Risk and Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening

Mark G. Stewart and John Mueller

Research Report No. 280.11.2010

January 2011

ISBN No. 9780 9807 6187 0
RISK AND COST-BENEFIT ANALYSIS OF ADVANCED IMAGING TECHNOLOGY
FULL BODY SCANNERS FOR AIRLINE PASSENGER SECURITY SCREENING

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
phone: +61 2 49216027   email: mark.stewart@newcastle.edu.au

John Mueller
Professor of Political Science and Woody Hayes Chair of National Security Studies
Mershon Center for International Security Studies and Department of Political Science
Ohio State University
Columbus, Ohio 43201, United States
phone: +1 614 2476007   email: bbbb@osu.edu

ABSTRACT
The Transportation Security Administration (TSA) has been deploying Advanced Imaging Technologies (AIT) that are full-body scanners to inspect a passenger’s body for concealed weapons, explosives, and other prohibited items. The terrorist threat that AITs are primarily dedicated to is preventing the downing of a commercial airliner by an IED (Improvised Explosive Device) smuggled on board by a passenger. The cost of this technology will reach $1.2 billion per year by 2014. The paper develops a cost-benefit analysis of AITs for passenger screening at U.S. airports. The analysis considered threat probability, risk reduction, losses, and costs of security measures in the estimation of costs and benefits. Since there is uncertainty and variability of these parameters, three alternate probability (uncertainty) models were used to characterise risk reduction and losses. Economic losses were assumed to vary from $2-50 billion, and risk reduction from 5-10%. 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, based on mean results, more than one attack every two years would need to originate from U.S. airports for AITs to pass a cost-benefit analysis. In other words, to be cost-effective, AITs every two years would have to disrupt more than one attack effort with body-borne explosives that otherwise would have been successful despite other security measures, terrorist incompetence and amateurishness, and the technical difficulties in setting off a bomb sufficiently destructive to down an airliner. The attack probability needs to exceed 160-330% per year to be 90% certain that AITs are cost-effective.

1. INTRODUCTION

Since the events of 9/11 there has been much focus on preventing or mitigating damage and casualties caused by terrorist activity. A key issue is whether counter-terrorism expenditure has been invested in a manner that optimises public safety in a cost-effective manner. This is why the 9/11 Commission report, amongst others, called on the U.S. government to implement security measures that reflect assessment of risks and cost-effectiveness (NC 2004). However, while the U.S. requires a cost-benefit analysis for government regulations (OMB 1992), this does not appear to have happened for most homeland security expenditures. On the other hand, cost-benefit and other risk acceptance studies are routinely conducted by the Nuclear Regulatory Commission, the Environmental Protection Agency, the Federal Aviation Administration, and other agencies even on politically-charged issues. These studies are particularly useful for low probability – high consequence events where public safety is a key criterion for decision-making.

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. Benjamin Friedman from the Cato Institute believes that “One strategy … is to enhance the use of cost-benefit analysis in DHS - institutionalizing rationality in a more technocratic DHS” (Friedman 2010). And Robert Hahn from the American Enterprise Institute Center for Regulatory and Market Studies also recommends that the “Department of Homeland Security should quantify and monetize the benefits of antiterrorism regulations” and “While determining precise quantitative estimates of benefits is often difficult, some quantitative or qualitative description may be possible. Even if estimates are not precise, some measure of whether the regulations will likely improve things would be useful.” (Hahn 2008). The need for DHS to adopt a risk-based approach (that includes cost-benefit analyses) has also been made by Poole (2008), who also states that “No security policy should be pursued “at all costs,” since resources are always limited” and “While it seems likely that commercial aviation will remain a high profile potential target, spending billions every year on static defenses at airports is almost certainly a poor use of resources.” Yet despite the massive expenditures involved, a senior economist at the Department of Homeland Security acknowledged five years after 9/11 that “We really don't know a whole lot about the overall costs and benefits of homeland security” (Anderson 2006). That condition does not seem to have changed in the intervening years.

The need for the DHS to develop and implement a risk-based framework lead to a 2008 U.S. Congress request to the U.S. National Research Council (NRC) to “assess how the Department of Homeland Security (DHS) is building its capabilities in risk analysis to inform decision making” (NRC 2010). The NRC committee was a multidisciplinary group with technical, public policy, and social science expertise and experience concerning the areas of DHS’s responsibilities. After a 15 month study period, 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. Moreover, it is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses other than for natural disasters.” and that “only low confidence should be placed in most of the risk analyses conducted by DHS.” More damning: “DHS has not been following the critical scientific practices of documentation, validation, peer review by technical experts external to DHS, and publishing. Given the lack of that disciplined approach, it is very difficult to know precisely how DHS risk analyses are being done and whether their results are reliable and useful in guiding decisions.” The NRC report compiles a litany of concerns about DHS risk analyses,
particularly their lack of documentation, transparency and peer-review.

