Journal of Homeland Security and Emergency Management

Volume 8, *Issue* 1 2011 *Article* 30

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

Mark G. Stewart, *The University of Newcastle, Australia*
John Mueller, *Ohio State University*

Recommended Citation:
Stewart, Mark G. and Mueller, John (2011) "Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening," *Journal of Homeland Security and Emergency Management*: Vol. 8: Iss. 1, Article 30.
DOI: 10.2202/1547-7355.1837
Available at: http://www.bepress.com/jhsem/vol8/iss1/30

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

Mark G. Stewart and John Mueller

Abstract

The Transportation Security Administration (TSA) has been deploying Advanced Imaging Technologies (AITs) 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 preliminary 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 percent. 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 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. However, the attack probability needs to exceed 160-330 percent per year to be 90 percent certain that full body scanners are cost-effective.

KEYWORDS: terrorism, security, cost-benefit analysis, aviation security, passenger screening

Author Notes: 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. 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.

INTRODUCTION

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 and explosives. The cost of this technology will reach $1.2 billion per year by 2014. The U.S. Government Accountability Office (GAO) remarked in 2010 that "conducting a cost-benefit analysis of TSA's AIT deployment is important.", and "would help inform TSA's judgment about the optimal deployment strategy for the AITs" (Lord 2010). Yet, before deciding to install AITs at considerable cost the TSA has not conducted a cost-benefit analysis. This absence of a cost-benefit analysis for AITs is the motivation for the present study.

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 optimizes 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. 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 expenditure.

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 forcefully made by many in government, industry and academe (e.g., Friedman 2010, Poole 2008). The U.S. National Research Council (NRC 2010), after a 15 month study period, made critical recommendations about 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 security costs. This is a challenging task, but necessary for any risk assessment, and the quantification of security risks is recently being addressed (e.g., 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 (Willis and LaTourette 2008, von Winterfeldt and O'Sullivan 2006, Stewart 2008, 2010, 2011). Much of this work can be categorized as 'probabilistic terrorism risk assessment'.

Stewart (2010) 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 2008). 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); a detailed assessment of threats and vulnerabilities leads to similar conclusions (Mueller 2010, Mueller and Stewart 2011). This suggests that policy makers within the U.S. government and 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 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 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).

For many engineering systems the threat rate is known, but for terrorism the threat is from an intelligent adversary who will adapt to changing circumstances. 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. 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). Hence, we will undertake a 'break even' cost-benefit analysis in this paper.

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 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. This preliminary study will also include uncertainty analysis in the cost-benefit calculations to reflect the uncertainty in underlying data and modeling assumptions, and will allow the probability of cost-effectiveness to be calculated. AITs are being trialed or deployed in the U.K., France, Netherlands, Italy, Canada, Australia and elsewhere which will cost 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.

RISK AND COST-BENEFIT METHODOLOGY

A security measure is cost-effective when the benefit of the measure outweighs the costs of the security measure. The *net benefit of a security measure* is:

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

- 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.
- 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.
- ΔR: The *reduction in risk* is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack.

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 favor 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.
- although we understand that people are often risk-averse when considering issues like terrorism, governments should be risk-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.

COST-BENEFIT ASSESSMENT OF FULL BODY SCANNERS

Costs ($C_{security}$)

The TSA will use AITs as a primary screening measure, and 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, $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 for support and airport management. The TSA estimates that the annualized 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 we assume 100% coverage at all airports in the U.S., although this 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 'intrusive' pat-downs. This perceived invasion of privacy, 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). On the other hand, it may be argued that AITs may provide a type of 'security theatre' that will make travelers feel safer which in itself is beneficial. Whether AITs will result in opportunity costs or not is beyond the scope of the present paper. In the present paper, we will assume that AITs will cost $C_{security}$=$1.2 billion per year and will ignore opportunity costs - although these have the potential to be very substantial. We also ignore any possible security theatre benefits - likely, however, to be small as there is little evidence that AITs by themselves will make travelers feel much safer, and could well have the opposite effect.

Economic Loss (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 loss of an airliner with 300 passengers by a shoulder fired missile, a shutdown of U.S. airspace for a week, and 15% drop in air travel in the 6 months following the attack would cause an economic loss of more than $15 billion (Chow et al. 2005). Another study, again assuming an 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 to derive loss estimates of $214-$420 billion. This seems overly conservative as adding up individual sectoral losses can lead to double counting and "that large scale terrorist attacks cause reallocations

of people and resources across sectors" and "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." (Enders and Olsen 2011).

