Homeland security: a case study in risk aversion for public decision-making

Mark G. Stewart*

Centre for Infrastructure Performance and Reliability,
The University of Newcastle,
New South Wales, 2308, Australia
E-mail: mark.stewart@newcastle.edu.au
*Corresponding author

Bruce R. Ellingwood

Georgia Institute of Technology,
School of Civil and Environmental Engineering,
Atlanta, GA 30332-0355, USA
E-mail: bruce.ellingwood@ce.gatech.edu

John Mueller

Mershon Center for International Security Studies,
Department of Political Science,
Ohio State University,
Columbus, Ohio 43201, USA
E-mail: bbbb@osu.edu

Abstract: Governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making. However, for low probability-high consequence events many decision-makers tend to be risk-averse because of the catastrophic or dire nature of the hazard or event. The degree of risk averseness can be described by utility theory. This paper will infer utility functions that reflect the level of risk averseness of regulatory agencies when adopting new safety measures – such as investing $75 billion per year of the homeland security budget to avert terrorist attacks in the USA. The utility analysis considers threat probability, risk reduction caused by regulatory action, cost of regulatory action, and losses. The expected utilities using an identical risk-averse utility function for:

1 no enhanced security expenditure
2 regulatory action associated with $75 billion of enhanced homeland security expenditure are compared and made equal to each other by modifying the risk-averse utility function.

This means that both policy options are equally preferable so if the decision-maker is more risk-averse than suggested by the risk-averse utility function then regulatory action is preferable. It will be shown that the level of risk averseness needed to justify current expenditures for homeland security is considerable.

Keywords: terrorism; risk aversion; decision-making; homeland security; utility theory; cost-benefit analysis; decision theory; USA.

Reference to this paper should be made as follows: Stewart, M.G., Ellingwood, B.R. and Mueller, J. (2011) 'Homeland security: a case study in risk aversion for public decision-making', *Int. J. Risk Assessment and Management*, Vol. 15, Nos. 5/6, pp.367–386.

Biographical notes: Mark G. Stewart is the Director of the Centre for Infrastructure Performance and Reliability and an Australian Research Council Professorial Fellow at The University of Newcastle in Australia. He is the co-author of *Probabilistic Risk Assessment of Engineering Systems*, as well as more than 300 technical papers and reports. He has more than 25 years of experience in probabilistic risk assessment of infrastructure systems that are subject to man-made and natural hazards. His main areas of expertise include structural reliability analysis of deteriorating structures, impact of climate change on infrastructure and assessing the cost-effectiveness of engineering adaptation strategies, and probabilistic and cost-benefit assessments of counter-terrorism protective measures for critical infrastructure.

Bruce R. Ellingwood is currently College of Engineering Distinguished Professor at the Georgia Institute of Technology, where he also holds the Raymond Allen Jones Chair in Civil Engineering. He is internationally recognised as an authority on structural load modelling, reliability and risk analysis of engineered facilities, and as a leader in the technical development and implementation of probability-based codified design standards for buildings. He has authored nearly 400 research papers and reports and is the Editor of *Structural Safety*. His research and professional service have garnered numerous awards from ASCE, AISC and other professional organisations. He is a member of the National Academy of Engineering and a Distinguished Member of ASCE.

John Mueller is a Professor and Woody Hayes Chair of National Security Studies at the Mershon Center for International Security Studies and a Professor of Political Science at Ohio State University, Columbus, Ohio. He is the author of over a dozen books, several of which have won prizes. Among the most recent of these: *The Remnants of War* (2004), *Overblown* (2006), and *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda* (2010). He has also published numerous articles in scholarly journals and general magazines and newspapers, is a member of the American Academy of Arts and Sciences, and has been a John Simon Guggenheim Fellow.

This paper is a revised and expanded version of a paper entitled 'Homeland security: a case study in risk aversion for public decision-making' presented at Fifth International Forum on Engineering Decision Making, Stoos, Switzerland, 7–10 December 2010.

1 Introduction

The threat posed by terrorism since the 9/11 attacks has received considerable political and media attention. This has resulted in the USA launching a 'war on terror' and implementing a series of counter-terrorism security measures for aviation, mass transit, ports, borders, places of public assembly, etc., to reduce the vulnerability of infrastructure

and people to terrorist attacks. While such measures may represent a reasonable course of action by government and security services, it comes at a cost. Mueller and Stewart (2011) estimate that in the ten years since 2001, increased US domestic homeland security expenditures (above 2001 levels) have totalled over $1.1 trillion – this includes federal, state and local government and private sector expenditure, as well as opportunity costs. The wars in Iraq and Afghanistan add at least an extra $1.2 trillion to this figure. The direct cost of US federal, state and local government expenditure on homeland security is approximately $75 billion per year higher than pre-2001 levels (Mueller and Stewart, 2011). It should be noted that the USA is not alone in these high levels of expenditure, though no other countries seem to match it in expenditure per capita or GDP. For instance, enhanced homeland security expenditures in the UK, Canada and Australia are approximately one half to one quarter of US expenditures in terms of per capita or GDP. Nonetheless, government spending worldwide on homeland security reached a staggering $141.6 billion per year in 2009, about half of if by the USA (GHS, 2009). It is projected to reach $300 billion by 2016 (Binning, 2009). The questions that need to be asked include:

1 What risk reduction has been achieved by this expenditure? How many lives have been saved? Or losses averted?

2 Is this a cost-effective utilisation of resources?

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 of the US Government. These studies are particularly useful for low probability – high consequence events where public safety is a key criterion for decision-making. This includes the design and assessment of buildings, bridges, levees, and other infrastructure systems for protection against seismic, flood, hurricane and other natural hazards. 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 this counter-terrorism expenditure has been invested in a manner that optimises public safety cost-effectively. This is why the 9/11 Commission report, amongst others, called on the US Government to implement security measures that reflect assessment of risks and cost-effectiveness (NC, 2004). However, while the USA requires a cost-benefit analysis for government regulations (OMB, 1992), such an analysis does not appear to have been conducted for homeland security in general, or for the US Department of Homeland Security (DHS) in particular. One reason may be that the DHS does not have the capability to undertake such analyses. A Committee of the National Research Council of the National Academies of Sciences, Engineering, and Medicine, requested by the US Congress to assess the activities of the DHS, worked for nearly two years on the project and came up with some striking conclusions (NRC, 2010). Except for the analysis of natural disasters, the committee "did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making" (NRC, 2010). As a result, "only low confidence should be placed in most of the risk analyses conducted by DHS". The committee also observed that "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".

Governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making. This is confirmed by the US Office of Management and Budget

(OMB) which specifically states that "the standard criterion for deciding whether a government programme 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). Farrow (2007) developed an expected cost analysis for homeland security expenditures. Stewart (2010a, 2010b) has shown that, based on expected values, the threat probability has to be extremely high for typical counter-terrorism measures for buildings and bridges to be cost-effective. Similar cost-benefit analyses have shown that the US 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, 2008b). It therefore appears that many homeland security measures would fail a cost-benefit analysis using standard expected value methods of analysis; a detailed assessment of threats and vulnerabilities leads to similar conclusions (Mueller, 2010). This suggests, not surprisingly, that policy makers within the US Government and their agencies (such as DHS) are risk-averse. This is understandable, since for low probability-high consequence events decision-makers tend to be risk-averse because of the catastrophic or dire nature of the hazard or event. However, while many individuals may be risk-averse, government and society are risk-neutral when assessing risks because governments have a high degree of cost and benefit diversification not available to individuals (e.g., Sunstein, 2002; Faber and Stewart, 2003; Ellingwood, 2006). This entails using mean or average estimates for risk and cost-benefit calculations, and not worst-case or pessimistic estimates. Paté-Cornell (2002) elaborates on this point by stating "If risk ranking is recognized as a practical necessity and if resource limitations are acknowledged, the maximum overall safety is obtained by ranking the risks using the means of the risk results (i.e., expected value of losses)".

This type of 'rational' approach to risky decision making is challenging to governments which might have other priorities and political concerns. Hardaker et al. (2009) noted that "policy-making is a risky business", and that "Regardless of the varied desires and political pressures, we believe that it is the responsibility of analysts forcefully to advocate rational decision methods in public policy-making, especially for those with high risk. We believe that more systematic analysis of risky policy decisions is obviously desirable". If rational approaches to public policy making are not utilised, then politically driven processes "may lead to raising unnecessary fears, wasting scarce resources, or ignoring important problems" (Paté-Cornell, 2002).

Terrorism is a threat with specific characteristics that frighten us and make us risk-averse – these include dread (or fear), their involuntary nature, catastrophic potential, little preventative control, certain to be fatal, and large number of people exposed (Wilson and Crouch, 1987). These attitudes will influence our willingness to accept risk and this is influenced by psychological, social, cultural and institutional processes. Another reason for individuals being risk-averse is that the events involving high consequences can cause losses to an individual that they cannot bear, such as loss of one's life or bankruptcy. Governments, large corporations, and other self-insured institutions, on the other hand, can absorb such losses more readily. It is important that follow-on consequences for a terrorist attack such as loss of consumer confidence leading to declining sales figures, reduced chances of new tourism investments, reduced government/tax revenue, etc., should be included in the estimation of losses as this will also lead to a 'risk neutral' risk analysis. Probability

neglect is a form of risk aversion as decision-makers are clearly averse to events of large magnitude irrespective of the probability of it actually occurring. Utility theory can be used if the decision maker wishes to explicitly factor risk aversion into the decision process (e.g., Jordaan, 2005). The degree of risk averseness is evident from utility theory.

This paper will infer utility functions that represent the level of risk averseness of regulatory agencies when adopting new safety measures – such as $75 billion of enhanced spending on homeland security per year to avert terrorist attacks in the USA. The expected utility analysis considers threat probability, risk reduction caused by regulatory action, cost of regulatory action, and losses. The expected utilities using an identical risk-averse utility function for

1 no enhanced security expenditure ('business as usual')

2 regulatory action associated with $75 billion of enhanced homeland security expenditure are compared and made equal to each other by modifying the shape of the risk-averse function.

This means that both policy options are equally preferable and represents a 'tipping point' – if the decision-maker is more risk-averse than suggested by the risk-averse utility function then regulatory action is more preferable to doing nothing ('business as usual'). It will be shown that the level of risk averseness needed for justify current expenditures for homeland security is considerable.

While quantitative decision analyses are seldom the sole criterion for decision making, it is important to understand the trade-offs that decision makers are prepared to make if their decision is 'sub optimal' in terms of a quantitative decision analyses. One trade-off is risk aversion, such as aversion or minimisation of political risk or risk to budgetary resources. It is thus instructive to assess the degree of public policy risk aversion necessary to justify decisions related to expenditure of hundreds of billions of dollars of public money.

2 Decision problem: counter-terrorism spending on US homeland security

2.1 US homeland security expenditures

The OMB defines "homeland security activities" as "activities that focus on combating and protecting against terrorism, and that occur within the US and its territories", and its data show that US Federal Government spending on such activities increased from $20.1 billion in 2001 (Hobijn and Sager, 2007) to $75 billion in 2009 (OMB, 2010). Figure 1 show that federal homeland security expenditures increased steadily in real terms since 2001, a pattern that is likely to continue. The expenditures are divided into three categories:

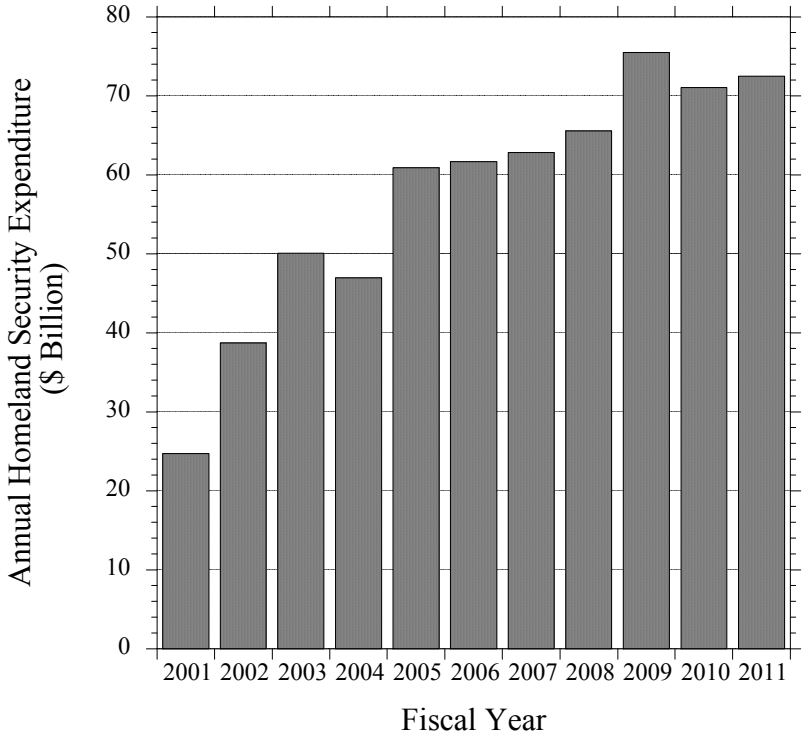
1 *Preventing and disrupting terrorist attacks:* Defined by OMB as "activities of both intelligence-and-warning and domestic counterterrorism aim to disrupt the ability of terrorists to operate within our borders and prevent the emergence of violent radicalisation".