To compare costs and benefits requires the quantification of threat probability, risk reduction, losses, and costs of security measures. This 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, Stewart and Netherton 2008, Stewart 2008, 2010, 2011). Much of this work can be categorised as ‘probabilistic terrorism risk assessment’ (Willis et al. 2007).

Stewart (2010, 2011) has shown that, based on expected values, the threat probability has to be very high for typical counter-terrorism measures for buildings and bridges to be cost-effective. Similar cost-benefit analyses have shown that the U.S. Federal Air Marshal Service which costs over $1 billion per year fails to be cost-effective, but that hardening cockpit doors is very cost-effective (Stewart and Mueller 2008a). 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). This suggests, not surprisingly, that policy makers within the U.S. government and the DHS are risk-averse.

Terrorism is a frightening threat that influences 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 (e.g., Sunstein 2002, Faber and Stewart 2003, Ellingwood 2006). Follow-on consequences from a terrorist attack such as loss of consumer confidence leading to economic decline, reduced tourism, and reduced government/tax revenue should be included in the estimation of losses in a ‘risk-neutral’ or expected value risk analysis. Hence, governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making. This is confirmed by the OMB which specifically states “the standard criterion for deciding whether a government program can be justified on economic principles is net present value - the discounted monetized value of expected net benefits (i.e., benefits minus costs)” and that “expected values (an unbiased estimate) is the appropriate estimate for use” (OMB 1992). The OMB also recognises that there are uncertainties in cost-benefit analyses and recommend: “Estimates of benefits and costs are typically uncertain because of imprecision in both underlying data and modelling assumptions. Because such uncertainty is basic to many analyses, its effects should be analyzed and reported. Useful information in such a report would include the key sources of uncertainty; expected value estimates of outcomes; the sensitivity of results to important sources of uncertainty; and where possible, the probability distributions of benefits, costs, and net benefits.”

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 2006, Willis and LaTourette 2008, Winterfeldt and O’Sullivan 2006, Akhtar et al. 2010). Hence, we will undertake a ‘break even’ cost-benefit analysis that will also include uncertainty modelling of losses and risk reduction.

The Transportation Security Administration (TSA) has been deploying Advanced Imaging Technologies (AIT) that are full-body scanners to inspect a passenger’s body for concealed weapons, explosives, and other prohibited items. As we will see later, the cost of this technology will reach $1.2 billion per year by 2014. Yet, before deciding to install AITs at considerable cost the TSA has not conducted a cost-benefit analysis of AITs. The U.S. Government Accountability Office (GAO) remarked in 2010 that “Cost-benefit analyses are important because they help decision makers determine which protective measures, for instance, investments in technologies or in other security programs, will provide the greatest mitigation of risk for the resources that are available.” And it specifically pointed out that “conducting a cost-benefit analysis of TSA’s AIT deployment is important. An updated cost-benefit analysis would help inform TSA’s judgment about the optimal deployment strategy for the AITs, as well as provide information to inform the best path forward, considering all elements of the screening system, for addressing the vulnerability identified by this attempted terrorist attack.” (Lord 2010). This absence of a cost-benefit analysis for AITs is the motivation for the present study. This study will also include uncertainty analysis in the cost-benefit calculations to reflect the uncertainty in underlying data and modelling assumptions, and will allow the probability of cost-effectiveness to be calculated.

The terrorist threat that AITs are primarily dedicated to is preventing the downing of a commercial airliner by an IED (Improvised Explosive Device) smuggled on board by a passenger. Since AITs operated by the TSA are effective only for passengers leaving or flying within the U.S., the present paper considers the threat probability, risk reduction and losses for a suicide bomber who attempts to board an aircraft at a U.S. airport. The paper focuses on aviation security in the U.S., however, AITs are being trialled or deployed in the U.K., France, Netherlands, Italy, Canada, Australia and Russia (EC 2010) which will cost many billions of dollars if they are also used for primary screening in those countries. Hence, the present paper will provide useful guidance to U.S. and international aviation security regulators.

2. RISK AND COST-BENEFIT METHODOLOGY

A security measure is cost-effective when the benefit of the measure outweighs the costs. The benefit of a security measure is a function of three elements:

\[
\text{Benefit} = p_{\text{attack}} \times C_{\text{loss}} \times \Delta R
\]

1. \(p_{\text{attack}}\): 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. \( C_{\text{loss}} \): 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.

