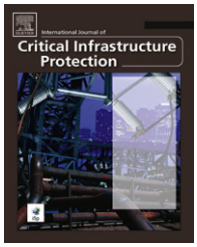
available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip



Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure

*Mark G. Stewart**

Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales, 2308, Australia

ARTICLE INFO

Article history:
Received 16 April 2009
Received in revised form
2 July 2009
Accepted 13 September 2009

Keywords:
Risk
Terrorism
Costs and benefits
Counter-terrorism
Decision making

ABSTRACT

The paper describes risk-informed decision support for assessing the costs and benefits of counter-terrorism (CT) protective measures for infrastructure. Such a decision support framework needs to consider threat scenarios and probabilities, value of human life, physical (direct) damage, indirect damage, risk reduction and protective measure costs. Probabilistic terrorism risk assessments that quantify the costs and benefits are conducted for three items of infrastructure using representative cost and vulnerability data. The illustrative examples show under what combination of risk reduction, threat probability, and fatality and damage costs the CT protective measures would be cost-effective for United States building, bridge and aviation infrastructure. It was found that if indirect losses (such as business interruption, loss of GDP, etc.) are considered, then CT protective measures are cost-effective even if the terrorist threat probability is not high. Opportunity costs can be considerable, which makes CT protective measures less cost-effective.

1. Introduction

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. 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. For example, since 2001 over $300 billion has been spent by US government agencies on counter-terrorism (CT) protective measures in the US homeland. Of this, approximately $90 billion has been spent by the US government on 'protecting critical infrastructure and key resources [1]'.[1] A key issue is whether this CT expenditure has been invested in a manner that optimises public safety in a cost-effective manner. This is why the 9/11 Commission report, amongst others, called on the US government to implement security measures that reflect assessment of risks and cost-effectiveness [2]. The present paper will thus describe risk-informed decision

[1] The National Strategy for Homeland Security uses the term "key assets", defined as individual targets whose destruction would not endanger vital systems, but could create a local disaster or profoundly damage the nation's morale or confidence. The Homeland Security Act and HSPD-7 use the term "key resources", defined more generally to capture publicly or privately controlled resources essential to the minimal operations of the economy or government.

* Tel.: +61 2 49216027.
E-mail address: mark.stewart@newcastle.edu.au.

1874-5482/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2009.09.001

support for assessing the costs and benefits of CT protective measures for infrastructure.

Many reports and studies in the US, Australia and elsewhere have highlighted the vulnerability of critical infrastructure to the continuing threat of terrorism (e.g., [3,4]). The list of vulnerable infrastructure entities is extensive, and typically includes buildings, bridges, airports, dams, pipelines, and nuclear facilities. In the United States the number of items of such infrastructure is immense and includes 600,000 highway bridges, hundreds of thousands of tall buildings, over 400 large airports, etc. Since mitigation measures often comprise many, and costly, protective measures, there is thus clearly a need to assess their effectiveness.

While there is often a high degree of certainty about CT protective expenditure, there is considerable uncertainty about the benefits of such expenditure – e.g., there is uncertainty about CT protective effectiveness, the threat may never materialise (or evolve over time), consequences may depend on time of day of attack, and so on. These uncertainties can be quantified by probabilistic and reliability methods, and it is these uncertainties that contribute to 'risk'. The conventional definition of risk is the combination of threat probability, risk reduction and consequences (e.g. [5]). This definition is consistent with that used by the US Department of Homeland Security (DHS) National Infrastructure Protection Plan [6] where risk is assessed 'from any scenario as a function of consequence, vulnerability, and threat'. However, it is interesting to note that the DHS National Infrastructure Protection Plan makes no reference to risk acceptance criteria, only the calculation of risks.

The need for a decision making framework that enables security risks to be quantified has been widely recognised (e.g., [3,7]) and decision frameworks for security risk management developed (e.g., [8–10]). Yet most decision frameworks are developed for initial risk screening or ranking/prioritisation purposes and so they cannot be used to directly compare costs and benefits. A key issue which is largely unresolved is the quantification of threat probability, risk reduction and costs of mitigating measures to predict expected losses or benefits. However, the quantification of security risks and their reduction due to protective measures is recently being addressed by some researchers (e.g., [11–17]), as well as recent life-cycle and cost–benefit analyses for infrastructure protective measures [18,14,19,20]. Much of this work can be categorised as 'probabilistic terrorism risk assessment' [21].

A cost–benefit analysis provides a means to measure the cost associated with reducing, avoiding or transferring the risk. This allows the decision maker to make a risk-informed decision about whether such a cost is excessive, therefore failing to be a productive utilisation of society's resources. Activities related to nuclear energy, chemical processes, aviation, etc. with large potential for loss of life or severe economic or social consequences have since the 1960's been subject to methodical and quantitative risk assessment [22]. Many of these systems are characterised by their low probability of failure and high consequences, as well as the need to address such contentious issues as value of life, risk aversion, risk acceptability, and in many cases, modelling human actions and reactions using a human reliability analysis. Terrorist threats have similar characteristics and decision support challenges and issues. The key exception, however, is in the estimation of threat probability.

For many engineering systems the hazard (or threat) rate is known or predicted '*a priori*', but for terrorism the threat is from an intelligent adversary who will adapt to changing circumstances to maximise likelihood of success. Some statistical approaches exist for terrorist threat prediction (e.g., [23,16,17]); however, these rely heavily on expert judgments from security experts, game theory, etc. so the inherent uncertainties can still be high. For this reason, a DHS report on bioterrorism risks [24] states that "the assessment of the probabilities that adversaries will choose courses of action should be the *outputs* of analysis, not required *input parameters*". Hence, it is recommended that the cost–benefit analysis be used to calculate the minimum (threshold) threat probability for a specific CT protective measure to be cost-effective. In other words, the threat probability is the output of the cost–benefit analysis and it is the prerogative of the decision maker, based on expert advice about the anticipated threat probability, to decide whether or not a CT protective measure is cost-effective. For example, expert advice about the anticipated threat probability is used by the Transportation Security Administration Office of Intelligence who have developed likelihood estimates for specific threat scenarios for highway infrastructure [25].

Several risk-informed approaches to cost–benefit analysis that consider economic and life-safety criteria for CT protective measures for buildings, bridges and other built infrastructure have been developed. Lakamp and McCarthy [26] conducted a cost–benefit assessment of campus security at the US Naval Postgraduate School where benefits included lives saved and reduced property damage from preventing a terrorist attack on an academic building. The study found that "the school is receiving a tiny benefit, at a very high cost". A simplified economic analysis by Little [18] showed that unless the probability of attack against a specific building is high, the expected benefits are unlikely to offset the cost of protecting multiple structures. Stewart [19,20] considered economic and risk acceptance criteria for assessing effectiveness of protective measures for infrastructure, and the economic risks for buildings due to terrorism were shown to be significantly lower than risks due to other (natural) hazards. The above studies all show that CT protective measures for most buildings are often not cost-effective. Following this approach, Stewart and Mueller [27,28] assessed the cost per life saved for Australian and US air marshal programmes and hardening of cockpit doors.

The present paper improves the work of Stewart [19,20] by describing a more detailed probabilistic terrorism risk assessment that considers multiple threat scenarios and likelihoods, value of human life, physical (direct) damage, risk reduction and protective measure costs. While the methodology is consistent with that used for other hazards, there are additional challenges and uncertainties in quantifying risks, particularly for threats such as terrorism where data are scarce or non-existent and where the threat is highly transient, in that the threat environment can change significantly, which may reveal new sources of vulnerability to infrastructure. Decision makers will thus need to rely on judgment and scenario analyses to develop and quantify threat

scenarios, risk reductions and damage consequences. The paper describes a cost–benefit framework and then presents cost–benefit assessments for three items of infrastructure using representative US cost and vulnerability data:

(i) commercial and institutional buildings,
(ii) highway bridges, and
(iii) hardening of cockpit doors.

These example applications will illustrate the cost–benefit process, and highlight where more data or analyses are needed. The risk-based decision support used herein is relatively simple, and so is most suitable for preliminary risk assessments or risk screening. In principle, however, the approach used herein can be extended for a more detailed analysis of costs and benefits of CT protective measures. It should be noted that the probabilistic terrorism risk assessment developed herein will provide complementary information to decision makers, but this or any other risk assessment should not be viewed as the sole criterion for decision making.

