Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Critical Infrastructure Protection

Mark G Stewart
Australian Research Council Professorial Fellow
Centre for Infrastructure Performance and Reliability
The University of Newcastle, Australia
email: mark.stewart@newcastle.edu.au

John Mueller
Mershon Center for International Security Studies, Ohio State University
Cato Senior Fellow, Cato Institute, Washington, DC
email: bbbb@osu.edu

Abstract: The loading and response of structures to explosive blast loading is subject to uncertainty and variability. This uncertainty can be caused by variability of dimensions and material properties, model errors, environment, etc. Limit state and LRFD design codes for reinforced concrete and steel have been derived from probabilistic and structural reliability methods to ensure that new and existing structures satisfy an acceptable level of risk. These techniques can be applied to the area of structural response of structures subject to explosive blast loading. The use of decision theory to determine acceptability of risk is crucial to prioritise protective measures for built infrastructure. Government spending on homeland security will reach $141.6 billion worldwide in 2009 and is projected to reach $300 billion by 2016. The question is, is this or other expenditure necessary? Clearly, scientific rigour is needed when assessing the effectiveness and the need for protective measures to ensure that their benefits exceed the cost. The paper will assess terrorist threats to buildings and airport infrastructure and the cost-effectiveness of protective and counter-terrorism measures. Structural reliability and probabilistic methods are used to assess risk reduction due to protective measures. The key innovation is incorporating uncertainty modelling in the decision analysis, which in this case will maximise net benefit. This analysis will then consider threat likelihood, cost of security measures, risk reduction and expected losses to compare the costs and benefits of security measures to decide which security measures are cost-effective, and those which are not.

Keywords: risk, reliability, terrorism, security, cost-benefit analysis, infrastructure, aviation

1. Introduction

Terrorist threats against civilian and military infrastructure, particularly buildings, bridges, pipelines and aviation infrastructure, seem to be increasing, as evidenced by recent terrorist attacks including Manchester and London city centres (1992, 1993 and 1996), U.S. Embassy in Kenya (1998), Pentagon and World Trade Center (2001), night clubs and restaurants in Bali (2002, 2005), Marriott Hotel in Jakarta (2003), Australian Embassy in Indonesia (2004), and 'near misses' such as the recent Christmas Day Northwest Airlines

5th International Conference on Reliable Engineering Computing (REC 2012)
Edited by M. Vořechovský, V. Sadílek, S. Seitl, V. Veselý, R. L. Muhanna and R. L. Mullen

ISBN 978-80-214-4507-9. Published by Ing. Vladislav Pokorný − LITERA

aircraft suicide bombing attempt (2009). The preferred method of attack is Improvised Explosive Devices (IEDs), often through suicide tactics, against buildings and transport infrastructure, see Figure 1.

Figure 1. VBIED Damage to Building in Jakarta (2004) and Bridge in Iraq (2009).

Securing airports and aircraft has been a high priority of governments world-wide after the 9/11 attacks. Several terrorist plots have recently been foiled, which if successful, would have killed many hundreds of people. The U.S. Transportation Security Administration (TSA) has arrayed '21 Layers of Security' to 'strengthen security through a layered approach'. This is similar to counter-terrorism (CT) strategies worldwide. Assessing the effectiveness and reliability of aviation CT measures is important to understanding their strengths and weaknesses, and assessing the need for additional security measures.

There are considerable uncertainties associated with threat scenarios, system response, effectiveness of CT measures and expected damage. Since IEDs are typically 'home made' and placed under imperfect conditions, then the probability of a successful detonation can be highly uncertain, as evidenced in recent failed attempts to blow up U.S. airliners. These uncertainties will affect damage risk predictions and the utility of subsequent decisions. Characterising these uncertainties using stochastic (probabilistic) methods is a logical step, which will lead to estimates of system reliability and risk. Only very few probabilistic and reliability analyses have been carried out for infrastructure systems subject to explosive blast loading (e.g. Twisdale 1994, Low and Hao 2001, 2002, Eamon 2007, Hao et al 2010). This is in contrast to the approach that has been used very widely and successfully for other man-made and natural hazards (e.g. Stewart and Melchers 1997). Risk and reliability analyses will allow comparisons to be made between the relative effectiveness of security measures, weapon selection, delivery method or other mitigation measures.

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

The cumulative increase in expenditures on U.S. domestic homeland security over the decade since 9/11 exceeds one trillion dollars (Mueller and Stewart 2011a,b). Up to 45% of this expenditure is devoted to protecting critical infrastructure and key resources. Yet there is little evidence that such expenditures have

been efficient. Clearly, for efficient decision-support to occur there is a need to quantify security risks and assess their level of acceptability and cost-effectiveness. A significant challenge is balancing the costs and benefits of counter-terrorism measures when the threat scenarios are highly transient and considerable risk averseness displayed by decision makers. For security and public policy purposes a quantification of security risks is essential for risk acceptability and robust decision-making.