2 *Protecting the American people, critical infrastructure, and key resources*: For OMB "critical infrastructure includes the assets, systems, and networks, whether physical or virtual, so vital to the USA that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof".

3 *Responding to and recovering from incidents*: Defined by OMB as "the ability to respond to and recover from incidents requires efforts to bolster capabilities nationwide to prevent and protect against terrorist attacks, and also minimise the damage from attacks through effective response and recovery".

Some 44% of this expenditure is devoted to preventing and disrupting terrorist attacks, and another 46% to protecting the American people, critical infrastructure, and key resources, while 9% is devoted to responding to and recovering from incidents. Funding goes to the DHS, the Department of Defence, the Department of Justice, the Department of Health and Human Services, the Department of Energy, and 26 other federal agencies as arrayed in Table 1. In all, federal government spending on homeland security for 2009 was $75 billion or $50 billion higher in 2010 dollars than in 2001, adjusting for inflation.

Figure 1 Annual federal expenditures on homeland security (inflation adjusted in 2010 dollars)



Notes: Funding fell in 2004 in part because of one-time force protection investments by the Department of Defence in 2003. Funding for 2010 and 2011 are budget figures and do not represent actual expenditures.

Source: Adapted from OMB (2010)

Table 1 USA homeland security 2009 expenditure by agency (inflation adjusted in 2010 million dollars)

Department of Homeland Security	\$39,730,000
Department of Defence	\$19,872,000
Department of Health and Human Services	\$4,771,000
Department of Justice	\$3,789,000
Department of Energy	\$1,978,000
Department of State	\$1,845,000
Others	\$3,490,000
Total	\$75,476,000

Source: OMB (2010)

To limit our focus to increases in expenditures by the federal government reported by the OMB would be a considerable restriction because this ignores the recently declassified national intelligence costs as well as state and local government outlays on homeland security. The budget for US intelligence operations was \$75 billion in 2009, and a core function is 'protecting against the threat of international terrorism in the USA'. Enhanced intelligence expenditures since 9/11 devoted to homeland security were approximately \$15 billion in 2009. Enhanced outlays for state and local homeland security spending are approximately \$10 billion per year. The increase in annual federal government outlays, then, is \$50 billion per year, and the addition of national intelligence and state and local homeland security outlays of \$25 billion gives a total of \$75 billion per year.

Federal government outlays on homeland security in 2001 totalled approximately \$25 billion in 2010 dollars (see Figure 1). Since intelligence and state and local expenditures since 9/11 are approximately 50% of federal outlays, then total government outlays in 2001 are estimated as \$25 billion plus 50% which is approximately \$35 billion per year. The increase in annual federal, state and local government and national intelligence outlays since 9/11, then, is \$75 billion per year which gives a total of \$110 billion. We will use this figure, although it is a very conservative measure of the degree to which homeland security expenditures have risen since 9/11 because we do not include private sector expenditures on homeland security-related measures, terrorism risk insurance premiums, hidden and indirect costs or 'dead weight losses' of implementing security-related regulations that amounted, various opportunity costs, and the costs of the terror-related wars in Iraq and Afghanistan. For more details of this cost analysis see Mueller and Stewart (2011).

2.2 Expected utility analysis

2.2.1 Method

The well known formulation for risk (expected loss) for a system exposed to a hazard is

$$E(L) = \sum_{H}\sum_{DS}\sum_{L} \Pr(H)\Pr(DS \mid H)\Pr(L \mid DS)L \tag{1}$$

where $\Pr(H)$ is the probability of hazard occurrence, $\Pr(DS|H)$ is the conditional probability of a damage state (e.g., safety hazard) given occurrence of the hazard, $\Pr(L|DS)$ is the conditional probability of a loss (e.g., damage costs, fatalities) given occurrence of the damage state, and L is the loss. The summation signs in equation (1)

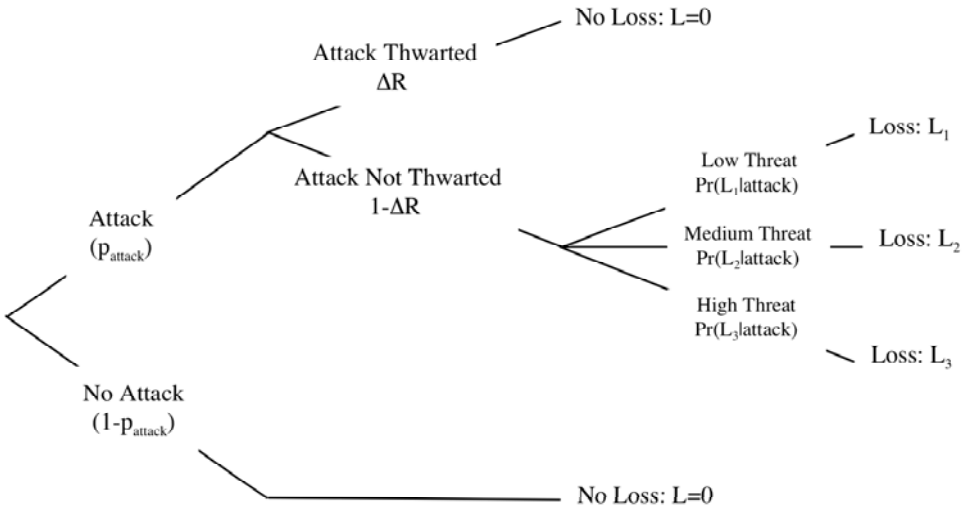
refer to the number of possible hazard intensity levels, damage states and losses. If the loss refers to a monetary loss, then $E(L)$ represents an economic risk.

If we simplify equation (1) by combining $\Pr(DS|H)\Pr(L|DS)$ to $\Pr(L|H)$, assigning $\Pr(H)$ as p_{attack}, and ΔR is the reduction in risk caused by security measures then expected loss is:

$$E(L) = \sum (1 - \Delta R) p_{attack} \Pr(L \mid attack) L \tag{2}$$

where the probability of a successful attack (p_{attack}) is the likelihood a successful terrorist attack will take place if the security measure were not in place. The losses sustained in the successful attack (L) 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. On the other hand, thwarting an attack may produce psychological and political benefits that instead of leading to zero loss might result in a gain. The latter effect is beyond the scope of the present paper but is unlikely to change the trends presented herein. The reduction in risk (ΔR) is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack. That is, it is the degree to which new security measures reduce the likelihood of a successful terrorist attack and/or the losses sustained in such an attack.