The downing of an airliner due to an passenger-borne IED is likely not to trigger the same response as a downing caused by a shoulder fired missile as no counter-measures exist for a missile attack that could be implemented quickly. On the other hand, a series of screening measures were implemented quickly following the 9/11 and subsequent attacks that provides assurance to the public that it is safe to fly. This all suggests that the losses forecast above for a shoulder-fired missile attack will over-estimate losses for our threat scenario.

A report for the DHS concludes that the best estimate for value of a statistical life (VSL) for homeland security analysis is $6.5 million in 2010 dollars (Robinson et al. 2010). 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 the losses inflicted by the terrorist attack that has been by far the most destructive in history, that of September 11, 2001. A 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 1.0 percent of GDP (Blomberg and Rose 2009). 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. 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 ($42 billion based on 2010 GDP figures) which we will round up to C_{loss}=$50 billion.

Results from uncertainty and probabilistic modeling may be sensitive to the shape of the probability distribution. 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. 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 mean loss of $18 billion.

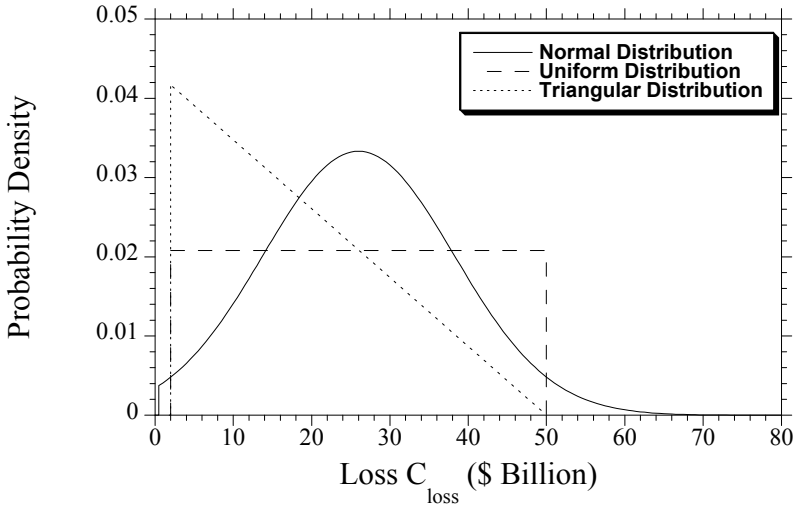

Figure 1. Alternative Loss Uncertainty Models.

Risk Reduction (ΔR)

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 by casting doubt on the ability of AITs to detect the weapon Abdulmutallab used in his attempted attack (Lord 2010). 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. Moreover, the search for a detonator is equally important and easier to detect since most detonators contain metal.

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 (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. 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) 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 (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 blasting a two meter hole in the fuselage. 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. In both instances the aircraft landed safely. 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. 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 of a successful detonation.

Since two Russian airliners were blown up by terrorists in 2004, the terrorist's task is obviously not impossible. 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. Moreover, many, but not all, terrorists lack bomb-making skills such as those behind the failed car bombings in London and Glasgow in 2007, and Times Square in 2010 (Kenney 2010). Assembling and detonating a small or miniaturized IED needed to minimize the chances of passenger screening detection is even more challenging than their larger compatriots. 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 - poor training, lack of hands-on experience and poor tradecraft means there is a good 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. A Europol (2009) study confirmed that

concealment of IEDs in rectal cavities was possible but that the body would absorb much of the blast. 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 - an act which increases the odds of detection.

The TSA has arrayed '21 Layers of Security' to 'strengthen security through a layered approach'. This is designed to provide defense-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): Intelligence, International Partnerships, Customs and border protection, Joint terrorism task force, No-fly list and passenger pre-screening, Crew vetting, Visible Intermodal Protection Response (VIPR) Teams, Canines, Behavioral detection officers, Travel document checker, Checkpoint/transportation security officers, Checked baggage, Transportation security inspectors, Random employee screening, and Bomb appraisal officers. The remaining six layers of security provide 'in-flight security': Federal Air Marshal Service, Federal Flight Deck Officers, Trained flight crew, Law enforcement officers, Hardened cockpit door, and Passengers.

The risk reduction (ΔR) is the additional risk reduction achieved by the presence of AITs when compared to the overall risk reductions achieved by the presence, absence and/or effectiveness of all other security measures. 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 and event trees and logic diagrams, together with systems engineering and reliability approaches, will aid in assessing these and other complex interactions. This is the approach used herein.