It was understandable, in the years immediately following the terrorist attacks of September 11, 2001 that there was a tendency to spend in haste on homeland security. For example, annual security costs for the U.S. airline industry have increased to over $8 billion (DHS 2011), yet little scientific rigour has been applied to assess the effectiveness of this expenditure as evidenced by a statement from the U.S. Department of Homeland Security that 'We really don't know a whole lot about the overall costs and benefits of homeland security.' (Anderson 2006). These concerns are equally valid for Australia, Canada and Europe. There is a need to examine homeland security expenditures in a careful and systematic way, applying the kind of system and reliability modelling approaches that are routinely applied to other hazards. This type of rigour, where security and public policy decisions are assessed on technical, social and economic considerations of risk acceptability, is much needed to ensure that public funds are expended on measures that maximise public safety.

Terrorism may be viewed as a 'new hazard', that although different in nature from other hazards, requires systems and reliability approaches similar to those adopted to other hazards to assess risk and safety. The paper will review recent research conducted at The University of Newcastle, including:

1. Stochastic modelling of blast loads
2. Stochastic modelling of structural response
3. Systems and Reliability analysis
4. Risk-based decision theory

This is a multi-faceted approach to probabilistic terrorism risk assessment that deals with existing and new (hardened) infrastructure. A capability to predict the likelihood and extent of damage and casualty levels has many potential uses; including:

1. infrastructure and security policy, as a decision support tool to mitigate damage
2. contingency planning and emergency response simulations
3. collateral damage estimation (CDE) for military planners
4. forensics to back-calculate charge weights.

A review of probabilistic risk assessments are given for specific example applications: (i) IED design and initiation, and predicting variability of time-pressure load history on infrastructure, (ii) reinforced concrete structural systems, (iii) airports subject to terrorist attack, and (iv) buildings subject to a terrorist Vehicle Borne Improvised Explosive Device (VBIED). The illustrative examples in this paper, where possible, use actual or representative threat, consequence and cost data. However, some hypothetical data is used (particularly when dealing with terrorist threats in Section 5) as the intention of the examples is to show the methodology of various risk acceptance criteria and not to make any definitive conclusions about a specific item of infrastructure.

For additional and wider-ranging assessments of the issues raised and the approaches used, including risk and cost-benefit assessments of buildings, bridges and aviation systems (air marshals, full-body scanners, etc.), see John Mueller and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*, Oxford University Press, 2011.

2. Risk-Based Decision Support Framework

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

$$E_b = E\left(C_B\right) + \sum_T \sum_H \sum_L Pr(T)\, Pr\left(H|T\right) Pr\left(L|H\right) \bullet L \bullet \Delta R - C_{security} \tag{1}$$

where $E(C_B)$ is the expected benefit from the security measure not directly related to mitigating terrorist threats (e.g. increased consumer confidence, reduction in crime), $Pr(T)$ is the annual threat probability per item of infrastructure, $Pr(H|T)$ is the conditional probability of a hazard (successful initiation/detonation of an IED, or other initiating event leading to damage and loss of life) given occurrence of the threat, $Pr(L|H)$ is the conditional probability of a loss given occurrence of the hazard, L is the loss or consequence (i.e., damage costs, number of people exposed to the hazard), ΔR is the reduction in risk due to CT measures, and $C_{security}$ is the extra cost of CT protective measures including opportunity costs. The product $Pr(L|H)L$ refers to the expected loss given the occurrence of the hazard. The summation signs in Eqn. (1) refer to the number of possible threat scenarios, hazard levels and losses. A protective measure is viewed as cost-effective or efficient if the net benefit exceeds zero (OBPR 2010). There are many risk acceptance criteria and these depend on the type of risk being quantified (life safety, economic, environmental, social), the preferences of the interested parties and the decision maker, and the quality of the information available. Risk acceptance criteria based on annual fatality risk or failure probability may also be used (e.g. Stewart 2010a,b, 2011).

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

Equation (1) can be generalised for any time period, discounting of future costs and more detailed time-dependent cost and damage consequences. Fatality risks can be computed as the product $Pr(T)Pr(H|T)Pr(L|T)$ which can be compared with appropriate societal risk acceptance criteria (Stewart and Melchers 1997). Security cost data are available from the literature and security practitioners. This is not so for losses, although indicative values for damages due to terrorist attacks in the UK, US and elsewhere are available from the literature (Mueller and Stewart 2011a).

It is very difficult to estimate the threat probability $Pr(T)$. Progress in quantifying $Pr(T)$ will need contributions from security analysts and other academic disciplines. If information about $Pr(T)$ is believed to be too unreliable, then the decision analysis can be used to calculate the minimum (threshold) threat probability for CT protective measures to be cost-effective (i.e., a break-even approach). It is then 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. Moreover, a decision analysis based on scenario analysis where threat probability is decoupled from Eqn. (1) provides an alternative decision-making criteria based on expected costs. The challenging aspect of risk-based decision theory is predicting values of $Pr(H|T)$, $Pr(L|H)$ and ΔR. This information may be inferred from expert opinions, scenario analysis, and statistical analysis of prior performance data, as well as system and reliability modelling. Since there is uncertainty associated with such predictions, the use of probability distributions to describe mean, variance and distribution type is recommended. However, it is recognised that data or models are often incomplete for such low probability − high consequence events, and so a sensitivity analysis should always be conducted to assess the robustness of results to parameter and modelling uncertainty.