The level of existing risk is \( p_{\text{attack}} \times C_{\text{loss}} \) and the benefit is the extent to which existing risks are reduced by an additional security measure. The *net benefit* is the benefit minus the *costs* of providing the risk-reducing security that are required to attain the benefit (\( C_{\text{security}} \)) leading to

\[
\text{Net Benefit} = \frac{p_{\text{attack}} \times C_{\text{loss}} \times \Delta R}{\text{benefit}} - \frac{C_{\text{security}}}{\text{cost}}
\]

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. **COST-BENEFIT ASSESSMENT OF ADVANCED IMAGING TECHNOLOGIES (AIT)**

3.1 **Costs of the Security Measure (\( C_{\text{security}} \))**

The TSA began rolling out AITs from 2009, and by the end of 2011 there will be 1,000 scanners that will provide coverage at 75% of Category X airports (U.S. largest and busiest airports, and so viewed as vulnerable to terrorism) and 60 percent of the total lanes at Category X through II airports (DHS 2010a). The TSA will use AITs as a primary screening measure, and to this end plans to procure and deploy 1,800 AITs by 2014 to reach full operating capacity (Lord 2010). The costs are considerable. The DHS FY2011 budget request for 500 new AITs includes $214.7 million for their purchase and installation ($430,000 each), $218.9 million for 5,355 new Transportation Security Officers (TSOs) and screen managers to operate the AITs at the checkpoints, and $95.7 million for 255 positions to fund the support and airport management costs associated with the 5,355 new TSOs and screener managers.
(DHS 2010b). In addition, this equipment will require maintenance, support and upgrading. Gale Rossides, Acting Administrator of the TSA, states that the annualised cost of purchasing, installing, staffing, operating, supporting, upgrading, and maintaining the first 1,000 units is about $650 million per year (Rossides 2010). We can then infer that 1,800 units will cost approximately $1.2 billion per year and will give 100% coverage at all airports in the U.S. The assumed 100% coverage may be too generous as the planned roll out of 1,800 scanners may still leave 500 airport checkpoints without AITs (Halsey 2010). If correct, the purchase, operation and maintenance of additional scanners will add considerably to the $1.2 billion cost used herein.

Since AITs provide scans that reveal genitals and other personal information, passengers who opt-out of an AIT are subject to pat-downs with “TSA agents using their open hands to search the clothed genital areas of passengers” which has “drawn huge web traffic, further escalating the controversy” (Memoli and Bettett 2010). This perceived invasion of privacy (EC 2010), inconvenience, or extra delays during screening, may deter some from travelling by air, and for short-haul passengers, to drive to their destination instead. Since driving is far riskier than air travel, the extra automobile traffic generated by existing aviation security measures has been estimated to result in 500 or more extra road fatalities per year (Blalock et al. 2007). Using DHS mandated value of statistical life of $6.5 million (Robinson 2008), this equates to a loss of $3.2 billion per year. On the other hand, it may be argued that “full body scanners area type of ‘security theatre’, and have little tangible effect on deterring terrorism, the mere act of making travellers feel safer may in itself be beneficial.” (Silver 2010). Whether AITs will result in opportunity costs or not is beyond the scope of the present paper, but is an area in need of quantitative research as opportunity costs might be many multiples of the direct cost of security measures. In the present paper, we will assume that AITs will cost approximately $1.2 billion per year and will ignore opportunity costs - although, as indicated, these have the potential to be very substantial. We also ignore any possible security theatre benefits - likely, however, to be small if not negligible.

3.2 Losses Sustained in a Successful Attack (C_loss)

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 billion1 (Chow et al 2005). Since the scenario hypothesised in the RAND study was the downing of an airliner by a shoulder fired missile, then a shutdown of U.S. airspace for a week would cause 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.

Another study on the economic impacts of a terrorist attack using shoulder fired missiles also assumed a seven day shutdown, but a two-year period of recovery (Gordon et al 2007). Losses were summed across airline, ground transportation, accommodation, food, gifts/shopping and amusement sectors, and then applied input-output multipliers of 1.2 and 3.6 to derive overall loss estimates of $214 billion to $420 billion. While the study factored in growth in consumption of telecommunication services, they include losses of over $55 billion and $30 billion for the gifts/shopping and amusement sectors, respectively. This seems overly conservative. Moreover, adding up individual sectoral losses can lead to double counting (Enders and Olsen 2011). Enders and Olsen (2011) observe: “Another reason to avoid adding

1 Assumed a value of life at only $2-2.5 million.
up the sectoral losses is that large scale terrorist attacks cause reallocations of people and resources across sectors. For example, in conjunction with the 9/11-induced decline in air travel, many U.S. tourist destinations experienced increased demand as people took fewer vacations necessitating an airplane flight and more vacations to areas that were within driving distance from their home.” and “The problem, of course, that it is relatively easy to measure the heavy losses experienced by some areas but very difficult to measure the small indirect gains experienced by thousands of areas.” The losses reported by Gordon et al. (2007) are thus likely to over-estimate actual losses.

The downing of an airliner due to a passenger-borne IED is likely not to trigger the same response as downing caused by a shoulder fired missile as no counter-measures exist for a missile attack that could be implemented quickly (such as installing laser jammers on each aircraft). On the other hand, a series of screening measures were implemented quickly following the 9/11 and subsequent attacks, such as screening of shoes following the 2001 failed attempt by Richard Reid and the banning of liquids in carry-on luggage immediately after foiling the August 2006 transatlantic plot to detonate liquid explosives on up to 10 commercial aircraft. While their effectiveness is in doubt, they do provide assurance to the general public that it is safe to fly. An attack involving a shoulder-fired missile would be “much more difficult to convince the public that it is safe to fly” (Pena 2005). The economic costs forecast in the above studies assumed a one week shutdown of U.S. airspace. However, for our scenario of a suicide bomber, a shutdown of a few days would be more reasonable considering that airspace over the U.S. was shutdown for three days following 9/11. This all suggests that the losses forecast above for a shoulder-fired missile attack will over-estimate losses for our threat scenario.