2. Cost–benefit assessment

Decision theory provides decision makers with a range of analytical techniques for assessing risk preferences, namely, comparing or balancing risk against costs. An approach that should be suitable for optimising CT protective measures is a decision analysis that compares the extra (marginal) costs of protective/CT measures with the extra (marginal) benefits in terms of fatalities and damage averted. The decision problem is then to maximise the net benefit E_b such that

$$E_b = E\left(C_B\right) + p_{attack} \sum_{i=1}^{M} \sum_{j=1}^{N} \Pr(\Theta_i|attack) \Pr(L_j|\Theta_i) L_j \frac{R_{i,j}}{100} - C_R$$

$$\sum_{i=1}^{M} \Pr(\Theta_i|attack) = 1.0 \tag{1}$$

where $E(C_B)$ is the expected benefit from the CT protective measure not directly related to mitigating terrorist threats (e.g., reduction in criminal behaviour due to enhanced building security, increased consumer confidence), C_R is the extra cost of the CT protective measure, p_{attack} is the annual probability of a successful terrorist attack assuming no protective measures, M is the number of threat scenarios where Θ_i is the threat scenario (e.g., $i = 1$: 50 kg Vehicle Borne Improvised Explosive Device—VBIED, $i = 2$: 250 kg VBIED, $i = 3$: RPG attack, etc.), $\Pr(\Theta_i|attack)$ is the relative threat probability given an attack, L_j is the loss or consequence, N is the number of loss attributes (e.g., $j = 1$: lives lost, $j = 2$: physical damage, $j = 3$: reduction of GDP, etc.), $\Pr(L_j|\Theta_i)$ is the conditional probability of loss given the occurrence of threat scenario Θ_i assuming no protective measures (e.g., probability of occupant fatality given a terrorist attack), and $R_{i,j}$ is the percentage reduction in risk due to CT measures for the ith threat and the jth loss attribute. The product $\Pr(L_j|\Theta_i)L_j$ refers to the expected loss given the occurrence of a threat. All consequences need to be given in the same units, which are usually monetary. It is most convenient to consider a time period of one year, such that Eq. (1) refers to an annual net benefit where costs and benefits are expressed as annual values. A CT protective measure is viewed as cost-effective if the net benefit exceeds zero. If more than one protective measure is assessed, then the CT protective measure with the maximum net benefit is the most cost-effective. The cost of CT protective measures (C_R) might also include opportunity costs such as increased delays due to parking restrictions caused by vehicle barriers or increased stand-off, emergency vehicle access may be delayed, etc.

Eq. (1) is a relatively simple expression of expected costs and benefits. What is novel is the application of such an expression to the field of counter-terrorism. Eq. (1) can be generalised to also consider multiple protective measures, multi-objective decision criteria, risk aversion, utility theory, discounting of future costs, etc. While more complex models are available, these require more input parameters and assumptions, and given that it is very difficult to establish the key parameters in even a simple security model the net benefit calculation given by Eq. (1) is very useful for preliminary risk assessments or risk screening.

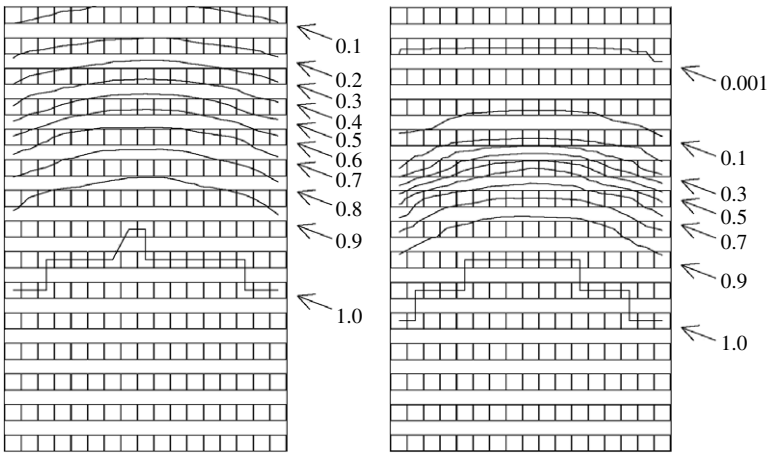
The percentage risk reduction (R) represents the percentage reduction in threat likelihood (p_{attack}, $\Pr(\Theta_i|attack)$) and/or extent of consequences and losses ($\Pr(L_j|\Theta_i)$, L_j). For any CT protective measure the percentage risk reduction R can vary from 0% to 100%. If a combination of CT protective measures will foil every threat then the sum of risk reductions from these CT protective measures is 100%. This soon becomes a multidimensional decision problem with many possible interactions between CT protective measures, threat scenarios, threat probabilities, risk reduction and losses. Fault trees and logic diagrams, together with systems engineering and reliability approaches, will aid in assessing these and other complex interactions involving threats, vulnerabilities and consequences (e.g., [29]).

If the loss attributes are in units other than cost (such as fatalities) then it may be appropriate to define cost-effectiveness using the marginal (or incremental) cost-effectiveness ratio (CER) defined as

$$CER = \frac{\text{cost spent on CT measure}}{\text{losses averted by CT measure}} = \frac{C_R}{p_{attack} \sum_{i=1}^{M} \Pr(\Theta_i|attack) \Pr(L|\Theta_i) L \frac{R_i}{100}}. \tag{2}$$

For example, if L is expressed as number of fatalities then Eq. (2) is the estimated cost per life saved.

A cost–benefit analysis is a robust indicator of societal risk acceptability as it considers costs and benefits in a logical and transparent manner. However, results should be interpreted with some flexibility as other non-quantifiable criteria may be important also in judging the overall acceptability of risks (e.g., [30,22,31,32]). Past experience shows that it is likely that decisions may be made (or over-ruled) on political, psychological, social, cultural, economic, security or other non-quantifiable grounds. For example, some risks may be deemed unacceptable under any conditions based on morality [33] or based on their symbolic value to society.



(a) 10 mm annealed glazing. **(b) 8 mm fully tempered glazing.**

Fig. 1 – Risk contours for High Safety Hazards to a 15-storey building facade [14].

2.1. *Risk reduction*

There are many CT protective measures for infrastructure, ranging from enhanced perimeter security to backup of IT systems to vehicle bollards to parking restrictions to strengthened perimeter columns to ballistic-resistant glazing, etc. The percentage risk reduction (R) is the additional risk reduction achieved by the presence of the CT protective measure when compared to the overall risk reductions achieved by the presence, absence and/or effectiveness of all CT protective measures. For example, consider the case where it is predicted that (i) the probability of strengthened bridge columns in preventing bridge collapse is 0.75, and (ii) the probability of strengthened bridge girders in preventing bridge collapse is 0.75. If this is viewed as a series system where each event probability is statistically independent then the probability of preventing bridge collapse is $1-(1-0.75)^2 = 0.9375$. Now, if an additional CT measure, such as surveillance (e.g., CCTV, security guards), is proposed and the probability of this surveillance foiling a terrorist attack is 0.5 then the probability of preventing bridge collapse is now expected to be $1-(1-0.5)(1-0.75)^2 = 0.9688$. The risk reduction from this proposed CT measure is $100(0.9688-0.9375) = 3.13\%$. So while an individual CT protective measure may be very effective, its contribution when compared to the overall risk reductions achieved by the presence of all CT measures is often reduced. In a similar study, Martonosi and Barnett [34] used system and reliability techniques to estimate the probability of terrorist detection due to security screening of airline passengers. Martonosi and Barnett [34] found that the probability of detection was approximately 0.35, which in our case would mean a risk reduction of $R = 35\%$. So an objective of a cost–benefit assessment is to optimise the extent of CT protective measures needed for this or any other item of infrastructure where many options for CT protective measures exist.