We recognise that Eqn. (1) is an overly simplification, however, it is a useful starting point for further discussion and perhaps for more detailed and complex analysis of how to manage the often conflicting societal preferences associated with assessments of risk, cost, and benefits. Clearly, risk and cost-benefit considerations should not be the sole criterion for public decision making. Nonetheless, they provide important insights into how security measures may (or may not) perform, their effect on risk reduction, and their cost-effectiveness. They can reveal wasteful expenditures and allow limited funds to be directed to where the most benefit can be attained. More important, if risk and cost-benefit advice is to be ignored, the onus is on public officials to explain why this is so, and the trade-offs and cuts to other programs that will inevitably ensue.

3. Probabilistic Blast Load Modelling

3.1. RELIABILITY OF IMPROVISED EXPLOSIVE DEVICES (IED)

Unlike conventional military hardware, the reliability of IEDs cannot be calculated through standard philosophies such as those identified at MIL-HDBK-217 (Department of Defense 1995). Much of this is because IEDs have not been designed, manufactured and utilised in accordance with standard systems engineering practices by competent personnel, nor necessarily have they been developed by personnel familiar with operations or with military training.

The threat of IED attack, and hence development of a probabilistic risk assessment, can be treated through a systems model, using an alternate paradigm to conventional munitions reliability. The components that make up the IED can be assessed as per traditional reliability methodologies, however, the effects of design, environment, manufacturing and operational considerations need to be independently considered and overlaid as performance shaping functions (PSFs) that introduce additional variability in traditional reliability functions.

A reliability function can then be used to identify what could be considered the reliability for an IED design and manufacture – that is, the reliability of the IED due to the selection of components, their format and the intended operating environment. A baseline reliability function adapted from Wolstenholme (1999) is employed to develop the baseline reliability of the IED (R) where the IED is modelled as a series system of n components:

$$R = \prod_{c=1}^{n} [\alpha_c - \lambda_s t_s] \tag{2}$$

where λ_s is the IED component storage failure rate, t_s is the time the IED component was in storage, α_c is the reliability of each IED component, and n is the number of components.

This paper uses several typical IED configurations of differing design complexities – simple (pipe bomb), medium (mobile phone initiated VBIED) and complex (improvised mortar). An example calculation for a medium complexity device, a mobile phone initiated VBIED (noting that most components are not disclosed for security reasons), derived from representative Operational Level Reliabilities for munitions systems data from Australia, U.K. and the U.S., and representative mobile phone data, to inform component reliabilities, is

$$R = 0.9994 \times 0.999 \times 0.98 \times 0.97 \times 0.97 \times 0.999 = 0.920 \tag{3}$$

Table I provides a summary of baseline IED reliabilities derived from conventional munitions' representative component reliability data for common IED designs (Grant and Stewart 2011). The baseline reliability assumes there are no errors in connecting components, and assumes statistical independence of component reliabilities. Hence, R reflects the reliability of an IED designed and manufactured to military specifications and standards.

Table I. Typical IED Baseline Reliability Estimates for Device Complexity

Device Complexity	Representative IED Design	Baseline Reliability R
Simple	Pipe Bomb	0.931
Medium	Mobile Phone initiated VBIED	0.920
Complex	Improvised Mortar	0.910

The probability of IED initiation is $Pr(H|T)$ where H is IED initiation(hazard) and T is the threat, is

$$Pr(H|T) = \prod_{i=1}^{K} PSF_i \bullet R \tag{4}$$

where PSF_i is the performance shaping function for attribute i. Typical PSFs might include design quality, manufacture quality, education, training and experience, organisational culture, stress, etc.

One open source database from which data is available to quantify the PSFs, the Global Terror Database (GTD), is collated by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland. Terrorist incidents were filtered based on Weapon Type and date (1998 to 2008). The dataset was re-characterised based on categorisation of device operation and device complexity – Unknown (insufficient incident information to make a categorisation); Simple (consisting of roadside bombs, hand-thrown devices and those containing conventional munitions as a warhead); Medium (car bombs, remotely-fused IEDs and use of homemade explosive); and Complex (devices such as homemade rockets, mortars and projectiles or IEDs with complex triggers). The limitations associated with the GTD constrained the fidelity of our model, however, we have been able to consider a PSF pertaining to device complexity based on Region and Organisational Culture, see Table II.

Table II shows significant variability in PSFs between organisational types and regions. One significant limitation of using the GTD as a dataset is that it has significant potential for bias related to open-source reporting, this is thought to be the reason why the results at Table II imply that IED initiation rates for Criminal, Terrorist and Insurgent Organisations equal that of their conventional equivalents used by Western militaries (i.e. $PSF = 1$). Despite this, particularly taking the data for Western incidents where reporting is more likely to be reflective of the actual incident population, we can identify that the lowest levels of performance were observed for individuals, as would be expected for conventional engineering and manufacturing activities since the diversity within teams means that they are better equipped to design and manufacture IEDs than individuals. It is also notable that the PSFs that were identified are similar to the critical factors that have been identified as impacting the performance of personnel and equipment for other industries/professions involving processes, skill and stress.

For more details, including probabilistic estimates of loss (damage, casualties) due to IED initiation, see Grant and Stewart (2011).

