Bank Working Paper.

Schneier, B. (2006), *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Copernicus, New York.

Smith, P. (2007), The Airport Security Follies. *nytimes.com*, December 28.

Stewart, M.G. and Melchers, R.E. (1997), *Probabilistic Risk Assessment of Engineering Systems*. London. Chapman & Hall.

Stewart, M.G., Netherton, M.D. and Rosowsky, D.V. (2006), Terrorism Risks and Blast Damage to Built Infrastructure. *Natural Hazards Review* 7(3):114-122.

Stewart, M.G. and Netherton, M.D. (2008), Security Risks and Probabilistic Risk Assessment of Glazing Subject to Explosive Blast Loading. *Reliability Engineering and System Safety*, 93(4): 627-638.

Stewart, M.G. (2008), Cost-Effectiveness of Risk Mitigation Strategies For Protection of Buildings Against Terrorist Attack, *Journal of Performance of Constructed Facilities*, ASCE, 22(2):115-120.

Stewart, M.G. and Mueller, J. (2008), A Risk and Cost-Benefit Assessment of U.S. Aviation Security Measures, *Journal of Transportation Security*, 1(3):143-159.

Stewart, M.G. (2010), Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-Terrorism Protective Measures for Infrastructure, *International Journal of Critical Infrastructure Protection*, 3(1): 29-40.

Stewart, M.G. (2011), Life Safety Risks and Optimisation of Protective Measures Against Terrorist Threats to Infrastructure, *Structure and Infrastructure Engineering,* 7(6): 431-440.

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

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

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

Twisdale, L.A., Sues, R.H. and Lavelle, F.M. (1994), Reliability-based Design Methods for Protective Structures. *Structural Safety*. 15(1-2):17-33.

Wilber, D.Q. (2007), Defense Training Goes Begging for Airline Crews, *Washington Post*, April 28.

Willis, H.H., LaTourrette, T., Kelly, T.K., Hickey, S. and Neill, S. (2007), *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, RAND Corporation, Santa Monica, CA.

Willis, H. and 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.

von Winterfeldt, D. and O'Sullivan, T.M. (2006), Should WE Protect Commercial Airplanes Against Surface-to-Air Missile Attacks by Terrorists?, *Decision Analysis*, 3(2): 63-75.

**THE UNIVERSITY OF NEWCASTLE**

**SCHOOL OF ENGINEERING**

**CIVIL, SURVEYING AND ENVIRONMENTAL ENGINEERING**

## RESEARCH REPORTS

This report is one of a continuing series of Research Reports published by Civil, Surveying and Environmental Engineering at the University of Newcastle. Requests for a detailed list and/or copies of other reports should be addressed to:

The Secretary
Civil, Surveying and Environmental Engineering
The University of Newcastle
University Drive
CALLAGHAN NSW 2308

Email: Cherie.Pilgrim@newcastle.edu.au
Telephone: (02) 4921 6058
Facsimile : (02) 4921 6991