We start assessing risk reduction by developing a simple systems model of new (AITs) and existing 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 layers of security: intelligence, international partnerships, customs and border protection, joint terrorism

task force, no-fly list and passenger pre-screening, behavioral 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 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 2008).

Figure 2 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.

Since there are uncertainties with quantifying these probabilities a sensitivity analysis is conducted later in the paper to assess robustness of results. For a series system where each event probability is statistically independent the probability of airliner loss is

$$\Pr(\text{airliner loss}) = \prod_{i=1}^{10} \Pr(\text{non-detection for preboarding security measure i}) \times \Pr(\text{Passengers/Crew non-detection}) \times \Pr(\text{IED detonates successfully}) \times \Pr(\text{aircraft downed by IED detonation}) = (0.9)^{10} \times 0.5 \times 0.75 \times 0.75 = 9.8\% \quad (2)$$

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

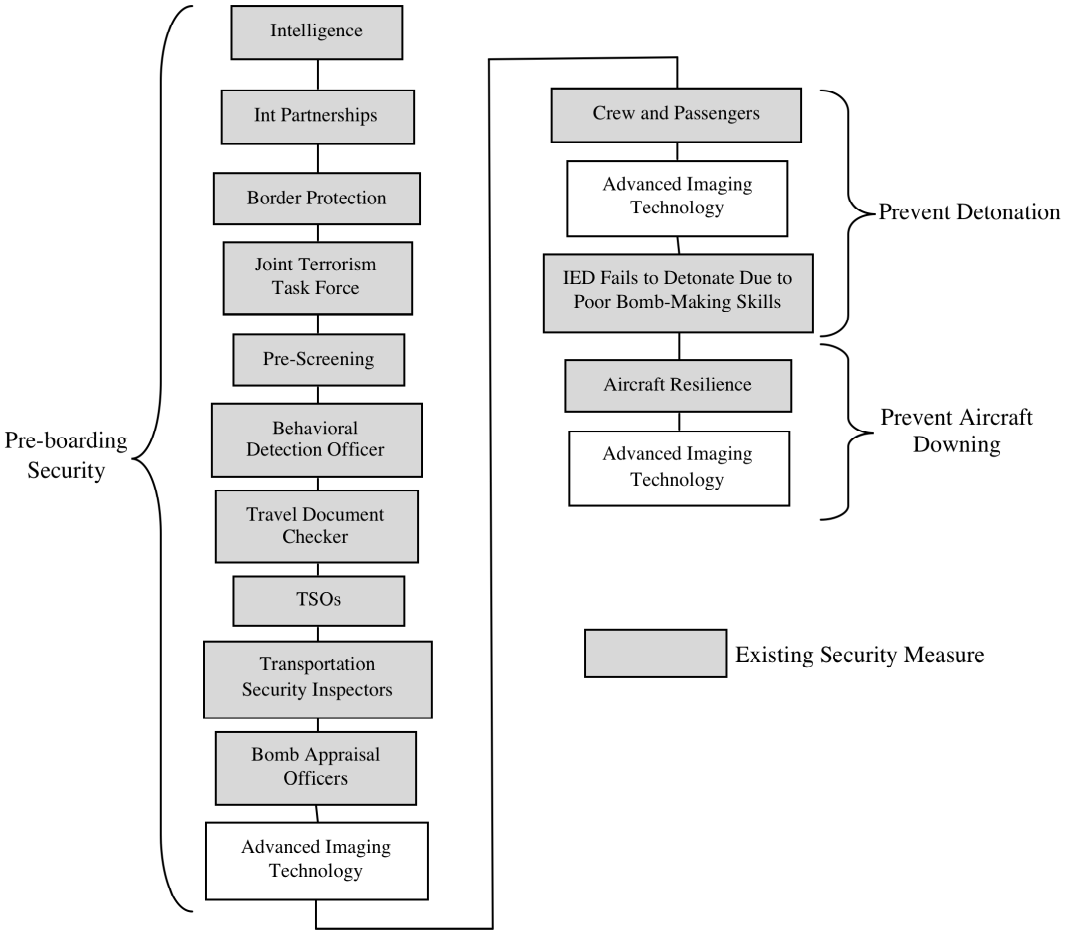

Figure 2. Reliability Block Diagram of Existing (shaded) and Enhanced Aviation Security Measures With Advanced Imaging Technology (AIT).