Table II. PSFs for IEDs in Regions of Interest

Organisational Culture	Device Complexity	Global	Western	Middle East & North Africa
Individual	Simple	0.588	0.537	0.614
	Medium	0.695	0.521	-
	Complex	-	-	-
Criminal	Simple	→1	0.986	1
	Medium	0.972	0.956	1
	Complex	0.550	-	-
Terrorist Organisation	Simple	0.981	0.855	0.990
	Medium	0.980	0.928	0.953
	Complex	0.905	0.761	1
Insurgent Organisation	Simple	→1	NA	1
	Medium	→1	NA	1
	Complex	→1	NA	1

3.2. TIME-PRESSURE LOAD HISTORY OF EXPLOSIVES

The variability in blast loading can be traced to:

(a) Parameter uncertainty,
(b) Inherent variability − natural, intrinsic, irreducible uncertainty of a situation, and
(c) Model error − measure of accuracy of predictive model.

In all cases the variabilities can be represented as one or more random variables described by their mean, COV (coefficient of variation) and probability distribution function. The probabilistic blast load model considers parameter uncertainties for (Netherton and Stewart 2010):

(a) User factor for mass of explosive (W_{user}),
(b) Net equivalent quantity (NEQ) of an explosive in terms of a mass of TNT (W_{NEQ})
(c) The range (R) and Angle of Incidence (AOI), and
(d) Air temperature (T_a) and pressure (P_a).

Probabilistic models for model error and inherent variability were obtained from field data of repeatable tests. The polynomial curves from the explosive blast loading model proposed by Kingery and Bulmash (1984) have been incorporated into widely used and well respected blast load design models, such as ConWep (1991), TM5-1300 (1990) and LS-DYNA. Given such wide acceptance, the polynomials of Kingery and Bulmash (1984) are used for predicting blast load values. The time-pressure history is idealised by an equivalent triangular pressure pulse.

The variability of blast load will be influenced by the type of explosive used, its manufacturer, its placement, etc. One explosive of significant interest to counter-terrorism personnel is "home-made" Ammonium Nitrate Fuel Oil (ANFO) delivered by a VBIED. The statistical parameters describing the variability of input parameters and model error (accuracy) are given in Table III, for a VBIED that uses ANFO as the explosive. For more details of the probabilistic blast load model see Netherton and Stewart (2010), which also includes a blast scenario for weapon delivery of a 500 lb Mark-82 GP bomb (89 kg Tritonal) using GBU-38 JDAM (GPS) guidance control.

Table III. Statistical Parameters for Blast Loading Model (Netherton and Stewart 2010).

Parameter	Mean	COV	Distribution
Energetic Output:			
User factor	1.00	0.102	Normal
NEQ factor	Mode = 0.82	0.359	Triangular
Detonation Location:			
VBIED Location	x = 0	σ = 3.06 m	Normal
	y = R	σ = 1.53 m	Normal
	z = 0	σ = 0 m	Deterministic
Ambient Air Temperature (^{o}C)	21.9 ^{o}C	0.356	Normal
Ambient Air Pressure (hPa)	1015.0 hPa	0.014	Uniform
Model Error:			
Peak reflected pressure (P_r)	1.032	0.069	Normal
Peak reflected impulse (I_r):			
0.59 m/kg$^{1/3}$ $\le Z <$ 6.0 m/kg$^{1/3}$	0.991	$0.178 - 0.0236Z$	Normal
6.0 m/kg$^{1/3}$ $\le Z <$ 40.0 m/kg$^{1/3}$	0.991	0.036	Normal
Time of positive phase duration (t_d):			
0.59 m/kg$^{1/3}$ $\le Z <$ 6.0 m/kg$^{1/3}$	$0.43 + 0.596\log_{10}Z$	$C_0 + C_1Z + C_2Z^2 + C_3Z^3$	Normal
6.0 m/kg$^{1/3}$ $\le Z <$ 9.0 m/kg$^{1/3}$	$0.43 + 0.596\log_{10}Z$	0.046	
9.0 m/kg$^{1/3}$ $\le Z <$ 40.0 m/kg$^{1/3}$	1.00	0.046	Normal

Note: $C_0 = 0.6267$, $C_1 = -0.3510$, $C_2 = 0.0713$, $C_3 = -0.0048$, Z is scaled distance (m/kg$^{1/3}$)

The blast scenario considered herein is a small van-sized VBIED comprising 116 kg of "home-made" ANFO. The explosive for this scenario detonates on or very near to the ground. It is thus considered a hemispherical charge detonating against a reflecting surface. The blast load is from a single uninterrupted emanation of the shock-wave and that reflections from other structures or surfaces are not considered. The probability distribution of peak reflected pressure (P_r), impulse (I_r), and the time of a blast-waves first positive phase duration (t_d) are the outcomes of the probabilistic analysis − see Figure 2 for W = 116 kg ANFO and stand-off R = 50 m. Figure 2 also shows the TM5-1300 (or ConWep) design values. Note that

the design value based on the TM5-1300 approach includes a 'safety factor' where explosive mass (W) is increased by 20%. It is observed that the variability of blast load parameters is considerable, with COVs of 0.15 to over 1.0. These are significant variabilities, and roughly equivalent to the observed variability for earthquake loadings which has the highest variability of all natural hazards. It is observed that the probability that the explosive load exceeds the TM5-1300 design value is 28%, 4% and 19% for P_r, I_r and t_d, respectively. More research is needed that calculates the probability of exceedance for a wider range of blast scenarios before any definitive conclusions can be made about the conservatism (or not) of ConWep, TM5-1300 and other design tools for explosive blast loading.