Hence, the estimation of the probabilities of effectiveness for individual CT protective measures and how they contribute to the overall probability of foiling a terrorist attack and the quantification of expected risk reductions is necessary. If predictive resistance, load and threat probabilistic models are available then probabilistic risk assessment is useful for assessing risk reductions. For example, consider the CT protective measure of installing fully tempered glazing for a typical 15-storey commercial building where the main safety hazard to building occupants is assumed to arise from glass fragments. The facade comprises 2 m × 2 m windows and according to Australian glazing design an acceptable design solution for wind loading is either 10 mm annealed glass or 8 mm fully tempered glass. A computational tool "Blast-RF" (*Blast* Risks for Facades) that undertakes a probabilistic risk assessment procedure is used to predict glazing safety hazard risks [35]. The reliability analysis considers the variability of explosive material energetic output, glazing stress limit, fragment drag coefficient, glazing dimensions, stand-off distance and explosive weight to calculate probabilities of glazing safety hazards. The threat scenario is a 100 kg VBIED at a stand-off of 10 m directly in front of the building. The results from Blast-RF are shown as High Safety Hazard risk contours, see Fig. 1. Across the whole facade, the average High Safety Hazard risk is 0.79 for the 10 mm annealed glazing, as compared to 0.63 for the 8 mm fully tempered glazing; i.e., a 20% reduction in risk. As there is a close correlation between a High Safety Hazard rating and extremely serious, if not fatal, wounds then 8 mm fully tempered glazing would reduce fatality risks by 20%. If no other CT protective measures were adopted then risk reduction for this situation is $R = 20\%$.

While there are many advantages to probabilistic and reliability analyses for calculating risk reductions, they are not always appropriate, particularly for the 'new hazard' of terrorism. Hence, as is the case with any risk analysis of a complex system, information about risk reductions may be inferred from expert opinions, scenario analysis, statistical analysis of prior performance data, system modelling as well as probabilistic and reliability analysis.

2.2. *Value of life, risk aversion and other issues*

One of the more contentious issues associated with cost–benefit analyses is how to place a monetary value on human life, often referred to as the value of a statistical

life (VSL). Paté-Cornell [30] suggests that a cost per life saved of $2 million or less is appropriate for current practice, and the United States Department of Transport adopts a figure of $3 million [36]. For most activities a VSL not exceeding $1–$10 million is typical for most US federal agencies as this provides a reasonably accurate reflection of societal considerations of risk acceptability and willingness to pay to save a life [36]. More recently, Robinson [37] in a report for the DHS concluded that $6.3 million is the best VSL estimate for homeland security regulatory analysis. As most VSL studies generally focus on relatively common risks (e.g., workplace or motor vehicle accidents), then Robinson [37] comments that 'more involuntary, uncontrollable, and dread risks may be assigned a value that is perhaps twice that of more familiar risks'. Hence, Robinson [37] also concludes that 'DHS may wish to explore the effects of doubling its VSL estimates in sensitivity analysis'. This doubling of VSL estimates is essentially a measure for including risk aversion in cost–benefit analyses. In the present paper, a VSL of $6.3 million (in 2008 dollars) is adopted, and double that value ($12.6 million) will be used in a sensitivity analysis.

Society tends to spend more money per life saved for efforts to prevent death from 'dread' type risks such as exposure to asbestos and arsenic than for some efforts to prevent death from more mundane activities such as driving a motor vehicle. This is often a function of psychological and political aspects of risk perception [38]. While many individuals may be risk averse, governments need to be risk neutral (i.e., use expected values) and distribute risk reduction funds in a consistent and equitable manner in order to achieve the best outcomes (risk reduction) for society as a whole. The reason for being risk averse is that the events involving high consequences often are associated with 'follow-on' events which themselves may contribute significantly to the risk [39]. The follow-on consequences for a terrorist attack may cause a significant loss of consumer confidence leading to declining sales figures, reduced chances of new tourism investments, reduced government/tax revenue, etc. All such 'follow-on' consequences should be included in the estimation of losses (L_j) which will lead to a 'risk neutral' risk analysis. Nevertheless, utility theory can be used if the decision maker wishes to explicitly factor risk aversion into the decision process (e.g., [40]).

There are also many issues related to assessing economic and financial aspects of costs and benefits. This includes the time horizon, annualising and discounting future costs and benefits to present values and ongoing economic effects of private and public expenditure. For example, Zycher [41] recommends that the total economic cost of security measures is at least twice the direct public expenditure due to the fact that "government must obtain such resources, whether now or in the future, through the tax system (or through such explicit taxation as inflation), which imposes indirect costs upon the economy in the form of resource misallocation". This may also be defined as the marginal excess burden of a tax (deadweight loss). The inclusion of excess tax burden in a cost–benefit assessment is a matter for the decision maker to decide, but it may be more appropriate to include the effects of excess tax burden in a sensitivity analysis.

There are many more issues associated with cost–benefit and decision analyses, issues which cannot all be covered in this paper. The field of cost–benefit analysis is one that encompasses technical (economics, finance, probability, reliability), social (political, psychological, cultural) and other multidisciplinary fields. The influence of all these fields on decision support is well described in the literature (e.g., [40,42,43]).

3. Examples

To illustrate the application of cost–benefit assessment to the protection of infrastructure systems, this section describes cost–benefit assessment for the following infrastructure systems:

(i) commercial and institutional buildings,
(ii) highway bridges, and
(iii) hardening of cockpit doors.

Due to the large number and configurations of these systems, only representative risks and costs are considered (based mainly on US sources) — although some effort has been made to quantify parameters for a typical item of infrastructure, so the results may be viewed as having some applicability to such infrastructure in general. However, for a specific item of infrastructure it is possible to more accurately assess threat scenarios, risks and costs and so produce a more detailed cost–benefit assessment.

In all cases the examples will focus on the minimum (threshold) threat probability or level of risk reduction needed for CT protective measures to be cost-effective. As discussed in Section 1, the threat probability is a matter for the security and intelligence services to predict, and this is an issue beyond the scope of the present paper. On the other hand, the extent of risk reduction can be based on expert judgment (or experience) or, preferably, on detailed reliability and systems analysis.

3.1. *Commercial and institutional buildings*

In this case, CT protective measures for existing multi-storey/large commercial and institutional buildings focus on strengthened perimeter columns and walls, and other structural improvements to the building. Three threat scenarios ($M = 3$) and loss attributes of two types ($N = 2$: direct physical damage and fatalities) are considered. It is assumed that the benefit of building CT protective measures does not extend beyond their intended purpose to prevent terrorist attacks on built infrastructure ($C_B = 0$). However, public awareness of enhanced security measures may mean a greater willingness to use the infrastructure leading to tangible direct and indirect benefits to the asset owner and society, and in principle such benefits could be included in a cost–benefit analysis as shown in Eq. (1). The net benefit given in Eq. (1) is re-expressed for this example as

$$E_b = p_{attack} \sum_{i=1}^{3} \Pr(\Theta_i|attack) \frac{R_i}{100} \times \left[\Pr(L_1|\Theta_i)L_1 + \Pr(L_2|\Theta_i)(L_2 \times C_{life})\right] - C_R \quad (3)$$

Table 1 – Hypothetical threats, losses and risk reduction for an example building.

Threat	Relative threat probability $\Pr(\Theta_i \mid attack)$	Probability of physical damage $\Pr(L_1 \mid \Theta_i)$	Probability of fatalities $\Pr(L_2 \mid \Theta_i)$	Risk reduction R_i (%)
$i = 1$, low	0.6	0.25	0.1	95
$i = 2$, medium	0.3	1.0	0.25	70
$i = 3$, high	0.1	1.0	0.5	50

Table 2 – Probability of occupant fatality for recent US terrorist attacks.

	Fatalities	Building occupants	Probability of occupant fatality $\Pr(L_2 \mid \Theta)$
World Trade Center (1993)	6	17,550[a]	0.0003
Alfred P. Murrah Federal Building (1995)	163	361–850	0.19–0.45[b]
World Trade Center (2001)	2427	35,100[a]	0.069
Pentagon (2001)	125	16,200[a]	0.008

[a]Estimated from average occupant density of four people per 100 m^2.
[b]Uncertainty of number of occupants at time of attack.

where L_1 is the cost of direct physical damage (building replacement, damage to contents), L_2 is the number of people exposed to the hazard (building occupants), C_{life} is the value of a single life (VSL) expressed in monetary units, and R_i is the percentage reduction in risk due to CT protective measures for the ith threat. It is assumed that percentage risk reduction is equal for all loss attributes. This example does not consider the risk and safety of people outside the building (such as pedestrians).