Figure 2 Event trees of losses



In the example to follow, we will consider three threat levels (low, medium and high) that may influence the threat probability and the losses sustained in a terrorist attack. In principle, risk reduction would also be influenced by threat level; for example, a low level threat such as a 20 kg improvised explosive device (IED) would perhaps be less likely to be detected than a five tonne truck-borne IED. Nonetheless, to assign risk reduction values to these threat levels in the absence of data would be speculative, and it would not aid in illustrating the effect of risk aversion on public decision making. Hence, equation (2) is modified to

$$E(L) = p_{attack}(1-\Delta R)\sum_{j=1}^{3}\Pr\left(L_j \middle| attack\right)L_j \tag{3}$$

where j is the threat level and L_j the losses sustained as a results of threat level j. Figure 2 shows an event tree of events that lead to losses L_j. We assume that a thwarted attack results in no damage (i.e., no fatalities or economic losses).

The attribute (x) under consideration is monetised costs of counter-terrorism and losses sustained from a terrorist attack. Utility theory provides a means of evaluating the risk preferences of the interested parties under choice uncertainty. The expected utility $E[u]$ is thus:

$$E[u] = \underbrace{p_{attack}\left[\Delta R u\left(C_{security}\right) + (1-\Delta R)\sum_{j=1}^{3}\Pr\left(L_j \middle| attack\right)u\left(C_{security}+L_j\right)\right]}_{attack} + \underbrace{\left(1-p_{attack}\right)u\left(C_{security}\right)}_{no\ attack} \tag{4}$$

where $u(x)$ is the utility for cost x expressed as a utility function, and $C_{security}$ is the annual cost of security. The objective of the decision-making process is to maximise the expected utility.

2.2.2 Threat scenarios

The definition of threat scenarios is subjective and subject to uncertainty. However, there is enough evidence to allow reasonable estimates of threat likelihood and their consequences.

If the loss of life from the 9/11 attacks is valued at $20 billion [value of statistical life equals $6.5 million – Robinson, (2008)], direct physical damage at $30 billion, and loss of GDP at $70 to $140 billion (equivalent to 0.5% to 1% of GDP), the total losses come to approximately $120 to $190 billion. To account for other indirect losses like social disruption, we will err on the conservative side and adopt $200 billion as the full cost of losses experienced from the 9/11 attacks (Mueller and Stewart, 2011).

A RAND study developed a 'moderate' case in which a terrorist attack on the USA results in 1,175 deaths and 8,700 injuries costing $6.1 billion. To this is added $1.6 billion in property damage and $6.1 billion in reduced GDP, for a total loss of $13.8 billion in direct and indirect damage in 2010 dollars (Zycher, 2003). And an Australian study commissioned by the Australian Federal Police investigated the economic effects of a terrorist attack similar in scope to the July 2005 London bombings, concluding that the total loss would range from $1 to $5 billion (Ungerer et al., 2008). The losses sustained from the 2005 London and 2004 Madrid bombings amounted to no more than $5 billion.

An analysis of the Global Terrorism Database (GTD) (1970–2007) shows that, of 219 terrorist incidents in the UK involving explosives, only two inflicted damage that were considered by the GTD to be 'catastrophic' – a bombing in London that killed three people in 1992 and the 1993 London financial area bombing, each causing damage of one or two billion dollars.[1] Sixteen others inflicted major damage (from $1 million to $1 billion), and 202 caused damage of less than $1 million dollars. While any death is

regrettable, the GTD shows that the most likely outcome from a terrorist attack in the USA (or UK) is one, perhaps two fatalities, inflicting damage that is limited, even minor. A monetary value placed on such attacks (including the costs of the loss of life) would run into the tens of millions of dollars per attack, and not much more. Most domestic and transnational terrorist attacks kill very few, if any, people. Few terrorist acts inflict many deaths, and most kill no one at all.

Actually, to substantially outdo 9/11, terrorists would need to acquire an atomic arsenal and the capacity to deploy and detonate it, a prospect that continues to excite great alarm. A specific effort to assess the effects of atomic terrorism is included in a 2006 RAND study evaluating the detonation of a 10-kiloton (that is, Hiroshima-size) nuclear device at the Port of Long Beach in California. It concludes that total losses of $1 trillion could be expected (Meade and Molander, 2006). While the potential losses of 'nightmare' scenarios are unlimited, the losses from a detonation of a 10-kiloton nuclear device would seem to be a credible upper limit on losses. For more details on threats and losses see Mueller and Stewart (2011).

We assume three levels of threat and losses associated with a major (even 'catastrophic') terrorist attack:

1 Low: L_1 = \$5 billion

   $\Pr(L_1|attack) = 0.85$

   Represents a London or Madrid mass transit attack. Most likely type of 'major' attack (most terrorist attacks cause much less than \$5 billion in losses).

2 Medium: L_2 = \$200 billion

   $\Pr(L_2|attack)=0.10$

   Represents a 9/11 scale of attack. Less likely type of attack (damage on the scale of 9/11 attack is unprecedented in history of terrorism).

3 High: L_3 = \$1 trillion

   $\Pr(L_3|attack)= 0.05$

   Represents a nuclear or other WMD terrorist attack. Remote probability of attack.

The losses include direct physical damage, loss of life and indirect losses such as loss of GDP or tourism. They also present worst-case type scenarios as most domestic and transnational terrorist attacks kill very few people.

2.2.3 Risk reduction

In assessing risk reduction ΔR, it is important first to look at the effectiveness of homeland security measures that were in place before 9/11 in reducing risk. The 9/11 commission's report points to a number of failures, but it acknowledges as well that terrorism was already a high priority of the US Government before 9/11, pointing out that a 1998 Presidential Decision Directive "reiterated that terrorism was a national security problem, not just a law enforcement issue" (NC, 2004). Moreover, it notes that the efforts of the National Security Council, State Department, Pentagon, CIA, and Justice

Department "were sometimes energetic and *sometimes effective*. Terrorist plots were disrupted and individual terrorists were captured" (NC, 2004). In a review of 20 studies, Mosteller and Youtz (1990) found that the expression 'sometimes' corresponds to a probability of 19% to 38%. The 9/11 commission report's observation that pre-9/11 security was 'sometimes effective' could quite reasonably be said to translate into a risk reduction in that range.