A 2008 report for the DHS by Robinson (2008) concludes that the best estimate for value of a statistical life (VSL) for homeland security analysis is $6.5 million in 2010 dollars. If we take 300 lives at VSL of $6.5 million then the economic loss caused by 300 fatalities is approximately $2 billion. If we add the cost of a large commercial airliner of $200-250 million then direct economic loss is approximately $2.5 billion if we also include forensic and air transport crash investigations. Passenger numbers less than 300 will reduce direct losses considerably, for example, 150 passenger will reduce direct losses to $1.5 billion. However, we will select $C_{loss} = $2 billion as a reasonable lower bound.

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).

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 behavioral 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 a telling 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 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.

While the $15 billion proposed by the RAND study would be a plausible upper value of economic loss, it may fail to consider full losses to the economy. As we saw above, losses sustained after the 9/11 attacks ranged form 0.3 to 1.0 percent of annual GDP. The economic consequences of a suicide bomber would likely be less than the shocking events of 9/11, so we will assume that a reasonable upper bound of losses is 0.3% of GDP or $42 billion plus loss of 300 lives at VSL of $6.5 million ($2 billion) plus cost of a commercial airliner ($250 million) which totals nearly $45 billion - which we will round up to $\text{Loss} = $50 billion.

Results from uncertainty and probabilistic modelling may be sensitive to the shape of the probability distribution selected to represent uncertainty and variability of the parameter of interest. In this case, we will assume three alternate probability distributions of loss (see Figure 1):

1. Normal Distribution - loss is normally distributed with 95% confidence interval between $2 billion and $50 billion, then mean loss is $26 billion and standard deviation is $12.2 billion. Since the normal distribution is unbounded, and to prevent generation of unrealistically low losses, the minimum loss is truncated at $500 million to represent loss of a single aircraft with few passengers and no indirect losses.
2. Uniform Distribution - equal likelihood of any loss between $2 billion and $50 billion, with mean loss of $26 billion.
3. Triangular Distribution - higher likelihood of smaller losses bounded by $2 billion and $50 billion, with a mean loss of $18 billion.
3.3 Reduction in Risk Due to the Security Measure ($\Delta R$)

The Advanced Imaging Technology (AIT) is a primary screening device to inspect a passenger’s body for concealed weapons (metal and non-metal), explosives, and other prohibited items. A key motivation for the rapid deployment of AITs was the foiled 2009 Christmas Day plot by Umar Farouk Abdulmutallab to hide liquid explosives in his underwear to blow-up Northwest Airlines Flight 253. There is little doubt that that full-body scanners improve the ability to detect weapons and explosives, however, there is doubt about their ability to detect all explosives that may be hidden on a person. The GAO follows this line of reasoning “While TSA officials stated that the laboratory and operational testing of the AIT included placing explosive material in different locations on the body, it remains unclear whether the AIT would have been able to detect the weapon Mr. Abdulmutallab used in his attempted attack based on the preliminary TSA information we have received” (Lord 2010). The TSA uses two types of imaging technology, millimeter wave and backscatter. A National Research Council study in 2007 concluded that “The technology base for millimeter-wavelength/terahertz security screening is expanding rapidly internationally, yet there is insufficient technology available to develop a system capable of identifying concealed explosives” (NRC 2007).

It is also suggested that existing screening methods, such as detectors that test swabs wiped on passengers and luggage for traces of explosives, would have detected the explosives used in the 2009 Christmas Day attack (Hsu 2009). Moreover, while the search for explosives is important “You need to look for some type of detonator, which is easier to find than the explosives themselves because most types of detonators have metal in them—a wire or a microchip, for example—that triggers a small spark or electrical signal,” says physicist Kurt Becker from the Polytechnic Institute of New York University (Greenemeier 2010).

Also relevant is the fact that it is not necessarily easy to blow up an airliner even if a bomb detonates. Airplanes are designed to be resilient to shock, and attentive passengers and airline personnel complicate the terrorists’ task further. Apparently, the explosion over Lockerbie...
was successful only because the suitcase bomb just happened to have been placed at the one place in the luggage compartment where it could do fatal damage. According to Christopher Ronay, former head of the FBI bomb unit, if the bomb had been placed where it was surrounded by other luggage to absorb the blast, the passengers and the plane would have survived (Bayles 1996).