The three threat scenarios are assumed to cover low, medium and high threats. A low threat may be a VBIED with low explosive weight or large stand-off, whereas medium or high threats would involve, for example, larger VBIED explosive weights and reduced stand-off. It is assumed that the relative threat probability $\Pr(\Theta_i \mid attack)$ reduces as the threat level increases due to reduced likelihood of conducting such an attack undetected as the size of vehicle increases or as the vehicle moves closer to the target building; see Table 1. Table 2 shows the probability of building occupant fatality given a terrorist attack $\Pr(L_2 \mid \Theta_i)$ for recent terrorist attacks on buildings in the US. The probability that an individual in such a building is killed is, in most cases, quite low and so $\Pr(L_2 \mid \Theta_i)$ is assumed relatively low for low and medium threats, and is unlikely to reach above 0.5 even for a high threat. Although a small VBIED or IED can cause low casualties, the effect on physical damage can be much higher as although a VBIED may not totally destroy a building, the building will often need to be demolished and replaced.

Significant strengthening of a building is likely to reduce damage and fatality levels to near zero for low threat events; however, even a significantly strengthened structure can experience damage and casualties if the threat is high, such as a 1000 kg TNT VBIED at a stand-off of 2 m from a critical supporting column. It follows that risk reduction will reduce, perhaps marginally, as the size of the threat increases; see Table 1. Table 1 summarises the hypothetical threats, losses and risk reduction assumed for this example.

A typical multi-storey building for which occupancy and loss data are available is an academic building located at the US Naval Postgraduate School in Monterey, California [26]. The academic building is sizable, with offices and teaching space, and peak usage comprising $L_2 = 319$ building occupants. The replacement value of the building is $19.9 million (in 2007 dollars) and the value of the contents is $8.0 million. Demolition costs can be substantial, as can design and utilities re-installation costs — these costs are assumed as 25% of the replacement value of the building. Hence, the cost of physical damage is approximately $L_1 = \$33$ million. These costs could be inflated significantly if relocation costs, staff and student interruption costs, etc. are considered.

A literature review by Stewart [20] found that the minimum cost of protective measures (C_R) needed for substantial risk reduction for an existing building is at least 10% of building costs. As the remaining service life for existing buildings is normally less than 50 years, a remaining service life of 25 years is assumed. If the 10% increase in costs is annualised over 25 years with a discount rate of 4% then this equates to a present value cost of 0.64% per year. If the initial building cost is $19.9 million then the minimum annual cost of CT protective measures needed for substantial risk reduction is $C_R = 0.64\% \approx \$130{,}000$ pa.

It should be noted that Lakamp and McCarthy [26] estimated that the additional (post-9/11) costs of extra security personnel at the Naval Postgraduate School was $962,000 pa. Other CT measures were the closing of three access gates and the restriction of parking within 25 m of buildings. The opportunity cost of these CT measures is considerable:

(i) increased travel distance to gate (12.5 person years) = $1.1 million pa;
(ii) gate delays (19.2 person years) = $1.7 million pa;
(iii) extra walking time to building (3.3 person years) = $297,000 pa.

These opportunity costs total $3.1 million per year, which is considerably more than the direct cost of the CT measures themselves. If all these costs were to be included in the analysis then $C_R = \$130{,}000 + \$962{,}000 + \$3100{,}000 = \$4.2$ million.

The cost–benefit analysis parameters for the building CT protective measures are:

- $C_R = \$130{,}000$ per year;
- $L_1 = \$33$ million;

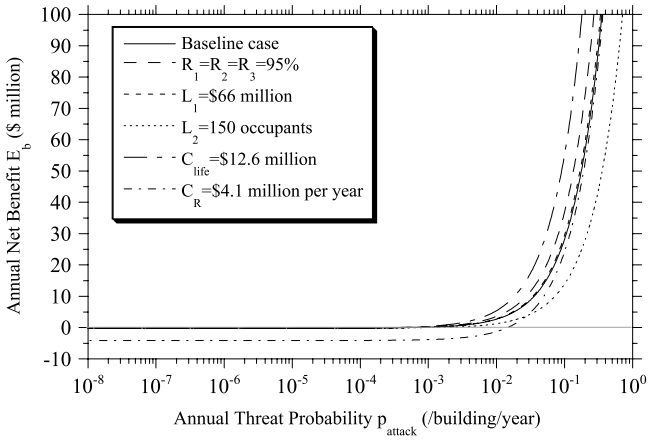


Fig. 2 – Annual net benefit (E_b) for commercial and institutional buildings.

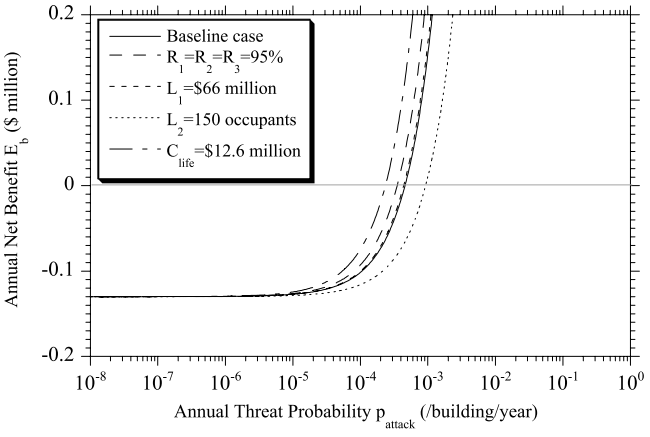


Fig. 3 – Detail of annual net benefit (E_b) for commercial and institutional buildings.

- $L_2 = 319$ occupants, $C_{life} = \$6.3$ million (VSL);
- $\Pr(\Theta_i|attack)$, $\Pr(L_1|\Theta_i)$, $\Pr(L_2|\Theta_i)$, R_i — see Table 1.

The expected number of fatalities is $\sum_{i=1}^{3} \Pr(L_2|\Theta_i)L_2 = 0.185 \times 319$ which in this case equals 59.0 fatalities. Fig. 2 shows the annual net benefit (E_b) calculated from Eq. (3) for the baseline case (see the above parameters). It is clear that when the threat probability is very high the net benefit can be hundreds of millions of dollars. Fig. 3 shows a detail of Fig. 2, focusing on the region where annual net benefit is near zero dollars. It is observed from Fig. 3 that protective measures for the (baseline case) building are cost-effective if the annual threat probability p_{attack} exceeds a threshold value of 4.5×10^{-4} per year.

Due to uncertainties inherent in such an analysis, a sensitivity analysis is essential — so analyses are conducted for:

(i) higher risk reduction for all threats ($R_1 = R_2 = R_3 = 95\%$);
(ii) cost of physical damage doubles ($L_1 = \$66$ million) or higher $\Pr(L_1|\Theta_i)$;
(iii) lower building occupancy (L_2=150 occupants) or lower $\Pr(L_2|\Theta_i)$ or lower VSL;
(iv) value of human life (VSL) doubles ($C_{life} = \$12.6$ million) or $\Pr(L_2|\Theta_i)$ doubles;
(v) perimeter security and opportunity costs ($C_R = \$4.1$ million).

If risk reduction for protective measures increases then net benefit increases, resulting in a slight decrease in threshold threat probability (3.5×10^{-4} per year). Doubling the cost of physical damage to $L_1 = \$66$ million (or increasing $\Pr(L_1|\Theta_i)$) has a negligible effect on net benefit, which illustrates that in this situation the expected losses are dominated by loss of life and not physical damage. Hence, if occupant numbers (or $\Pr(L_2|\Theta_i)$ or value of life) reduce then the benefits in terms of lives saved are reduced and a decrease in net benefit results in an increase in threshold threat probability (9.2×10^{-4}). However, if value of life doubles (or number of occupants doubles), then there is an increase in net benefit and so the threshold threat probability reduces to 2.2×10^{-4}. A higher cost of protective measures to $C_R = 4.1$ million pa means that net benefits decrease causing the threshold threat probability to increase substantially to 1.4×10^{-2} per year. In other words, the threat probability must be very high for protective measures to be cost-effective. If the expected benefit from CT protective measures not directly related to mitigating terrorist threats $E(C_B)$ is included then the threshold probability will reduce.