More pointed is an observation of Sheehan (2008), former New York City Deputy Commissioner for Counterterrorism:

> "The most important work in protecting our country since 9/11 has been accomplished with the capacity that was in place when the event happened, not with any of the new capability bought since 9/11. I firmly believe that those huge budget increases have not significantly contributed to our post-9/11 security …. The big wins had little to do with the new programs."

There is another consideration. The tragic events of 9/11 massively heightened the awareness of the public to the threat of terrorism, resulting in extra vigilance that has often resulted in the arrest of terrorists or the foiling of terrorist attempts. Most dramatically, because airplane passengers have become much more attuned to suspicious behaviour of their fellow passengers, two terrorist attempts to blow up airliners have been foiled: the shoe bombing effort of 2006 and the underwear effort of 2009. Both were detected and restrained by crews and passengers, not by the many costly enhanced security measure put into place by the Transportation Security Administration (TSA). The same holds for the peddler in New York who reported the smoking vehicle bomb in Times Square in 2010. And tip-offs have been key to prosecutions in many of the terrorism cases in the USA since 9/11. This cost-free, and effective, response to a threat has likely helped to reduce risk considerably.

In our analysis we will assume that risk reduction caused by the security measures in place before 9/11, re-deployment of existing capabilities, and the extra vigilance of the security services and public after 9/11 reduced risk by 50%. This is a conservative estimate not only because of Sheehan's observation, but because security measures that are at once effective and relatively inexpensive are generally the first to be implemented – for example, one erects warning signs on a potentially dangerous curve in the road before rebuilding the highway. Thus, a 2006 RAND study on reducing terrorism risks at shopping centres found that the least costly measures, suspicious package reporting, reduced risk by 60%, but the costly and inconvenient searching of bags at entrances achieved only 15% risk reduction. Overall, in fact, the cheapest six security measures reduced risk by 70%, and the remaining 12 more costly security measures reduced risks by only another 25% (LaTourrette et al., 2006). Furthermore, most terrorists (or would-be terrorists), do not show much intelligence, cleverness, resourcefulness, or initiative (e.g., Kenney, 2010), and terrorist organisations often suffer from difficulties of coordination (Eilstrup-Sangiovanni and Jones, 2008). Therefore, measures to deal with them are relatively inexpensive and are likely to be instituted first. Dealing with the smarter and more capable terrorists or their organisations is more difficult and expensive, but these people represent, it certainly appears, a decided minority among terrorists.

The DHS and TSA provide possibly the best yardstick of what additional risk reductions are possible due to enhanced expenditures. In a 2008 press release they were proud to announce that regulations associated with rail transportation of toxic inhalation

hazards, which were aimed at reducing risk by 50%, actually achieved an overall risk reduction of more than 60% (TSA, 2008). These agencies are not known for under-selling their achievements. If they can trumpet that their target risk reduction is 50% (to be achieved by developing 'sound security measures without excessively burdening owners and operators'), this can only be viewed as a target that they are eager to endorse. A target or aim is something that is ambitious in nature, and the fact that the TSA was aiming for a risk reduction of 50%, and not a more newsworthy 80% or 90% or 99%, is an excellent indicator of the kind of risk reduction they believe can be achieved at reasonable cost.

In addition, we will assume that the increase in US expenditures on homeland security since 2001 has been effective, reducing the remaining risk by an additional 45%. Total risk reduction, then is assumed to be 95% with the pre-existing measures and the extra public vigilance responsible for 50% of the risk reduction and the enhanced expenditures responsible for the remaining 45%. This, too, is a very conservative assumption, because a risk reduction of 95% is extremely challenging to achieve for any complex system: given the ease with which a bomb can be set off or a bullet fired, no set of security measures is guaranteed to foil or protect against nearly every terrorist attack.

2.2.4 Utility functions and maximising expected utility

While there are many policy options and strategies available to counter-terrorism planners, for the sake of illustration we will assume that the decision-maker has two policy options:

1 No enhanced security expenditure since 9/11:
   - $C_{security}$ = \$35 billion per year
   - ΔR = 50%
2 Increased homeland security expenditure of \$75 billion per year:
   - $C_{security}$ = \$110 billion per year
   - ΔR = 95%

The expected utilities for:

1 no enhanced security expenditure since 9/11 E_{NO}
2 regulatory action associated with enhanced homeland security expenditure of \$75 billion per year $E_{\$75}$ are thus:

$$
\begin{aligned}
E_{NO}[u] &= \underbrace{p_{attack}\left[0.5u(\$35\text{ billion}) + 0.5\sum_{j=1}^{3}\Pr\left(L_j\middle|attack\right)u\left(L_j\right)\right]}_{attack} \\
&\quad + \underbrace{\left(1-p_{attack}\right)u(\$35\text{ billion})}_{no\ attack} \\
E_{\$75}[u] &= \underbrace{p_{attack}\left[0.95u(\$110\text{ billion}) + 0.05\sum_{j=1}^{3}\Pr\left(L_j\middle|attack\right)u\left(\$110 + L_j\right)\right]}_{attack} \\
&\quad + \underbrace{\left(1-p_{attack}\right)u(\$110\text{ billion})}_{no\ attack}
\end{aligned}
\tag{5}
$$

where $u(x)$ is the utility for cost x.

Large firms or government organisations tend to be risk-neutral (e.g., Ang and Tang, 1984; Sunstein, 2002; Faber and Stewart, 2003; Ellingwood, 2006). If the utility functions in equation (5) are expressed as linear utility functions then this is a risk neutral analysis. If the attribute x is a monetary unit, then a risk neutral or linear utility function implies that a decision will be made solely on the expected monetary value. In this case, the utility function is:

$$u(x) = 1.0 - \frac{x}{1{,}110} \quad \$0 \le x \le \$1{,}110 \text{ billion} \tag{6}$$

where utility is highest ($u = 1.0$) when costs and losses are zero, and lowest ($u = 0$) when costs equal total loss of \$1.110 trillion ($C_{security} + L_3$).