Logically, then, a terrorist will not leave such matters to luck, which may be why the shoe and underwear bombers both carried their bombs onto the planes and selected window seats that are, of course, right next to the fuselage (Woods 2009, Johnson and Dugan 2009). Yet even if their bombs had exploded, the airliner might not have been downed. The underwear bomber was reported to be carrying 80 grams of the explosive PETN (PETN or Pentaerythritol tetranitrate is one of the strongest known high explosives, and it is also difficult to detect) and when his effort was duplicated on a decommissioned plane in a test set up by the BBC, the blast did not breach the fuselage, leading air accident investigator Captain J. Joseph to conclude, “I am very confident that the flight crew could have taken this aeroplane without any incident at all and get it to the ground safely” (BBC 2010), although the explosive test was conducted while the aircraft was on the ground.

Moreover, an aircraft may not be doomed even if the fuselage is ruptured. In 2008 an oxygen cylinder exploded on a Qantas flight from Hong Kong. Although it blasted a two metre hole in the fuselage and the plane suddenly depressurized, the aircraft returned safely to Hong Kong (ATSB 2009). In 1989, a cargo door opened on a United Airlines flight heading across the Pacific extensively damaging the fuselage and cabin structure adjacent to the door. Nine passengers and their seats were sucked out and lost at sea, but the plane was able to make an emergency landing in Honolulu. Aircraft, like many types of infrastructure are more robust and resilient than we often give them credit for.

PETN has a long history of use in terrorist attacks but, like most stable explosives, it’s not easy to ignite (Walsh 2009). Presumably because airport screening makes smuggling a metal detonator a risky proposition, the underwear bomber used a syringe filled with a liquid explosive like nitroglycerin. However, this adds to the difficulty: notes Jimmie Oxley, Director of the Centre of Excellence Explosives Detection, Mitigation, Response and Characterization at the University of Rhode Island, “It looked like he was trying to use a chemical initiation, and that takes a lot of pre-experimentation to find out what would work.” (Walsh 2009).

Since two Russian airliners were blown up by terrorists in 2004, the terrorist’s task is obviously not impossible (Chivers 2004). However, it is a difficult one, and terrorists trying to detonate explosives in flight are likely to end up with more duds than successes. Moreover, although their explosion may cause real damage and loss of life, this result is by no means guaranteed: aircraft have shown themselves to be resilient to accidental explosions or other mid-air mishaps, and so ‘blowing up’ an airliner is more challenging than we imagine.

Although some terrorists are skilled and well trained, many terrorist attacks in the U.K, U.S. and Afghanistan were averted by the ‘ineptitude’ of the terrorists themselves (Byman and Fair 2010). Moreover, many, but not all, terrorists lack bomb-making skills such as those behind the failed car bombings in London and Glasgow in 2007 (Kenney 2010), and Faisal Shahzad, the Pakistani Taliban-trained, naturalized American citizen who tried to bomb New York City’s Times Square in May 2010 (Bergen and Hoffman 2010). Assembling and detonating a small or miniaturised IED needed to minimise the chances of passenger screening detection is even more challenging than their larger counterparts. This all suggests that even if a terrorist
can board an aircraft and attempt to detonate the device undetected, there is no 100% surety that the bomb will successfully detonate - i.e. poor training, lack of hands-on experience and poor tradecraft means there is a reasonable chance that the IED will be a ‘dud’.

Suicide bombers, like drug couriers, can go to inordinate lengths to conceal weapons or contraband - including body cavities. In August 2009 Abdullah Hassan al-Asiri attempted to assassinate a Saudi prince by detonating 100 grams of PETN, which according to some reports was concealed in his underwear, and other reports, his rectum (Bergen 2009). A Europol study confirmed that concealment of IEDs in rectal cavities was possible, “but that the body itself would act as a shield for the expansion of the explosive wave, amortising its effects.” (Europol 2009). This explains why Asiri succeeded in only killing himself, while the Saudi prince who stood close by escaped unharmed. It would seem that a terrorist would need to remove explosives from their underwear for it to be fully effective against a target - but an act which will increase the odds of detection. The Europol (2009) report also suggested “Should there be conclusive proof that the attack took place with an IED concealed inside the perpetrator’s body, it would definitely have an impact in aviation safety and the current standard operational procedures in place should be reviewed.” The ability of AITs to detect this type of concealed explosives and detonator is unclear.

The risk reduction ($\Delta R$) is the additional risk reduction achieved by the presence AITs 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., Biringer et al. 2007). This is the approach used herein.

The TSA has arrayed ‘21 Layers of Security’ to ‘strengthen security through a layered approach’ – see Figure 2. 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

![Layers of U.S. Aviation Security](image)

Figure 2. TSA’s 21 Layers of Security.

We start assessing risk reduction by developing a simple systems model of existing and new (AITs) aviation security measures. For a suicide bomber to succeed in downing a commercial airliner requires that all stages of the planning, recruiting and implementation of the plot go undetected. We will focus on three steps linked to aviation security:

1. success in boarding aircraft undetected
2. success in detonating IED
3. location and size of IED is sufficiently powerful to down the aircraft

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

1. success in boarding aircraft undetected - 10 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 officer, travel document checker, checkpoint/transportation security officers (TSO), transportation security inspectors, bomb appraisal officers
2. success in detonating IED - trained flight crew and passengers
3. location and size of IED is sufficiently powerful to down the aircraft - aircraft resilience
If any one of these security measures are effective, or the capabilities of the terrorist are lacking, then the terrorist 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 suicide bomber. Note that four of the inflight security measures - air marshals, hardened cockpit door, armed flight crew, and on-board law enforcement officers - are designed to protect against hijackings or replication of a 9/11 style attack. Moreover, air marshals are on less than 10% of aircraft and so are unlikely to be deter, foil or disrupt a suicide bomber (Stewart and Mueller 2008a,b).