Again assuming a series system, and since Pr(AIT effectiveness) is 50%, the probability that a terrorist plot will not be foiled, disrupted or deterred by AITs is $[1\text{-Pr(AIT effectiveness)}]^3=(1-0.5)^3=12.5\%$ and so probability of airliner loss is now calculated as $9.8\%\times12.5\%=1.2\%$. 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), (ii) flight crew and passenger vigilance in disrupting a suicide bomber, 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 modeling. Nonetheless, the systems approach to modeling effectiveness of aviation security measures described herein is instructive.

Risk reduction is an uncertain variable. Using the figures above, the best case scenario is that AITs are 100% effective in eliminating this remaining risk then the best case risk reduction is $\Delta R=9.8\%$. If AITs are less effective than assumed above, but still twice as effective than any existing layer of TSA pre-boarding security [Pr(AIT effectiveness)=20%], then risk reduction is reduced to 4.8%. Lower and upper bound risk reductions is thus taken as 5% and 10%, respectively. We will also assume three alternate probability distributions of risk reduction (see Figure 3):

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%.

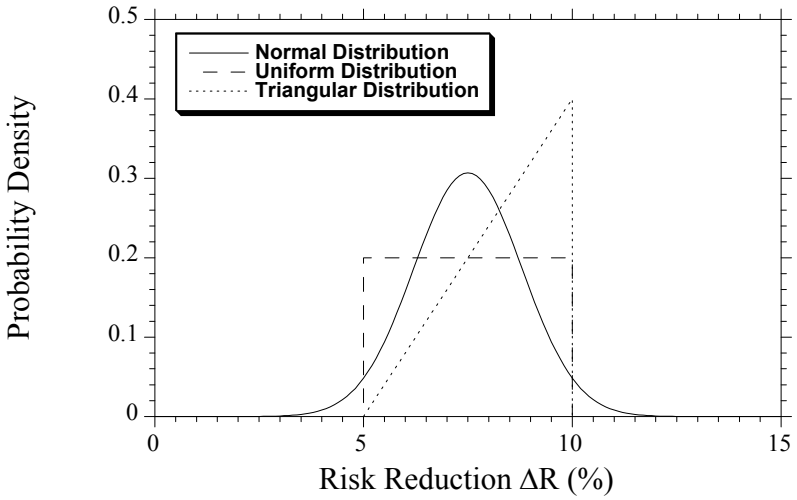

Figure 3. Alternative Risk Reduction Uncertainty Models.

Results

An expected value cost-benefit analysis is one that uses mean values. In this case, the minimum attack probability for full body scanners to be cost-effective is 61.5% per year calculated as $1.2 billion divided by $26 billion in losses divided by 7.5% risk reduction. Thus, full body scanners must deter or foil more than one otherwise successful attack every two years for the security measure to be deemed cost-effective. However, this type of cost-benefit analysis fails to consider the uncertainty of losses and risk reduction - this is now described in the following section. 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.

Uncertainty Analysis

Monte-Carlo simulation analysis is used as the computational tool to propagate uncertainties through the cost-benefit analysis. The analysis assumes that losses and risk reductions are either normally, uniformly or triangularly distributed. If inputs are random variables then the output of the analysis (net benefit) will also be variable and so the probability that net benefit exceeds zero, Pr(cost-effectiveness), can be calculated for any attack probability. Figure 4 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 so 100% likelihood of a net loss. On the other hand, 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.

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). 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.

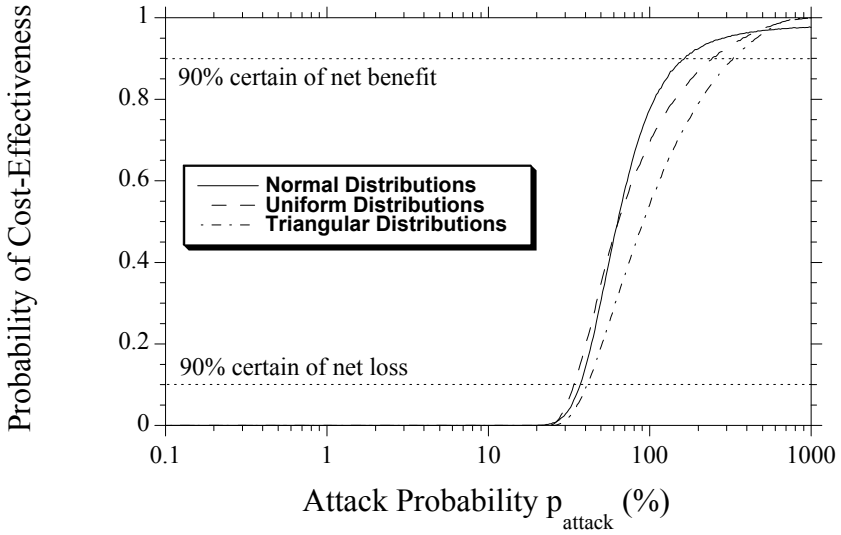

Figure 4. Probability of Cost-Effectiveness (Net Benefit Exceeds Zero).