In utility theory, the value of $u(B)$ is generally expressed as:

$$u(B) = pu(A) + (1-p)(C) \text{ where } u(A) > u(B) > u(C) \tag{7}$$

and where p is selected such that the decision-maker is indifferent (i.e., outcomes equally preferable) between selecting consequence B with a certain outcome, and a lottery in which he or she would receive consequence A with a probability p and receive consequence C with a probability of $(1 - p)$. A linear utility function is, in general, appropriate for decision-makers in governments or large companies that can afford to sustain a loss (C) on a 50–50 chance ($p = 0.5$) of making a substantial profit (A). However, this would not be true among individuals making decisions involving monetary values that are large in relation to their working capital (Benjamin and Cornell, 1970). Therefore, it would be expected that these individual decision-makers would only take a gamble if the risk of loss $(1 - p)$ is small (e.g., $p = 0.8$). For larger risks (e.g., $p < 0.8$) the individual might prefer to take no risk (avoid the gamble) and settle for the guaranteed expected outcome B. Such a decision-maker is 'risk-averse' and his/her preferences are manifested in a concave utility function.

While there are many types of risk-averse utility functions, the normalised exponential utility function (Ang and Tang, 1984) is used herein due to its improved tractability for this decision problem when compared to other utility functions:

$$u(x) = \frac{1}{1-e^{-\gamma}}\left(1 - e^{-\gamma\left(\frac{x_{\max}-x}{x_{\max}}\right)}\right) \quad \gamma \ge 0 \tag{8}$$

where γ is the risk-averse shape factor and $x_{\max}$ in this case is \$1,110 billion. As γ increases the utility function becomes more concave and so the level of risk averseness increases. The utility faction is linear when $\gamma = 0$. An exponential utility function implies constant absolute risk aversion.

2.3 Results

2.3.1 Risk neutral utility function

A risk neutral or linear utility function reveals that when p_{attack} = 1.0 per year the expected utility of no enhanced security expenditure is vastly higher than for regulatory action – i.e., $E_{NO}[u] = 0.9508$ and $E_{\$75}[u] = 0.8976$. This means that even if there is one

major attack per year, the no enhanced security expenditure policy option is preferable. If the attack probability is reduced to 0.5 per year (or mean rate of major attack is once every two years), then a linear utility function yields $E_{NO}[u] = 0.9597$ and $E_{\$75}[u] = 0.8992$. Clearly, if the attack probability is less than 1.0 per year then no enhanced security expenditure is preferred to regulatory action.

The OMB recommends an expected value analysis when assessing costs and benefits of US regulations. This type of analysis is obtained by replacing the utility function $u(x)$ by cost x, such that for example, $u(C_{security} + L_j)$ is replaced by $C_{security} + L_j$ in equation (5). The expected cost is thus:

$$E[x] = \underbrace{p_{attack}\left[\Delta R C_{security} + (1-\Delta R)\sum_{j=1}^{3}\Pr\left(L_j \middle| attack\right)\left(C_{security} + L_j\right)\right]}_{attack} + \underbrace{\left(1 - p_{attack}\right)C_{security}}_{no\ attack} \tag{9}$$

where the preferred policy option is one with least expected costs.

If $p_{attack} = 1.0$ per year then this expected value analysis yields $E_{NO}[x] = \$72.125$ billion and $E_{\$75}[x] = \$113.713$ billion. This suggests that regulatory action requiring \$75 billion in homeland security expenditure results in an increase in expected costs of \$41.6 billion per year. In other words, spending \$75 billion in additional homeland security expenditure reduces losses by \$33.4 billion and so the benefits are minor and outweighed by the additional costs.

Evidence to date suggests that the number of foiled attacks that had the potential to cause more than \$5 billion in losses (L_1) in the USA are very few, and significantly less than one per year. Even if the attack probability was taken as 1.0 per year then a rational decision analysis would only support \$75 billion of enhanced homeland security expenditure if the decision maker is risk-averse.

2.3.2 Risk-averse utility function

To assess the tipping point shape of the risk-averse utility function, the attack probability is fixed, and the expected utilities using an identical risk-averse utility function for both policy options are calculated from equation (5) and compared and made equal to each other by modifying the risk-averse shape factor γ'. This means that both policy options are equally preferable when $E_{\$75}[u] = E_{NO}[u]$ and the shape factor γ represents a 'tipping point' – so if the decision-maker is any more risk-averse ($\gamma > \gamma'$) then $E_{\$75}[u] > E_{NO}[u]$ and so regulatory action (\$75 billion homeland security expenditure) is preferable. On the other hand, if the decision-maker is less risk-averse ($\gamma < \gamma'$) then no enhanced security expenditure is the preferable policy option. Hence,

$$\begin{aligned} &E_{NO}[u] > E_{\$75}[u] \text{ if } \gamma < \gamma' \\ &E_{NO}[u] = E_{\$75}[u] \text{ if } \gamma = \gamma' \\ &E_{NO}[u] < E_{\$75}[u] \text{ if } \gamma > \gamma' \end{aligned} \tag{10}$$

When $p_{attack} = 1.0$ per year both policy options are equally preferable when $\gamma' = 2.74$ and so $E_{NO}[u] = E_{\$75}[u] = 0.9757$. Figure 3 shows the shape of this risk-averse utility function, and if the decision-maker is any more risk-averse than Figure 3 then DHS policy is

preferable. The level of risk aversion is significant even when the mean rate of attack is one per year, as when $\gamma' = 2.74$ this infers that the decision maker will be indifferent to choosing a certain \$500 billion loss or a lottery with 83.2% probability of zero loss and 16.8% chance of a \$1.11 trillion loss. In other words, when decision makers are risk-averse they accept less probability of loss the larger the loss.

Figure 3 Comparison of 'tipping point' risk-averse utility functions defined by shape factor γ'