4. Probabilistic Modelling of Structural Response and Reliability Analysis

The probability of the hazard for infrastructure conditional on the occurrence of a specific threat is

$$Pr\left(H|T\right) = Pr\left[G(\mathbf{X}) \le 0\right] \tag{5}$$

where $G(\mathbf{X})$ is the limit state function (of structural response) and $\mathbf{X}$ is the vector of all relevant variables. $G(\mathbf{X}) = 0$ defines the boundary between the 'unsafe' and 'safe' domains. The limit state functions can be expressed in terms of structural damage, safety hazards and casualties. The exposure of people to blast effects is highly dependent on site location, building layout, occupancy rates, etc. and so the effect of low and high exposures will be considered, both deterministically and probabilistically. As a structure ages the effect of deterioration and other time-dependent processes may lead to higher values of $Pr(H|T)$.

Computer software Blast-RF (Blast Risk for Facades) that calculates $Pr(H|T)$ for damage, safety level and casualties for glazing systems is currently under development and intended as freeware in the near future. Details are available elsewhere (Stewart and Netherton 2008, Netherton and Stewart 2009).

The discussion to follow will focus instead on the structural capacity and reliability of RC columns subject to explosive blast loading. The RC column is representative of a ground floor central column of a two storey RC frame building (Shi et al. 2008). The RC column is H = 4.6 m high and is of rectangular cross-section (see Figure 3). Table IV shows the design (nominal) material and dimensional properties of the RC column. The finite element model used herein is identical to that developed by Shi et al. (2008) using explicit FEM software LS-DYNA.

Since RC columns are designed to support an axial load, then the damage criterion is based in axial load-carrying capacity. The damage index (D) is defined as (Shi et al. 2008):

$$D = 1 - \frac{P_{residual}}{P_{design}} \tag{6}$$

where $P_{residual}$ is the residual axial load-carrying capacity of the damaged column, and P_{design} is the maximum axial load-carrying capacity of the undamaged column. Shi et al. (2008) define four damage limit states based on the damage index D:

1. D = 0−0.2 low damage
2. D = 0.2−0.5 medium damage
3. D = 0.5−0.8 high damage
4. D = 0.8−1.0 collapse

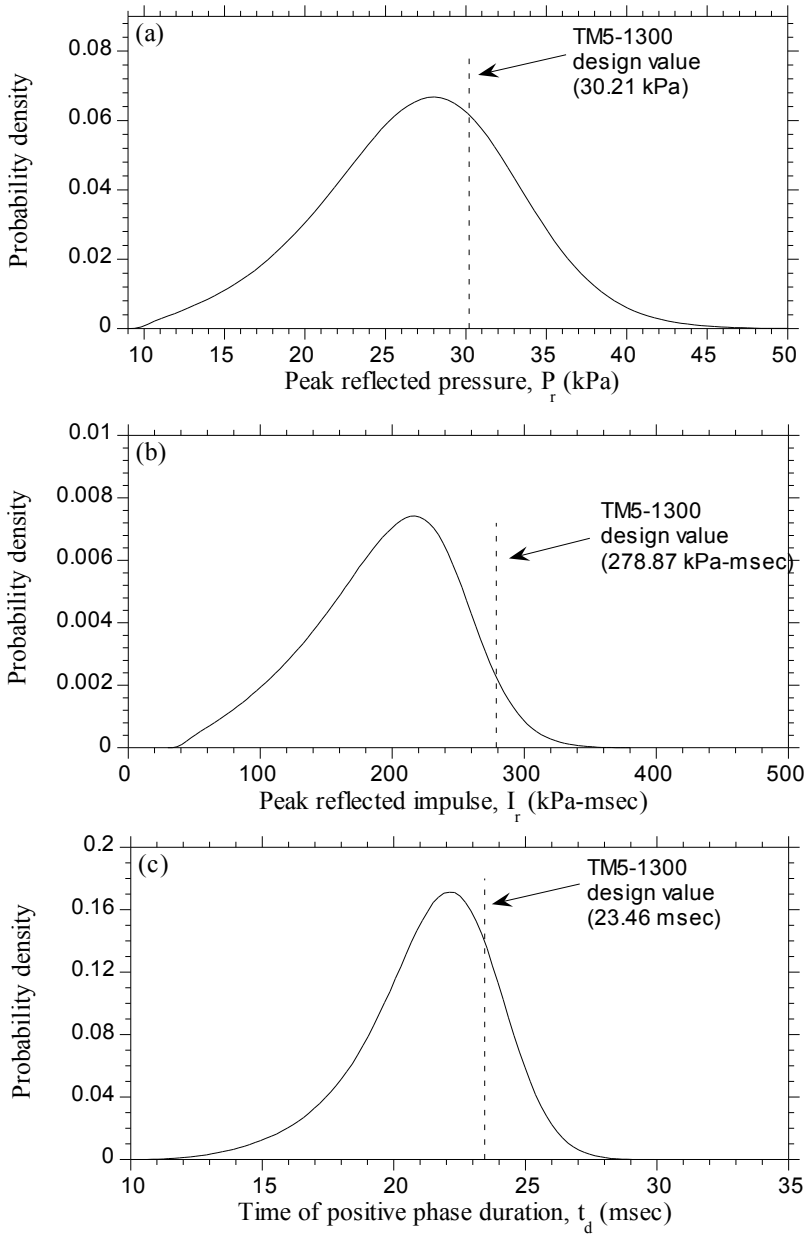

Figure 2. Probability Distributions of Blast Load Parameters and Comparison with TM5-1300 Design Values (adapted from Netherton and Stewart 2010).

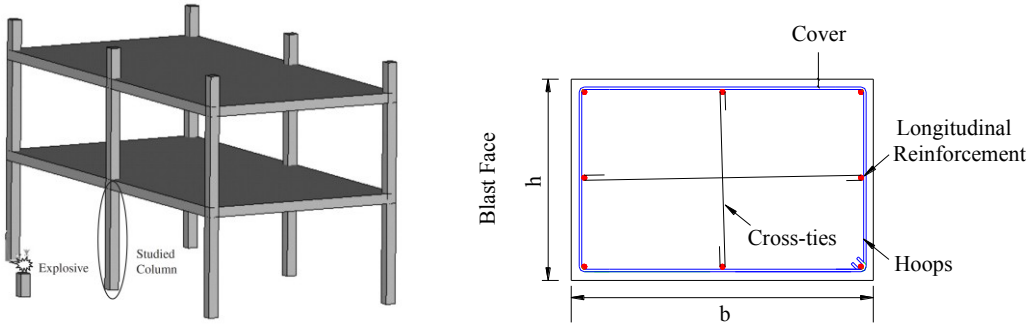

Figure 3. Location and Cross-section of RC Column.

Table IV. Material and Dimensional Properties for RC Column.

Parameter	Design Value
Column width (h)	400 mm
Column depth (b)	600 mm
Hoops/Cross ties spacing (s)	200 mm
Longitudinal reinforcement	8 × 20 mm diameter
Yield strength of longitudinal steel (F_y)	413.7 MPa (Grade 60)
Hoops/Cross ties	10 mm @ 200 mm spacing
Yield strength of hoops and cross-ties	275.8 MPa (Grade 40)
Cover	25 mm
Concrete Compressive Strength (F'_c)	42 MPa

Monte-Carlo simulation (MCS) is used for reliability estimation of the RC column. The probability of damage states conditional on threat T is $Pr(H|T)$:

$$Pr\left(\text{low damage}|T\right)=\frac{n\left[D<0.2\right]}{N} \qquad Pr\left(\text{medium damage}|T\right)=\frac{n\left[0.2\le D\le 0.5\right]}{N}$$
$$Pr\left(\text{high damage}|T\right)=\frac{n\left[0.5<D\le 0.8\right]}{N} \qquad Pr\left(\text{collapse}|T\right)=\frac{n\left[D>0.8\right]}{N} \tag{7}$$

where $n[]$ is the number of realisations when D matches the damage criterion, and N is the number of simulation runs.

The blast scenario considered is a $W = 100$ kg ANFO VBIED detonated from $R = 2.5$ m to $R = 20$ m from the front face of the RC column. The probabilistic load model described in Section 3.2 is used herein, where statistical parameters are given by Table III. The statistical parameters for cover, concrete compressive strength and yield strength of reinforcement are given in Table V. These statistics are representative of new RC columns constructed in the United States. Due to high computational demand associated with LS-DYNA, $N = 100$ simulation runs were used to generate distributions of load-carrying

capacity, damage index and probabilities of damage and collapse.

Table V. Statistical Parameters for RC Column (adapted from Stewart et al. 2011).

Parameter	Mean	COV	Distribution
Cover (mm)	C_{nom} + 6.4 + 0.004h	σ = 24.9 mm	Normal[a]
Yield Strength (MPa)	$1.145F_y$	0.05	Normal[b]
Concrete Compressive Strength	F'_c + 7.5 MPa	σ = 6 MPa	Lognormal

Note: [a] truncated at stirrup diameter (10 mm), [b] truncated at zero.

Results show that the COV of load-carry capacity of the undamaged (P_{design}) and damaged ($P_{residual}$) columns when R = 10 m are 0.13 and 0.32, respectively. Clearly, there is increased variability for a damaged structural element. Blast Reliability Curves (BRCs) are shown in Figure 4. The 90% confidence bounds are also shown − more simulation runs would reduce the 90% confidence intervals, but those shown in Figure 4 are sufficient to infer the BRCs. As expected, the probability of collapse reduces as stand-off (R) increases, and when R exceeds 15 m the probability of collapse is negligible. On the other hand, even though the risk of collapse is less than 10% when R = 10 m, there still remains a very high likelihood of low or medium damage. The BRCs provide a useful metric for assessing safety and damage risks. For more details see Stewart et al. (2011).