Figure 3 shows a reliability block diagram used to represent the system of foiling, deterring or disrupting an IED terrorist attack 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. Assume:

○ Probability that a terrorist is successful in avoiding detection by any one of the 10 layers of pre-boarding TSA security is a high 90%.
○ 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
  - Aircraft resilience - a 75% chance of an airliner crashing if a bomb is successfully detonated.

Figure 3. Reliability Block Diagram of Existing (shaded) and Enhanced Aviation Security Measures With Advanced Imaging Technology (AIT).
For a series system where each event probability is statistically independent the probability of airliner loss is

\[
\Pr(\text{airliner loss}) = \prod_{i=1}^{10} \Pr(\text{non-detection for pre-boarding security measure } i) \\
\times \Pr(\text{Passengers/Crew non-detection}) \times \Pr(\text{IED detonates successfully}) \\
\times \Pr(\text{aircraft downed by IED detonation}) \\
= (0.9)^{10} \times 0.5 \times 0.75 \times 0.75 = 9.8\%
\]

The probability then that the plot is foiled, deterred or disrupted is 1-Pr(airliner loss) = 90.2% assuming existing security measures.

AITs have the potential to (i) reduce the success of a suicide bomber boarding an aircraft in the U.S. undetected, (ii) deter the terrorist from using conventional, but more reliable detonators hence reducing likelihood of successful IED detonation, and (iii) deter the terrorist from using larger mass, but more detectable, explosives hence reducing likelihood of IED being sufficiently large to down an aircraft. Now, if the additional security measure is AITs, then we assume:

- The probability of this technology in preventing a suicide bomber boarding an aircraft is five times higher than any existing layer of TSA pre-boarding security - i.e., 50%
- The probability of this technology in preventing a suicide bomber from successfully detonating an IED is 50% because AITs may deter a terrorist from using more reliable, but more detectable, detonator.
- The probability of this technology in preventing an IED from being sufficiently large to down the aircraft is 50%.

Again assuming a series system, the probability that a terrorist plot will not be foiled, disrupted or deterred by AITs is

\[
\Pr(\text{AITs will not foil, deter or disrupt an IED attack}) = \left[1 - \Pr(\text{AIT effectiveness})\right]^3 \quad (4)
\]

and since Pr(AIT effectiveness) is 50% the probability that AITs will not foil, disrupt or deter a terrorist attack is thus (1-0.5)^3=12.5% and so airliner loss is now calculated as 9.8% x 12.5%/1.2%. Hence, the probability of preventing a terrorist attack and the downing of an airliner is now 100-1.2=98.8% due to AITs. The additional risk reduction from this single security measure is \(\Delta R=98.8-90.2=8.6\%\). This is the risk reduction in stopping a suicide bomber boarding a plane in the U.S., detonating it successfully or the explosive energy is insufficient to down the aircraft. We have taken conservative assumptions about (i) efficacy of TSA pre-boarding security (only 10% chance of detection for each layer), (ii) flight crew and passenger vigilance in disrupting a suicide bomber as to date flight crew and passengers have foiled many suicide bombers, and (iii) the would-be terrorist shows more skill and tradecraft than many of his or her compatriots in keeping their plot secret and avoiding detection by the public, police or security services.

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 and reliability approach to modelling effectiveness of aviation security measures described above is instructive.
Clearly, risk reduction is an uncertain variable. Using the figures above, the risk remaining after allowing for existing security measures is 9.8%. The best case scenario is that AITs are 100% effective in eliminating this remaining risk then the best case risk reduction is $\Delta R=9.8\%$. We will round this up to $\Delta R=10\%$ as an upper bound of risk reduction. This is a sizeable risk reduction from a single security measure. If AITs are less effective than assumed above, but still twice as effective than any existing layer of TSA pre-boarding security $\Pr(\text{AIT effectiveness})=20\%$, then risk reduction is reduced to 4.8%. A lower bound risk reduction is thus taken as $\Delta R=5\%$.

To be consistent with loss estimations, we will assume three alternate probability distributions of risk reduction (see Figure 4):

1. Normal Distribution - risk reduction is normally distributed with 95% confidence interval between 5% and 10%, then mean risk reduction is 7.5% and standard deviation is 1.3%.
2. Uniform Distribution - equal likelihood of any risk reduction between 5% and 10%, with mean risk reduction of 7.5%.
3. Triangular Distribution - higher likelihood of higher risk reduction bounded by 5% and 10%, with mean risk reduction of 8.3%.