Ellingwood [44], Little [18] and Stewart [19] have suggested that p_{attack} for US commercial buildings is approximately 10^{-6} to 10^{-7}/building/year. Ellingwood [45] suggests that the minimum attack probability may increase to 10^{-4}/building/year for high density occupancies, key governmental and international institutions, monumental or iconic buildings or other critical facilities with a specific threat. It should be noted that although the probability of a terrorist attack in the US or elsewhere may be high, the probability that any particular item of infrastructure will be attacked is very low. If this analysis is to be used for real-world decision support, and if it is assumed that this analysis is representative of commercial and institutional buildings in general, then the analysis herein suggests that even the lowest threshold threat probability of 2.2×10^{-4}/building/year obtained from the above sensitivity analysis is still higher than the expected threat probabilities of 10^{-7} to 10^{-4}/building/year and so protective measures assumed herein appear not to be cost-effective. For example, for the baseline case and for a building with a specific threat ($p_{attack} = 10^{-4}$/building/year) then it can be shown that \$1 of cost yields \$0.22 in benefits. For a building subject to a non-specific threat ($p_{attack} = 10^{-6}$/building/year) then \$1 of cost yields only \$0.0022 in benefits.

A maximum expected net loss of \$130,000 per year ($E_b = -C_R$) may seem low for one building, and so an acceptable cost to the asset owner if he/she is risk averse and so may consider this to be a prudent investment in a time of threat uncertainty. However, if this level of risk aversion is repeated across a portfolio of buildings then the accumulated costs (and expected losses) will be significant. Such expenditure could be used more productively elsewhere.

3.2. *Highway bridges*

Also items of key infrastructure subject to terrorist threats are highway bridges (e.g., [46,47,10,25]). In this case, a single

threat scenario is considered; namely, a 1,800 kg TNT VBIED considered to be a practical threat using a light, single rear-axle delivery vehicle [48]. Two kinds of loss attributes are considered. As there is only one threat scenario then $\Pr(\Theta|attack) = 1.0$. The net benefit given in Eq. (1) is re-expressed for this example as

$$E_b = p_{attack}\frac{R}{100}\left[\Pr(L_1|\Theta)L_1 + \Pr(L_2|\Theta)(L_2 \times C_{life})\right] - C_R. \quad (4)$$

Islam and Yazdani [49] show that typical two-lane 24 m span Type III AASHTO girder bridges are very susceptible to extensive damage for explosive blast loading above or under a bridge even if the blast load is less than 226.98 kg TNT. Seible et al. [50] found in field trials that a 90.9 kg TNT explosive charge caused 'catastrophic damage' to a slab on girder bridge. It is assumed herein that a large VBIED would cause collapse of a typical highway bridge and so $\Pr(L_1|\Theta) = 1.0$. The probability of loss of life will be less than 1, as not all vehicle occupants on a collapsed bridge will be killed. For example, the I35W bridge collapse in Minneapolis in 2007 killed 13 people, but it is estimated that 100 vehicles were on the bridge at the time of collapse. The I40 Webbers Falls bridge collapse over the Arkansas River in 2002 killed 14 people after 11 vehicles plunged into the river [51]. To be sure, there were many more vehicles on the bridge that did not plunge into the river. However, an explosive blast may also damage vehicles and occupants, resulting in a higher fatality rate. In this case, it is assumed that $\Pr(L_2|\Theta) = 0.2$ and the number of people exposed to the hazard for a typical two-lane highway bridge is assumed as $L_2 = 80$. The expected number of fatalities is the product $\Pr(L_2|\Theta)L_2 = 0.2 \times 80$ which in this case equals 16 fatalities.

As highway bridges have a large variety of spans, widths, geometry, etc. it is not possible to generalise about damage costs. However, several case studies of recent US bridge collapses may be instructive. Bai and Burkett [51] found that the replacement and demolition costs for two US interstate highway bridges recently damaged were \$4 million and \$11.75 million. On the other hand, the replacement cost for bridges in Los Angeles varied from \$6.2 million to over \$60 million [52]. The replacement cost for the recently completed 10-lane, 14-span, 580 m long I35W bridge in Minneapolis was \$234 million [53]. In the present paper, a replacement cost for a typical bridge is taken as \$20 million. User delay costs for a bridge under construction can total \$430,000 per day, which even for a rapid bridge replacement for a failed bridge in Oklahoma of only 46 days' reconstruction will amount to nearly \$20 million [51]. If user delay costs are considered then $L_1 = \$40$ million.

While there is much information available about bridge retrofitting options for mitigating the effects of blast damage (e.g., [46,47,54]), there is very little information about their cost. A broad estimate, though, may be obtained from examining seismic retrofit costs as the scope of seismic retrofit works is not dissimiliar to that required to mitigate blast loading effects (e.g., [50]). Kuprenas et al. [52] reported that the seismic retrofit cost for the historic Cesar Chavez highway bridge in Los Angeles was 15% of its replacement value. However, Wang [55] found that a Class B "full blown" seismic rehabilitation of a US four-span steel girder bridge was 51.5% of its replacement value. Clearly, seismic retrofit costs can be substantial, and so blast-resistant retrofit costs would be similarly large. In the present case, it is conservatively assumed that substantial mitigation of blast load effects ($R = 90\%$) can be achieved at a cost of 20% of a bridge replacement value. If the bridge replacement value is \$20 million, remaining service life is 25 years, and the discount rate is 4% then this equates to $C_R = \$260{,}000$ pa.

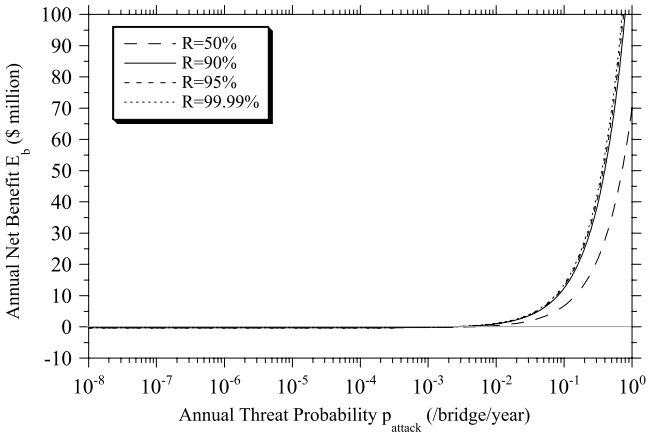


Fig. 4 – Annual net benefit (E_b) for highway bridges.

The cost–benefit analysis parameters for highway bridge CT protective measures are:

- $C_R = \$260{,}000$ per year;
- $L_1 = \$40$ million;
- $L_2 = 80$ vehicle occupants, $C_{life} = \$6.3$ million;
- $\Pr(L_1|\Theta) = 1.0$, $\Pr(L_2|\Theta) = 0.2$;
- $R = 90\%$.

Fig. 4 shows annual net benefit as a function of percentage risk reduction (R). There is little effect on net benefit when risk reduction exceeds 90%, where in these cases the annual threat probability must exceed 2.0×10^{-3}/bridge/year for bridge protective measures to be cost-effective. If risk reduction is reduced to only 50%, then the minimum annual threat probability increases to 3.6×10^{-3}/bridge/year for bridge protective measures to be cost-effective. A sensitivity analysis of parameters is recommended, but the trends would not be dissimilar to those presented for buildings as described previously.

As discussed earlier, Eq. (2) shows that if life safety is the main criterion for risk acceptability, then cost per life saved may be a useful measure of cost-effectiveness. In this case, Eq. (3) is re-expressed as

$$CER = \frac{C_R}{p_{attack}\frac{R}{100}\Pr(L_2|\Theta)L_2}. \quad (5)$$

Using Eq. (5), Fig. 5 shows annual cost per life saved as a function of annual threat probability. In nearly all cases the annual cost per life saved is well above the accepted value of \$6.3 million per life saved. If the annual threat probability is below 10^{-4}/bridge/year then the cost per life saved exceeds \$180.6 million and so would fail a cost–benefit assessment.