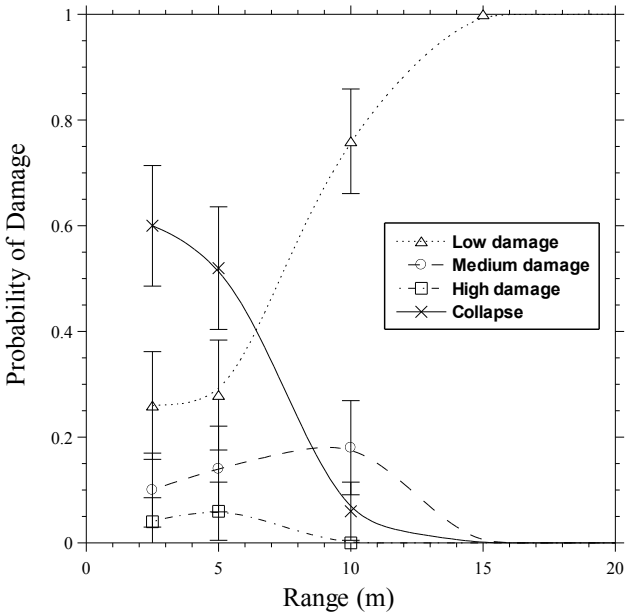

Figure 4. Blast Reliability Curves (BRC) for RC Column.

5. Cost Benefit Assessment of Infrastructure Protection

To illustrate the benefits of probabilistic terrorism risk assessment an airport terminal and institutional building subject to a terrorist Vehicle Borne Improvised Explosive Device (VBIED) are considered. The illustrative example will show under what combination of security costs, risk reduction, fatality and damage costs, and attack probability the protective measures would be cost-effective.

5.1. AIRPORTS

Although there may be special reasons to protect airplanes, it is not at all clear that there are any special reasons to protect airports. Compared with many other places of congregation, people are more dispersed in airports, and therefore, a terrorist attack is likely to kill far fewer than if, for example, a crowded stadium is targeted. The 2011 suicide bombing of the arrivals area of Moscow's Domodedovo airport, which killed 36 and injured 15 others, shows that airports are not unattractive targets, but in the previous year, suicide bombers targeted the Moscow metro, killing 25, and the year before that, derailed the Moscow to St. Petersburg high-speed train, killing 27.

In addition, airports sprawl and are only two or three stories high, and therefore damage to a portion is not likely to be nearly as significant as damage to a taller or more compact structure. Moreover, if a bomb does go off at an airport, the consequences would probably be comparatively easy to deal with: passengers could readily be routed around the damaged area, for example, and the impact on the essential function of the airport would be comparatively modest.

In the 10 year period 1998−2007 there were ten (2 fatalities) and nine (29 fatalities) attacks on airports in Europe and Asia-Pacific, respectively. The annual fatality risk is approximately 2×10^{-10} and 6.5×10^{-9} for Europe and Asia-Pacific, respectively. These are very low risks, and are considered "acceptable" based on a fair degree of agreement about acceptable risk (Stewart and Melchers 1997). However, terrorism is a hazard where risk acceptability might not be a matter of fatality risks due to the significant direct and indirect economic consequences of a terrorist attack. For example, losses inflicted by the terrorist attack that has been by far the most destructive in history, that of September 11, 2001 approached $200 billion (Mueller and Stewart 2011a).

The threat considered herein is a bombing of an airport terminal. A small IED might kill say five people, no structural damage, and minimal disruption to flight schedules - we value this attack at $50 million based on the value of a single life (VSL) is $6.5 million (Robinson 2010) plus other costs. On the other hand, a larger VBIED might kill 100 people ($65 million), severe structural damage to part of a terminal building ($100 million), and flight disruptions and relocation of check-in counters, etc. might total several billion dollars as a plausible upper bound. Security and protective measures to mitigate IED or VBIED attacks might include extra security personnel, vehicle entry screening for explosives, bollards, parking restrictions, etc. To be conservative, we assume that the increased cost of security is $C_{security}$ = $2 million per year for each airport terminal. For Sydney Airport, this would be equivalent to an 8% increase in their security budget. Opportunity costs associated with some security measures might be considerable, such as parking restriction near the terminal might deter passengers, or extra security screening will delay passengers. We do not consider such opportunity costs in this analysis.

Equation (1) can be simplified by assuming that $Pr(H|T) = Pr(L|H) = 1$, and so a break-even analysis to calculate how many attacks would have to take place to justify the expenditure gives

$$p_{attack-min} = \frac{C_{security}}{L \bullet \Delta R} \tag{8}$$

Table VI arrays the annual attack probabilities ($p_{attack\text{-}min}$) required at a minimum for enhanced security expenditures on protecting an airport terminal to be cost-effective.

This break-even analysis shows that protective measures that reduce risk by an impressive 75% and that successfully protect against an attack that would otherwise inflict $50 million in damage would be cost-effective only if the annual probability of a successful terrorist attack without them exceeds 0.05 or one in 20 per terminal per year. If we assume a $2.5 billion attack, and risk is reduced by 75 percent, the minimum attack probability per year required for airport protective measures to be considered cost-effective reduces to 0.001 per terminal per year. There have been five bomb attacks in the ten year period 1998−2007 in the Asia-Pacific region. If we assume there are 500 airport terminals in the Asia-Pacific region, then the attack probability is 0.001 per terminal per year. In this case, security and protective measures that cost $2 million per year would only be cost-effective if they reduce risk by 75% and prevent losses of $2.5 billion. For lower losses, or risk reductions, such security and protective measures would only be cost-effective if the attack probability greatly exceeded 0.001 per terminal per year.