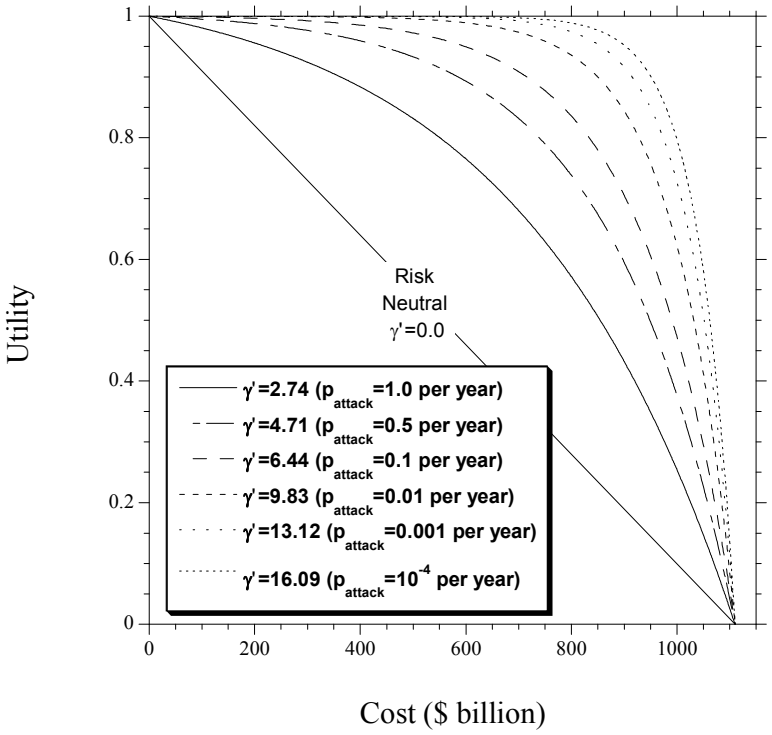


Table 2 Tipping point shape factor (γ') for risk-averse utility function

Attack probability per year (p_{attack})	$E_{NO}[u] = E_{\$75}[u]$	γ'
1.0	0.9757	2.74
0.5	0.9889	4.71
0.1	0.9983	6.44
0.01	0.9999	9.83
10^{-3}	0.9999	13.12
10^{-4}	1.0000	16.09

Table 2 shows the 'tipping point' shape factor γ' needed to ensure that $E_{NO}[u] = E_{\$75}[u]$, for attack probabilities ranging from 10^{-4} to 1.0 per year. The shape factor increases as attack probability decreases, indicating higher levels of risk aversion. Figure 3 shows the utility functions are increasingly concave as attack probability decreases. It is observed that when the probability of a major attack falls below 0.1 per year (or mean rate of major attack is once every ten years), the preference of no loss or a loss of several hundred

billion dollars are near identical. Moreover, when the attack probability is 0.01 per year then the decision maker will be indifferent to choosing a $500 billion loss or a lottery with 99.6% probability of zero loss and 0.4% chance of a $1.11 trillion loss.

2.3.3 Sensitivity analysis

Note that the results will change for different input variables, but the trends are still the same. For example, if major loss L_3 is less than $1 trillion or $\Pr(L_3|attack)$ is less than 0.05, then γ' increases, leading to increased risk averseness. If maximum loss (L_3) is doubled to $2 trillion, then γ' decreases to 1.23 and 2.39, for attack probabilities of 1.0 and 0.5, respectively. If $\Pr(L_1|attack)$ is increased from 0.85 to 0.90, and $\Pr(L_2|attack)$ reduced from 0.10 to 0.05, then 'tipping point' shape factors change negligibly. The shape factor reduces slightly if there is higher probability of more severe attacks; for example, the shape factor reduces to 1.78 and 3.50 when $\Pr(L_1|attack) = 0.5$ and $\Pr(L_2|attack) = 0.45$, for attack probabilities of 1.0 and 0.5, respectively. If it is believed that the risk reduction in the absence of enhanced homeland security expenditure is overly-optimistic and risk reduction resulting from enhanced homeland security expenditures is too pessimistic, then we may assume that $\Delta R = 25\%$ and $\Delta R = 99\%$, for no enhanced security expenditure and $75 billion enhanced homeland security expenditures, respectively. In these cases, $\gamma' = 1.77$ and $\gamma' = 2.98$, for attack probabilities of 1.0 and 0.5, respectively. However, the level of risk averseness for utility functions with these shape factors still represents significant levels of risk averseness.

Different risk averse utility functions, such as lognormal or quadratic expressions, might also have been used in this analysis. However, the analysis herein is a comparative analysis, so while the expected utilities would differ for other utility functions, the trends exhibiting increasing risk averseness with reducing attack probability would be very similar to those shown in Figure 3.

A recent statement by DHS Secretary Janet Napolitano that there had been "a metamorphosis of the tactics and techniques ... from the large-scale conspiracy to smaller-scale smaller events that are more difficult by their nature to infiltrate" (Dombey, 2010) suggests that large scale attacks are less likely. A reasonable upper limit loss might then be $L_1 = L_2 = \$5$ billion and not $1 trillion as assumed above. In this case, $\Pr(L_1|attack) = 0.85$, $\Pr(L_2|attack) = 0.15$ and $L_3 = 0$ then the 'tipping point' shape factor γ' must exceed 999.0 when attack probability is 1.0 per year. The same result holds true if the upper limit of loss is increased to $200 billion. Clearly, this is as extreme a case of risk aversion as possible since $u(x) = 1.0$ for all costs x.

The results presented in Table 1 and Figure 3 is not overly sensitive to the threat likelihood, risk reduction or loss scenarios. Moreover, we have taken conservative assumptions, and less conservative assumptions would lead to even higher levels of risk aversion being required for $75 billion of homeland security to be the preferred policy option.

2.4 Discussion

Since the attack probability or mean rate of attacks in the USA for attacks with the potential to cause more than $5 billion of damage (or loss of life) is likely to be less than one per year, then the only rational explanation as to why the DHS is making decisions to invest $75 billion per year in homeland security is that the agency is significantly risk-

averse. This in itself is not surprising, but what is significant is the quantifiable extent of risk averseness as represented in Figure 3. Experience would suggest that few, if any, government agencies such as the NRC or EPA exhibit anywhere near this level of risk aversion in their public decision making. These differences are the focus of future research.

The decision analysis used herein is preliminary, and serves to illustrate some important aspects of risk aversion for public decision-making. We have used well known and accepted utility theory, and while the methods are not novel, the application to homeland security has not been attempted previously. In policy making there are often more than two policy options, and the two selected herein represent two extreme policy decisions to illustrate the key points. In reality, the allocation and effectiveness of homeland security expenditure would result in many policy options, and each would need careful and detailed decision analysis to gain insights into their costs and benefits. Moreover, if public policy makers are to make decisions that might not be supported by a quantitative decision analysis, then their degree of risk averseness needs to be quantified, and compared with other public policy decisions. This would make the trade-offs more transparent, and highlight if the degree of risk aversion is excessive or justified.

It would also highlight if public funds could be used more productively elsewhere since risk-averse behaviour will lead to allocation of funds away from more effective risk mitigating policy options. For example, what is foregone in order to expend $75 billion per year on homeland security? Diverting a small percentage of that sum could save many lives at a fraction of the cost. Specifically, the money would be more effective – save far more lives – if it were instead spent on (Mueller and Stewart, 2011):

- seat belts at a cost of $40,000 per life saved
- bike helmets for children at a cost of $120,000 per life saved
- tandem mass spectrometry screening programme at a cost of $800,000 per life saved
- adult bike helmets for adults at a cost of $1 million per life saved
- front air bags at a cost of $2 million per life saved
- smoke alarms at a cost of $2 million per life saved
- tornado shelters at a cost of $6 million per life saved.