![Figure 4. Alternative Risk Reduction Uncertainty Models.](image)

### 3.4 Results

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 a successful $26$ billion attack with body-borne explosives have to be to justify spending $1.2$ billion per year to reduce the total risk of this possibility by 7.5%? The minimum attack probability for full body scanners to be cost-effective is thus 61.5% per year - calculated following Eqn. (1) as $1.2$ billion divided by $26$ billion in losses divided by 7.5% risk reduction. Thus, a mean rate of attack of more than one attack every two 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 50% chance of foiling an
attempt to set off a bomb, the bomb is only 25% likely to be a dud or to fail to explode, and there is only a 25% chance a rather small bomb will fail to bring down the aircraft. The analysis also assumes a successful attack will cause an average $26 billion in damage, a rather high estimate according to some accountings, and it further ignores all opportunity costs inflicted by the body-scanning security measure, costs which could be quite substantial.

Note that the attack probability is the probability of an attack that originates in the U.S. and the bomber boards an aircraft in the U.S. and not elsewhere. This is an important distinction as the shoe and underwear bombers boarded their aircraft at international locations and not in the U.S. Finally, this type of cost-benefit analysis fails to consider the uncertainty of losses and risk reduction - this is now described in the following section.

### 3.4.1 Uncertainty Analysis

Monte-Carlo simulation analysis is used as the computational tool to propagate uncertainties through the cost-benefit analysis, although analytical methods could also be used (e.g., Stewart and Melchers 1997). The analysis assumes that losses and risk reductions are either normally, uniformly or triangularly distributed, and so the output of the analysis (net benefit) is also variable. The probability that a security measure is cost-effective is

\[
\Pr(\text{cost-effective}) = \Pr(\text{net benefit} > 0)
\]  

(5)

Figure 5 shows the probability histograms of net benefit for an attack probability of 50% per year. In this case, the probability that net benefit exceeds zero is \(\Pr(\text{cost-effective})=30.8\%\), 35.0% and 19.4%, for normal, uniform and triangular loss and risk reduction distributions, respectively. This suggests that even if there is one attack every two years there is a strong likelihood that full-body scanners are not cost-effective.

![Probability Distributions of Net Benefit](image-url)
Figure 6 shows the probability of cost-effectiveness for attack probabilities from 0.1% to 1,000%. If attack probability is less than 20% per year then there is zero likelihood that AITs are cost-effective and 100% likelihood of a net loss. If attack probabilities exceed 1,000% or ten attacks per year then AITs are certain to be cost-effective (i.e. Pr(cost-effective)=100%). Clearly, as attack probability decreases then benefit reduces thus reducing net benefit.

![Figure 6. Probability of Cost-Effectiveness (Net Benefit Exceeds Zero).](image)

The decision problem can be recast another way. In a break-even analysis, the minimum attack probability for AITs to be cost effective is selected such that there is 50% probability that benefits equal cost (see Table 1). Hence, if attack probability exceeds values given in Table 1 then there is more than a 50/50 chance that AITs are cost-effective. However, a decision-maker may wish the likelihood of cost-effectiveness to be higher before investing billions of dollars in a security measure - to say 90% so there is more certainty about a net benefit and small likelihood of a net loss. Table 1 shows the minimum attack probabilities needed for there to be a 90% chance that AITs are cost-effective. For all three uncertainty models, the attack probability needs to exceed 160-330% per year to be near certain that AITs are cost-effective. This means that there is 90% confidence that AITs will pass a cost-benefit analysis if the mean rate of attack is two to three attacks per year originating from U.S. airports. Conversely, Table 1 shows that if attack probability is less than 34-41% per year then there is only a 10% chance of a net benefit, and a 90% likelihood of a net loss. The results are not overly sensitive to the probabilistic models used for loss and risk reduction.

<table>
<thead>
<tr>
<th>Probabilistic Models of Loss and Risk Reduction</th>
<th>Pr(cost-effective)=10%</th>
<th>Pr(cost-effective)=50%</th>
<th>Pr(cost-effective)=90%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>37.2%</td>
<td>63.2%</td>
<td>161.8%</td>
</tr>
<tr>
<td>Uniform</td>
<td>34.0%</td>
<td>63.9%</td>
<td>247.7%</td>
</tr>
<tr>
<td>Triangular</td>
<td>41.0%</td>
<td>91.2%</td>
<td>330.4%</td>
</tr>
</tbody>
</table>

Table 1. Minimum Attack Probability for AITs to be Cost-Effective.
3.4.2 Sensitivity Analysis