While there are numerous instances of buildings being attacked by terrorists, there are very few reported attacks on

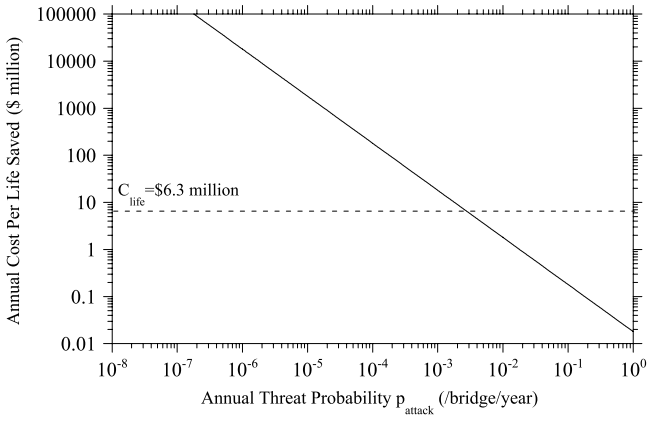


Fig. 5 – Annual cost per life saved for highway bridges.

bridges. To be sure, some bridges have been the target of terrorist activity in Iraq and Afghanistan, but these are war zone situations where bridges are an attractive tactical target for insurgents (or terrorists). An analysis of terrorism incidents compiled by the Memorial Institute for the Prevention of Terrorism (MIPT — see www.mipt.org) shows that of the 13 bridges attacked by insurgents in Iraq and Afghanistan the total number of fatalities was relatively few at 22 — thus while bridges may be an attractive tactical target, the evidence suggests that terrorist attacks on typical highway bridges will not cause significant casualties. The MIPT database of terrorism incidents shows only three attacks on bridges in the UK (all IRA sponsored; minor damage, no fatalities), and none in continental Europe or North America. Moreover, Jenkins and Gersten [56] report that only 5% of 'guerrilla and terrorist attacks' on public surface transportation systems in the period 1920–2000 were directed as bridges and tunnels, and this figures reduces to only 1% for the period July 1997 to December 2000.

It follows that the likelihood of a terrorist attack on a typical highway or railway bridge in the United States, Europe, Australia and other western nations is very remote as incident data suggests that bridges are simply not an 'attractive' target for terrorists. Hence, the annual threat probability is likely to be less than 1×10^{-4}/bridge/year and so bridge protective measures not cost-effective. If there is a specific threat or if a bridge is deemed an iconic structure (such as a bridge classified as a 'key resource') then bridge protective measures may be cost-effective.

3.3. *Hardening of cockpit doors*

After 9/11 the Federal Aviation Administration (FAA) required operators of more than 6000 planes to install hardened cockpit doors in order to protect cockpits from intrusion and small-arms fire or fragmentation devices. While this appears to be an effective initiative, it is not clear whether the amount of structural hardening is sufficient or whether other security measures, such as a secondary barrier, could further enhance security in a cost-effective manner. In this case study the focus is on the costs and benefits of hardening cockpit doors that seek to prevent a duplication of 9/11 in which a commercial passenger aircraft is commandeered, kept under control for some time, and then crashed into a specific target.

The purchase and installation cost of each hardened cockpit door is typically $30,000 to $50,000. The annual cost to airlines is estimated as $30–$50 million, including the cost of increased fuel consumption due to the heavier doors [57]. A best estimate annual cost of hardening cockpit doors is C_R = $40 million pa.

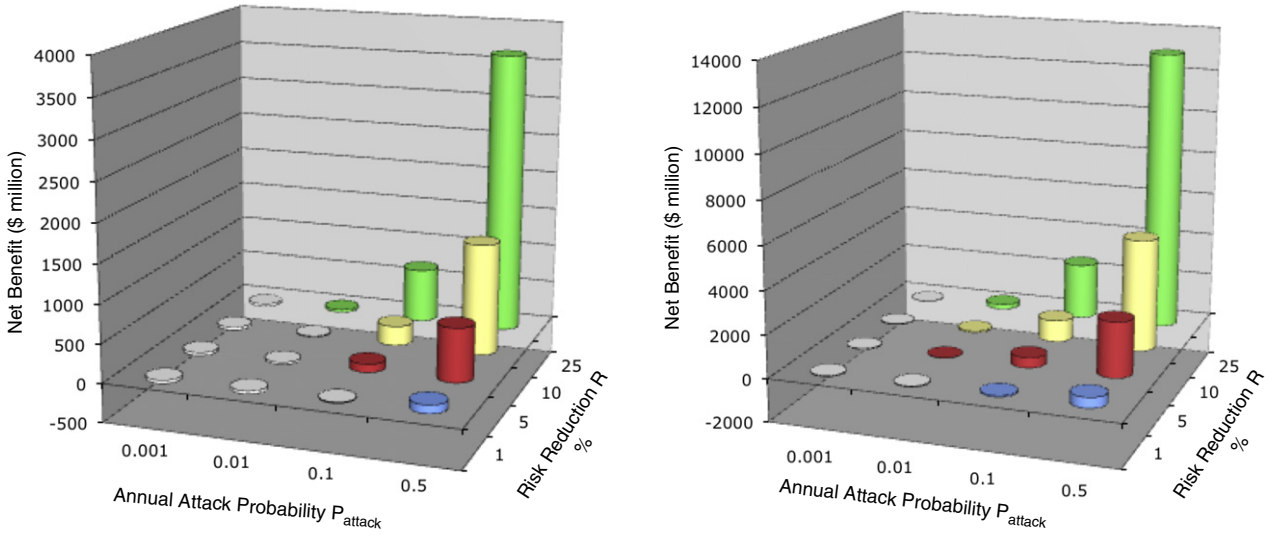
Estimates suggest that the direct physical damage and clean-up costs caused by the 9/11 attacks amounted to approximately $25 billion (including damage to the Pentagon and loss of aircraft) [58], and Dixon and Stern [59] estimate that the direct losses and losses to business in New York city totalled $37.4 billion. As we are considering damage due to a single hijacking, then L_1 = $20 billion and $\Pr(L_1|\Theta) = 1.0$ seem appropriate, albeit upper-bound, estimates. The number of fatalities from the 9/11 attacks to a single tower of the World Trade Centre was approximately 1500 fatalities. If the number of people exposed to this hazard (building occupants, passengers, pedestrians, emergency workers) is assumed at L_2 = 25,000, then $\Pr(L_2|\Theta) = 0.06$, so the expected number of fatalities is 1500.

The cost–benefit analysis parameters for hardened cockpit doors are:

- C_R = $40 million per year;
- L_1 = $20 billion;
- L_2 = 25,000, C_{life} = $6.3 million;
- $\Pr(L_1|\Theta) = 1.0$, $\Pr(L_2|\Theta) = 0.06$.

In this case the total losses $C_{loss} = \Pr(L_1|\Theta)L_1 + \Pr(L_2|\Theta)L_2C_{life}$ = $29.45 billion. Using Eq. (4), Fig. 6(a) shows annual net benefit (E_b) as a function of risk reduction (R) and annual threat probability (p_{attack}). If risk reduction exceeds 1% then the minimum (threshold) threat probability is approximately 0.1 per year for hardened cockpit doors to be viewed as cost-effective. If the threat probability is higher than 0.1 per year then the lower bound of risk reduction is less than 1%. If the threat probability is less than 0.1 then the benefits of hardened cockpit doors reduce and so their effectiveness (R) has to increase for hardened cockpit doors to be viewed as cost-effective. Yet even if the threat probability is 0.01 per year, then Eq. (4) shows that the lower bound of risk reduction is approximately 13.6%. Since security experts believe that strengthening cockpit doors is one of the few security measures post-9/11 to be effective [33] then it is highly likely that the risk reduction achieved by the hardening of cockpit doors is well in excess of 1%, and is more likely to be 10%–25% [28]. Hence, if the threat probability is believed to be greater than 0.01 then under this analysis hardening cockpit doors appears to be a cost-effective CT protective measure.