There are countless examples where governments can invest wisely in programmes that provide a net life-saving benefit to society.

3 Conclusions

There has been an increase of more than a trillion dollars in homeland security expenditures in the USA in the ten years since 2001. This large public and private expenditure has not been subject to cost-benefit analysis as recommended by the US OMB. Governments and their regulatory agencies normally exhibit risk-neutral attitudes that use expected values or linear utility functions in their decision-making. The paper inferred utility functions that reflect the level of risk averseness of regulatory agencies when adopting new safety measures – such as $75 billion of enhanced homeland security spending per year to avert terrorist attacks in the USA. The utility analysis considered

threat probability, risk reduction caused by regulatory action, cost of regulatory action, and losses. The expected utilities using an identical risk-averse utility function for:

1 no enhanced security expenditure

2 regulatory action associated with \$75 billion of enhanced homeland security expenditure are compared and made equal to each other by modifying the risk-averse function.

This means that both policy options are equally preferable and represents a 'tipping point' – if the decision-maker is more risk-averse than suggested by the risk-averse utility function then regulatory action is preferable. It was found that the level of risk averseness needed to justify current expenditures for homeland security is considerable. Moreover, the degree of risk averseness increased as the threat probability decreased.

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

Ang, A.H-S. and Tang, W.H. (1984) 'Probability concepts in engineering planning and design', *Decision, Risk and Reliability*, Vol. 2, John Wiley & Sons, New York.

Benjamin, J.R. and Cornell, C.A. (1970) *Probability, Statistics, and Decision for Civil Engineers*, McGraw-Hill, New York.

Binning, D. (2009) 'The price of homeland security', available at http://www.Army-technology.com (accessed on 5 June 2009).

Dombey, D. (2010) 'Al-Qaeda shift raises US terror risk', *Financial Times*, 8 November 2010.

Eilstrup-Sangiovanni, M. and Jones, C. (2008) 'Assessing the dangers of illicit networks: why Al-Qaeda may be less dangerous than many think', *International Security*, Vol. 33, No. 2, pp.7–44.

Ellingwood, B.R. (2006) 'Mitigating risk from abnormal loads and progressive collapse', *Journal of Performance of Constructed Facilities*, Vol. 20, No. 4, pp.315–323.

Faber, M. and Stewart, M.G. (2003) 'Risk assessment for civil engineering facilities: critical overview and discussion', *Reliability Engineering and System Safety*, Vol. 80, No. 2, pp.173–184.

Farrow, S. (2007) 'The economics of homeland security expenditures: foundational expected cost-effectiveness approaches', *Contemporary Economic Policy*, Vol. 25, No. 1, pp.14–26.

GHS (2009) *Global Homeland Security 2009–2019 – Our New Defence Report Explains How and Why This Market Will Grow Strongly*, Visiongain, June.

Hardaker, J.B., Fleming, E. and Lien, G. (2009) 'How should governments make risky policy decisions?', *Australian Journal of Public Administration*, Vol. 68, No. 3, pp.256–271.

Hobijn, B. and Sager, E. (2007) 'What has homeland security cost? An assessment: 2001–2005', *Current Issues in Economics and Finance*, Vol. 13, No. 2, pp.1–7, Federal Reserve Bank of New York.

Jordaan, I. (2005) *Decisions under Uncertainty: Probabilistic Analysis for Engineering Decisions*, Cambridge University Press, Cambridge, UK.

Kenney, K. (2010) ''Dumb' yet deadly: local knowledge and poor tradecraft among Islamist militants in Britain and Spain', *Studies in Conflict and Terrorism*, Vol. 33, No. 10, pp.1–22.

LaTourrette, T., Howell, D.R., Mosher, D.E. and MacDonald, J. (2006) *Reducing Terrorism Risk at Shopping Centers An Analysis of Potential Security Options*, RAND Corporation, Santa Monica, CA.

Meade, C. and Molander, R.C. (2006) *Considering the Effects of a Catastrophic Terrorist Attack*, RAND, Santa Monica.

Mosteller, F. and Youtz, C. (1990) 'Quantifying probabilistic expressions', *Statistical Science*, Vol. 5, No. 1, pp.2–12.

Mueller, J. (2010) 'Assessing measures designed to protect the homeland', *Policy Studies Journal*, Vol. 38, No. 1, pp.1–21.

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

NC (2004) *The 9/11 Commission Report*, National Commission on Terrorist Attacks Upon the United States, 22 July.

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

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

OMB (2010) *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2011,* Office of Management and Budget, Washington, DC.

Paté-Cornell, E. (2002) 'Risk and uncertainty analysis in government safety decisions', *Risk Analysis*, Vol. 22, No. 3, pp.633–646.

Robinson, L.A. (2008) *Valuing Mortality Risk Reductions in Homeland Security Regulatory Analyses*, Final Report, US Customs and Border Protection, Department of Homeland Security, June 2008.

Sheehan, M.A. (2008) *Crush the Cell: How to Defeat Terrorism without Terrorizing Ourselves*, Crown Publishers, New York.

Stewart, M.G. (2010a) 'Acceptable risk criteria for infrastructure protection', *International Journal of Protective Structures*, Vol. 1, No. 1, pp.23–39.

Stewart, M.G. (2010b) 'Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure', *International Journal of Critical Infrastructure Protection*, Vol. 3, No. 1, pp.29–40.

Stewart, M.G. and Mueller, J. (2008a) 'A risk and cost-benefit and assessment of US aviation security measures', *Journal of Transportation Security*, Vol. 1, No. 3, pp.143–159.

Stewart, M.G. and Mueller, J. (2008b) 'A cost-benefit and risk assessment of Australian aviation security measures', *Security Challenges*, Vol. 4, No. 3, pp.45–61.

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

TSA (2008) Transportation Security Administration, *DHS Announces Security Standards for Freight and Passenger Rail Systems*, Press Release, 13 November.

Ungerer, C., Ergas, H., Hook, S. and Stewart, M.G. (2008) *Risky Business: Measuring the Costs and Benefits of Counter-Terrorism Spending*, Special Report – Issue 18, November, Australian Strategic Policy Institute, Canberra.

Wilson, R. and Crouch, E.A.C. (1987) 'Risk assessment and comparisons: an introduction', *Science*, Vol. 236, pp.267–285.

Zycher, B. (2003) *A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures*, RAND, Santa Monica.

Notes

1 The GTD defines a single terrorist attack as one occurring in the same geographic area and at the same point in time. Hence, the 2005 London attacks are regarded as four incidents.