While we have tried to err on the generous side - i.e. towards improving the cost-effectiveness of full-body scanners - we recognise that the probability estimates for effectiveness of security measures are uncertain and subjective. If the effectiveness of pre-boarding security is reduced, then the additional risk reduction of AITs increases. Hence, assume that effectiveness of pre-boarding security measures is half of those used above (i.e. probability of avoiding detection increases from 90% to 95%), and (ii) effectiveness of AITs increases from 50% to 75%. Then $\Pr(\text{airliner loss})$ is 16.8% and 0.3% for existing and enhanced security measures, respectively. The risk reduction is thus $\Delta R = 16.5\%$. Or if we assume that $\Pr(\text{successful IED detonation})$ increases from 75% to 100% due to highly skilled and experienced terrorists, then risk reduction is $\Delta R = 11.5\%$. If we modify the three alternative uncertainty models of risk reduction so that their range is 5-20% (as opposed to 5-10% when generating Table 1 and Figures 5-6), then the attack probability needs to exceed 115-192% for there to be 90% confidence that AITs are cost-effective. A break-even 50/50 analysis shows that the attack probability needs to exceed 39-53% for AITs to be cost-effective. However, if opportunity costs are considered then this would increase the threshold attack probabilities.

The predicted losses can also be quite uncertain. However, if the upper bound of loss is doubled to $C_{\text{loss}} = $100 billion (as opposed to $2-$50 billion when generating Table 1 and Figures 5-6), then the attack probability needs to exceed 89-209% for there to be 90% confidence that AITs are cost-effective. While doubling risk reduction or losses reduces threshold attack probabilities, they still remain at relatively high levels.

3.5 Discussion

The present paper has shown the utility of systems and uncertainty modelling for cost-benefit analysis for homeland security expenditure. The preliminary results suggest that the threat probability needs to be high for full-body scanners to be cost-effective. But we recognise that the preliminary cost-benefit analysis conducted herein will not give a definitive answer to whether AITs 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.

4. CONCLUSIONS

The paper has developed a cost-benefit analysis of Advanced Imaging Technologies (AITs) using full-body scanners for passenger screening at U.S. airports. The analysis considered threat probability, risk reduction, losses, and security costs in the estimation of costs and benefits. Since there is uncertainty and variability of these 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 full-body scanners to be cost-effective were inferred. It was found that, based on mean results, more than one attack every two years would need to originate from U.S. airports for AITs to pass a cost-benefit analysis. In other words, to be cost-effective, AITs every two years would have to disrupt more than
one attack effort with body-borne explosives that otherwise would have been successful
despite other security measures, terrorist incompetence and amateurishness, and the technical
difficulties in setting off a bomb sufficiently destructive to down an airliner. The uncertainty
modelling also allowed the minimum attack probability to be estimated for the probability
that AITs will be cost-effective exceeds 90%. For all three uncertainty models, the attack
probability needs to exceed 160-330% per year to be near certain that AITs are cost-effective.

ACKNOWLEDGEMENTS

Part of this work was undertaken while the first author was a Visiting Professor in the
Department of Civil, Structural and Environmental Engineering at Trinity College Dublin. He
greatly appreciates the assistance provided by Trinity College. The first author also
appreciates the financial support of the Australian Research Council.
REFERENCES


Europol (2009), *The Concealment of Improvised Explosive Devices (IEDs) in Rectal Cavities*, SC5 - Counter Terrorism Unit, Europol, The Hague, 18 September 2009, p.8


Pena, C.V. (2005), *Flying the Unfriendly Skies: Defending Against the Threat of Shoulder Fired Missiles*, Policy Analysis, No. 541, Cato Institute, April 19 2005, p.3


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. An abridged list of recently published titles in this series is provided below. Requests for a more 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

Telephone: (02) 4921 6058
Facsimile: (02) 4921 6991

<table>
<thead>
<tr>
<th>REPORT NO.</th>
<th>ISBN NO.</th>
<th>TITLE AND AUTHOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>271.11.2008</td>
<td>9780 9805 0357 9</td>
<td>Damage Risk Assessment Of Buildings To Tropical Cyclones Under Enhanced Greenhouse Conditions Y. Li and M.G. Stewart</td>
</tr>
<tr>
<td>272.01.2009</td>
<td>9780 9805 0359 3</td>
<td>A Risk and Cost-Benefit Assessment Of Counter-Terrorism Protective Measures To Infrastructure Mark G. Stewart</td>
</tr>
<tr>
<td>273.01.2009</td>
<td>9780 9806 0341 5</td>
<td>Cost-Benefit Assessment Of United States Homeland Security Spending Mark G. Stewart and John Mueller</td>
</tr>
<tr>
<td>274.01.2009</td>
<td>9780 9806 0340 8</td>
<td>Structural Reliability and Partial Safety Factors For Unreinforced Masonry In Vertical Bending Stephen J. Lawrence and Mark G. Stewart</td>
</tr>
<tr>
<td>275.05.2009</td>
<td>9780 9806 0345 3</td>
<td>Corrosion-Induced Cover Cracking Of RC Structures: New Experimental Data and Predictive Models John A. Mullard and Mark G. Stewart</td>
</tr>
<tr>
<td>276.07.2009</td>
<td>9780 9806 0344 6</td>
<td>Impact and Adaptation Assessment of Cyclone Damage Risks to Climate Change Mark G. Stewart and Yue Li</td>
</tr>
</tbody>
</table>