The International Monetary Fund (IMF) estimates that the 9/11 attacks cost the US economy up to $75 billion in lost GDP in that year alone, and others estimate that associated business costs and loss of tourism cost the US economy a further $160 billion over three years [60]. If we now assume an additional (indirect) loss of $75 billion then L_1 = $95 billion and so C_{loss} = $104.45 billion. Fig. 6(b) shows annual net benefit (E_b) as a function of risk reduction (R) and annual threat probability (p_{attack}). As expected, net benefit increases considerably, which makes hardening cockpit doors even more cost-effective.



(a) Net benefit (C_{loss} = $29.45 billion). **(b) Net benefit (C_{loss} = $104.45 billion).**

Fig. 6 – Annual net benefit (E_b) for hardened cockpit doors: (a) C_{loss} = $29.45 billion and (b) C_{loss} = $104.45 billion.

3.4. *Discussion*

The example illustrations assumed a single terrorist attack. In principle, threat scenarios assuming multiple terrorist attacks can also be included in the cost–benefit calculations. It is likely that the threat probability and risk reduction would be reduced as in many cases it would be increasingly difficult for terrorists to successfully coordinate multiple attacks, and equally as likely, for CT measures to deter or foil a multiple attack. The losses would clearly increase.

Many uncertainties exist in quantifying risks, particularly for threats such as terrorism. Cost–benefit outcomes will be most sensitive to threat probability and risk reduction arising from CT protective measures. Hence, we need to rely on judgment and scenario analyses, and so it is essential that any cost–benefit analysis be subject to a sensitivity analysis. While the present analysis uses single-point estimates for parameter values, in principle, the parameters could be represented by random (or correlated) variables that could explicitly consider aleatory and epistemic uncertainties if such data were available.

While it is well established that terrorism is a threat from an intelligent adversary who will adapt to changing circumstances, it is not so clear how this might affect threat probability in a dynamic environment. Moreover, evidence suggests that some, maybe many, terrorist attacks are opportunistic in nature (e.g., 2007 Glasgow international airport attack), and so should be modelled as essentially a random process [61]. This is particularly appropriate for items of infrastructure where there are no specific threats and the 'targets' are numerous which is the case with most buildings and bridges. There is also the issue of risk transfer, where hardening of one item of infrastructure may encourage terrorists to attack a 'softer' target and so there may be no change in overall threat probability or consequences as a result of hardening this one item of infrastructure. These are issues with no clear outcome, but need to be considered when assessing threat probability, undertaking sensitivity analyses and deciding how such uncertainty might affect the outcome of a cost–benefit assessment.

In addition to the benefits of quantifying costs and benefits for decision support, the process of undertaking a cost–benefit assessment, in a structured and methodical manner, will lead to a better understanding of the CT protective measures and their interactions with other security systems and the wider environment. In other words, a risk assessment gives a better appreciation of how one or more CT protective measures fit within the overall 'system'. This can often lead to new insights into the performance of CT protective measures, as well as inefficiencies.

To be sure, a number of other metrics can be used to assess and compare costs and benefits and the methods described herein provide one relatively straightforward approach, that over time, can be refined and improved to allow for more meaningful decision support about the acceptability of existing risks and the cost-effectiveness of risk mitigation strategies for the protection of infrastructure against terrorist threats. While quantitative decision support tools hold some appeal to decision makers, they cannot capture the full and diverse range of societal considerations of risk acceptability. Hence, the results of the present paper should be viewed only as an aid to decision support, where decisions about public safety will often require social, economic, cultural, environmental, political and other considerations.

4. Protecting critical infrastructure and key resources

There is no doubt that a terrorist attack on an item of infrastructure could cause significant loss of life and devastating damage. However, while highways, pipelines, mass transit, water supply, communications and other infrastructure may be essential to the economy and well-being of society, with

very few exceptions, damage to one or even several individual items of infrastructure will not be 'critical' to the economy, to the state or to our way of life. For example, if several bridges were attacked the effects at a local level may be highly disruptive, but not at a national level. Infrastructure designers and operators place much effort on systems modelling to ensure that 'failure' of one node in an infrastructure network will still enable the network to operate, though at reduced efficiency. This is done routinely; for example, many bridges need to be closed from time to time for maintenance or repair and so asset owners need to be able to redirect traffic so that the traffic network is not interrupted. Other 'failures' that infrastructure designers and operators routinely plan for that could restrict the operation of infrastructure include traffic accidents, severe weather, earthquakes, equipment malfunctions, etc. In other words, as a matter of course infrastructure is designed with 'inbuilt' redundancies and backup systems to ensure resilience in the event of anticipated or unexpected hazards.

The results of the cost–benefit assessment suggest that many individual items of infrastructure (particularly bridges and buildings) require no protective measures as they cannot be classified as 'critical' to society. So while 'critical infrastructure protection' is a worthy goal, many individual items of infrastructure are likely to be not 'critical' to the nation or the economy.

However, there may be some 'key resources' – defined by the US government as 'publicly or privately controlled resources essential to the minimal operations of the economy or government' [6] – that might warrant protective measures. This might include, for example, monuments and iconic structures such as the Golden Gate Bridge, Empire State Building, Brooklyn Bridge, Washington Monument, etc. as well as nuclear power plants, dams and government facilities. The protection of 'key resources' should also be subject to rigorous cost and benefit assessments as many thousands of individual assets would meet the definition of 'key resources' and a need still exists for optimal resource allocation for their protection.

5. Conclusions

A cost–benefit assessment needs to consider risk reduction, threat probability, and fatality and damage cost estimates. Three illustrative examples showed under what combination of risk reduction, threat probability, and fatality and damage costs the CT protective measures would be cost-effective for buildings, bridges and aviation infrastructure. It was found that unless terrorist threat probabilities are high, then typical CT protective measures are not cost-effective. Opportunity costs associated can be considerable which makes CT protective measures even less cost-effective. It was found that if a higher value of life or other losses (such as business interruption, loss of GDP, etc.) are considered then CT protective measures become more cost-effective even if the terrorist threat probability is not high. With the exception of 'key resources', many individual items of infrastructure are likely to be not 'critical' to the nation or the economy and so not cost-effective to protect against terrorism. The benefits of quantifying costs and benefits of CT protective measures for decision support also include the ability to reveal inefficiencies and suggest where resources may be better allocated to maximise public safety.

Acknowledgements

The support of the Australian Research Council under grant DP0878347 is gratefully acknowledged. The helpful discussions with Professor John Mueller from Ohio State University are much appreciated.

REFERENCES

[1] USG, Analytical Perspectives, Budget of the United States Government, Fiscal Year 2008, Office of Management and Budget, Washington, DC, 2008.
[2] NC, The 9/11 Commission Report, National Commission on Terrorist Attacks Upon the United States, July 22, 2004.
[3] ASCE, Protecting Infrastructure, in: Civil Engineering Research Foundation Monograph Series, American Society of Civil Engineers, New York, 2001.
[4] IEAust, Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment, Institution of Engineers, Canberra, Australia, 2003.
[5] AS/NZS 4360, Risk Management, Standards Australia, Strathfield, NSW, 2004.
[6] DHS, National Infrastructure Protection Plan, Department of Homeland Security, Washington, DC, 2009.
[7] B.J. Garrick, J.E. Hall, M. Kilger, et al., Confronting the risks of terrorism: Making the right decisions, Reliability Engineering and System Safety 86 (2004) 129–176.
[8] FEMA 452, Risk assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, Risk Management Series, Federal Emergency Management Agency, Report FEMA 452, US, 2005.
[9] NISTIR-7349, Users Manual for Version 2.0 of the Cost-Effectiveness Tool for Capital Asset Protection, US Department of Commerce, Technology Administration, National Institute of Standards and Technology. Office of Applied Economics, Building and Fire Research Laboratory, Gaithersburg, MD, 2006.
[10] J.C. Ray, Risk-based prioritization of terrorist threat mitigation measures on bridges, Journal of Bridge Engineering, ASCE 12 (2) (2007) 140–146.
[11] L.A. Twisdale, R.H. Sues, F.M. Lavelle, Reliability-based design methods for protective structures, Structural Safety 15 (1–2) (1994) 17–33.
[12] H.Y. Low, H. Hao, Reliability analysis of direct shear and flexural failure modes of RC slabs under explosive loading, Engineering Structure 24 (2) (2002) 189–198.
[13] M.G. Stewart, M.D. Netherton, D.V. Rosowsky, Terrorism risks and blast damage to built infrastructure, Natural Hazards Review 7 (3) (2006) 114–122.
[14] M.G. Stewart, M.D. Netherton, Security risks and probabilistic risk assessment of glazing subject to explosive blast loading, Reliability Engineering and System Safety 93 (4) (2008) 627–638.
[15] E. Eamon, Reliability of concrete masonry unit walls subjected to explosive loads, Journal of the Structural Engineering, ASCE 133 (7) (2007) 935–944.
[16] R.L. Dillon, R. Liebe, T. Bestafka, Risk-based decision making for terrorism applications, Risk Analysis 29 (3) (2009) 321–335.
[17] L.A. Cox, Improving risk-based decision-making for terrorism applications, Risk Analysis 29 (3) (2009) 336–341.