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

Loss and Risk Reduction Distributions	Pr(cost-effective)=10%	Pr(cost-effective)=50%	Pr(cost-effective)=90%
Normal	37.2%	63.2%	161.8%[1]
Uniform	34.0%	63.9%	247.7%
Triangular	41.0%	91.2%	330.4%

[1] 1.62 attacks per year

Sensitivity Analysis

While we have tried to err on the generous side - i.e. towards improving the cost-effectiveness of full-body scanners - we recognize that the probability estimates for effectiveness of security measures are uncertain. 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% due to, for example, a higher deterrent capability. Then Pr(airliner loss) is 16.8% and 0.3% for existing and enhanced security measures, respectively. The risk reduction is ΔR=16.5%. If AITs are 100% effective then they reduce existing risk to zero and so ΔR=16.8%. Or if we assume that Pr(successful IED detonation) increases from 75% to 100% due to highly skilled and experienced terrorists, then risk reduction is ΔR=11.5%. If we modify the three alternative uncertainty models of risk reduction so that their range is 5-20%, then the attack probability needs to exceed 115-192% for there to be 90% confidence that AITs are cost-effective. A break-even 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.

If the lower bound of loss is increased to $5 billion, then the attack probability needs to exceed 131-201% for there to be 90% confidence that AITs are cost-effective. If the upper bound of loss is doubled to C_{loss}=$100 billion, 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.

Discussion

The present paper has shown the utility of systems and uncertainty modeling for cost-benefit analysis for homeland security expenditure. The preliminary results suggest that the threat probability - the likelihood an attack will be otherwise successful - needs to be high for AITs to be cost-effective. But we recognize 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 minimize 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 security measures.

CONCLUSIONS

The paper has developed a preliminary 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. Monte-Carlo simulation methods were used to propagate risk reduction and loss uncertainties in the calculation of net 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. The uncertainty modeling also allowed the probability of cost-effectiveness to be calculated. It was found that the attack probability needs to exceed 160-330% per year to be 90% certain that AITs are cost-effective.

REFERENCES

Bayles, F. (1996), 'Planes Don't Blow Up' Aviation Experts Assert, *International Herald Tribune*, July 24, 1996.

BBC News (2010), Boeing 747 Survives Simulated 'Flight 253' Bomb Blast, 5 March 2010.

Blalock, G., Kadiyali, V. and Simon, D.H. (2007), The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel, *Journal of Law and Economics*, 50(4): 731-55.

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*, May 2009, 15(2):1-14.

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, Santa Barbara, 2005.

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.

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

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

Enders, W. and Olsen, E. (2011), Measuring the Economic Costs of Terrorism, In M. Garfinkel and S. Skaperdas eds. *Oxford Handbook of the Economics of Peace and Conflict,* Forthcoming.

Europol (2009), *The Concealment of Improvised Explosive Devices (IEDs) in Rectal Cavaties*, Europol, The Hague, 18 September 2009, p.8

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.

Freidman, 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*, B.H. Friedman, J. Harper, and C.A. Preble (Eds.), Cato Institute, p. 211.

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

Halsey, A. (2010), All check-points wont get body scanners, *The Washington Post*, December 2, 2010.

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.

Lord, S. (2010), *Aviation Security: TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to this Effort and Areas of Aviation Security Remain*, United States Government Accountability Office, GAO-10-484T, March 17 2010, p.5

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

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

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

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.

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, December 2008.

Robinson, L.A., Hammitt, J.K., Aldy, J.E., Krupnick, A. and Baxter, J. (2010), Valuing the Risk of Death from Terrorist Attacks, *Journal of Homeland Security and Emergency Management,* 7(1).

Rossides G. (2010), Advanced Imagining Technology - Yes, It's Worth It, *The Blog@Homeland Security*, April 1 2010.

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, *J. 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.

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

TSA (2010), Passenger Screening Program: Program Specific Recovery Act Plan May 24 2010, Department of Homeland Security, Washington, DC, p.3

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.