[18] R.G. Little, Cost-effective strategies to address urban terrorism: A risk management approach, in: H.W. Richardson, P. Gordon, J.E. Moore (Eds.), The Economic Costs and Consequences of Terrorism, Edward Elgar Publishing, Cheltenham, UK, 2007, pp. 98–115.
[19] M.G. Stewart, Cost-effectiveness of risk mitigation strategies for protection of buildings against terrorist attack, Journal of Performance of Constructed Facilities, ASCE 22 (2) (2008) 115–120.
[20] M.G. Stewart, Life safety risks and optimisation of protective measures against terrorist threats to infrastructure, Structure and Infrastructure Engineering (2010) (in press) (Available online http://dx.doi.org/10.1080/15732470902726023).
[21] H.H. Willis, T. LaTourrette, T.K. Kelly, S. Hickey, S. Neill, Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection, RAND Corporation, Santa Monica, CA, 2007.
[22] M.G. Stewart, R.E. Melchers, Probabilistic Risk Assessment of Engineering Systems, Chapman & Hall, London, 1997.
[23] E. Paté-Cornell, S. Guikema, Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among counter-measures, Military Operations Research 7 (4) (2002) 5–23.
[24] DHS, Department of Homeland Security Bioterrorism Risk Assessment: A Call For Change, The National Academies Press, Washington, DC, 2008.
[25] GAO, Highway Infrastructure: Federal Efforts to Strengthen Security Should be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure, United States Government Accountability Office, Washington, DC, January 2009.
[26] D.J. Lakamp, G.H. McCarthy, A Cost–Benefit Analysis of Security at the Naval Postgraduate School, MBA Professional Report, Naval Postgraduate School, Monterey, California, 2003.
[27] M.G. Stewart, J. Mueller, A cost–benefit and risk assessment of Australian aviation security measures, Security Challenges 4 (3) (2008) 45–61.
[28] M.G. Stewart, J. Mueller, A risk and cost–benefit and assessment of US aviation security measures, Journal of Transportation Security 1 (3) (2008) 143–159.
[29] B.E. Biringer, R.V. Matalucci, S.L. O'Connor, Security Risk Assessment and Management, Wiley, New Jersey, 2007.
[30] M.E. Paté-Cornell, Quantitative safety goals for risk management of industrial facilities, Structural Safety 13 (1994) 145–157.
[31] S.G. Reid, Acceptable risk criteria, Progress in Structural Engineering and Materials 2 (2000) 254–262.
[32] R.E. Melchers, On the ALARP approach to risk management, Reliability Engineering and System Safety 71 (2001) 201–208.
[33] B. Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World, Copernicus, New York, 2006.
[34] S.E. Martonosi, A. Barnett, How effective is security screening of aircraft passengers, Interfaces 36 (6) (2006) 545–552.
[35] M.D. Netherton, M.G. Stewart, Probabilistic modelling of safety and damage blast risks for window glazing, Canadian Journal of Civil Engineering 36 (8) (2009) 1321–1331.
[36] W.K. Viscusi, The value of life in legal contexts: Survey and critique, American Law and Economic Review 2 (1) (2000) 195–222.
[37] L.A. Robinson, Valuing Mortality Risk Reductions in Homeland Security Regulatory Analyses, Final Report, US Customs and Border Protection, Department of Homeland Security, June 2008.
[38] P. Slovic, The Perception of Risk, Earthscan Publications, London, 2000.
[39] M. Faber, M.G. Stewart, Risk assessment for civil engineering facilities: Critical overview and discussion, Reliability Engineering and System Safety 80 (2) (2003) 173–184.
[40] I. Jordaan, Decisions Under Uncertainty: Probabilistic Analysis for Engineering Decisions, Cambridge University Press, Cambridge, UK, 2005.
[41] B. Zycher, A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures, RAND, Santa Monica, 2003.
[42] W. Edwards, R.F. Miles, D. von Winterfeldt, Advances in Decision Analysis, Cambridge University Press, Cambridge, UK, 2007.
[43] G. Bammer, M. Smithson, Uncertainty and Risk: Multidisciplinary Perspectives, Earthscan Publications, London, UK, 2008.
[44] B.R. Ellingwood, Strategies for mitigating risk to buildings from abnormal load events, International Journal of Risk Assessment and Management 7 (6/7) (2007) 828–845.
[45] B.R. Ellingwood, Mitigating risk from abnormal loads and progressive collapse, Journal of Performance of Constructed Facilities, ASCE 20 (4) (2006) 315–323.
[46] FHWA, Recommendations for Bridge and Tunnel Security, Blue Ribbon Panel on Bridge and Tunnel Security, Federal Highway Administration, September 2003.
[47] E.B. Williamson, D.G. Winget, Risk management and design of critical bridges for terrorist attack, Journal of Bridge Engineering, ASCE 10 (1) (2005) 96–106.
[48] E.J. Conrath, T. Krauthammer, K.A. Marchand, P.F. Mlakar, Structural Design for Physical Security: State of the Practice, ASCE, Reston, 1999.
[49] A.K.M.A. Islam, N. Yazdani, Blast capacity and protection of AASHTO bridge girders, in: Proceedings of the 2006 Structures Congress, ASCE, CD-ROM, 2006.
[50] F. Seible, G. Hegemier, V.M. Karbhari, J. Wolfson, et al., Protection of our bridge infrastructure against man-made and natural hazards, Structure and Infrastructure Engineering 4 (6) (2008) 415–429.
[51] Y. Bai, W.R. Burkett, Rapid bridge replacement: Processes, techniques, and needs for improvements, Journal of Construction Engineering and Management, ASCE 132 (11) (2006) 1139–1147.
[52] J.A. Kuprenas, F. Madjidi, A. Vidaurrazaga, C.L. Lim, Seismic retrofit program for Los Angeles bridges, Journal of Infrastructure Systems, ASCE 4 (4) (1998) 185–191.
[53] J. Foti, 35W bridge on pace to open in Sept., Star Tribune, 4 May 2008.
[54] E.B. Williamson, K.A. Marchand, Recommendations for blast-resistant design and retrofit of typical Highway Bridges, in: Proceedings of the 2006 Structures Congress, ASCE, CD-ROM, 2006.
[55] E. Wang, Optimizing bridge seismic retrofit strategy implementing bridge fragility curves, in: Proceedings of the 2006 Structures Congress, ASCE, CD-ROM, 2006.
[56] B.M. Jenkins, L.N. Gersten, Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices, Mineta Transportation Institute, San José State University, MTI Report 01-07, September 2001.
[57] FAA, Airlines Meet FAA's Hardened Cockpit Door Deadline, Federal Aviation Administration Office of Public Affairs Press Release, April 2003.
[58] J. Bram, J. Orr, C. Rapaport, Measuring the effects of the September 11 attack on New York city, FRBNY Economic Policy Review (November) (2002) 5–20.
[59] L. Dixon, R.K. Stern, Compensation for Losses From The 9/11 Attacks, RAND Institute for Civil Justice, RAND Corporation, Santa Monica, CA, 2004.
[60] C. Ungerer, H. Ergas, S. Hook, M.G. Stewart, Risky Business: Measuring the Costs and Benefits of Counter-Terrorism Spending, Special Report — Issue 18, Australian Strategic Policy Institute, Canberra, November 2008.
[61] J. Mueller, Establishing Principles for evaluating measures Designed to Protect The Homeland From Terrorism, National Convention of the International Studies Association, New York, NY, February 15–18, 2009.