Table VI. The number of otherwise successful attacks per year in which enhanced airport security would have to be solely responsible for deterring, foiling, or protection against in order for its enhanced yearly security budget of $2 million to be cost-effective, at various levels of loss and risk reduction − that is, for the security benefit of the expenditures to equal their costs.

Risk Reduction Caused by Enhanced Airport Security Expenditure (ΔR)	Losses from a Successful Terrorist Attack (C_{loss})				
	$50 million	$100 million	$500 million	$1 billion	$2.5 billion
5 percent	0.80	0.40	0.080	0.040	0.0160
10 percent	0.40	0.20	0.040	0.020	0.0080
25 percent	0.16	0.08	0.016	0.008	0.0032
50 percent	0.08	0.04	0.008	0.004	0.0016
75 percent	0.05	0.03	0.005	0.003	0.0011
100 percent	0.04	0.02	0.004	0.002	0.0008

5.2. BUILDINGS

A typical multi-storey building for which occupancy and loss data are available is an academic building located at the U.S. Naval Postgraduate School in Monterey, California (Lakamp and McCarthy 2003). In this case, measures to protect the building from VBIED and other explosive blast loads include strengthening perimeter columns and walls, blast-resistant glazing and other improvements to structurally harden the building.

Damage and loss parameters are considered as random variables that explicitly consider aleatory and epistemic uncertainties. Three threat scenarios are assumed as $i = 1$: low, $i = 2$: medium and $i = 3$: high terrorist threats, and two types of loss attributes $j = 1$: direct physical damage and $j = 2$: fatalities. The net benefit from eqn. (1) is re-written for this example as

$$E_b = \sum_{i=1}^{3}\sum_{j=1}^{2} p_{attack}\, Pr(T_i|attack) Pr(H_i|T_i) Pr(L_j|H_i) \bullet L_j \bullet \Delta R_i - C_{security} \quad (9)$$

where p_{attack} is the annual attack probability, $Pr(T_i|attack)$ is the relative threat probability given an attack, 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), and ΔR_i is the percentage reduction in risk due to CT protective measures for the i^{th} threat. We assume that $C_B = 0$ and $Pr(H_i|T_i) = 1$.

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 $Pr(T_i|attack)$ 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 VII. Stewart (2011) has shown that the probability of building occupant fatality given a terrorist attack $Pr(L_2|H_i)$ varies from 0.0003 to 0.45 and so $Pr(L_2|H_i)$ is assumed relatively low for low and medium threats, and is unlikely to reach above 0.5 even for a high threat. This example does not consider the risk and safety of people outside the building (such as pedestrians).

Although a small VBIED can cause low casualties, the effect on physical damages can be much higher as although a VBIED may not totally destroy a building, it will often need to be demolished and replaced, hence the probability of physical damage is high even for a medium threat. As there is uncertainty about these threat and loss probabilities then they are treated as random variables and Table VII shows their assumed statistical parameters and probability distributions. Note that a coefficient of variation (COV) of 0.25 represents a 95% confidence interval of approximately ± 50% about the mean value.

Table VII. Probabilistic Models for Hypothetical Threats and Losses (Stewart 2010b).

	Relative Threat Probability $Pr(T_i\|attack)$	Probability of Physical Damage $Pr(L_1\|H_i)$			Probability of Fatalities $Pr(L_2\|H_i)$		
Threat		mean	COV	Distribution	mean	COV	Distribution
$i = 1$ Low	0.6	0.25	0.1	Lognormal	0.1	0.25	Lognormal
$i = 2$ Medium	0.3	0.80	0.1	Lognormal	0.25	0.25	Lognormal
$i = 3$ High	0.1	1.0	-	-	0.5	0.25	Lognormal

Note: probability distributions censored at 0.0 and 1.0

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. It follows that risk reduction will reduce, perhaps marginally, as the size of the threat increases. Risk reductions are also modelled as a random variables, see Table VIII, where it is assumed that the risk reduction is accurate to ± 10%.

Table VIII. Probabilistic Models for Hypothetical Risk Reduction (Stewart 2010b).

	Risk Reduction ΔR_i		
Threat	mean	COV	Distribution
$i = 1$ Low	90%	0.064	Uniform [80−100]
$i = 2$ Medium	65%	0.089	Uniform [55−75]
$i = 3$ High	50%	0.115	Uniform [40−60]

The cost of physical damages is approximately L_1 = \$35 million − this includes replacement value of the building, value of contents, and demolition costs. There is more certainty about damage losses so L_1 is modelled as a normal distribution with mean = \$35 million and COV = 0.05. The academic building is sizeable, with offices and teaching space, and peak usage comprising 319 building occupants (Lakamp and McCarthy 2003). To maximise the impact of a terrorist attack, an attack would most likely occur at a time of high building occupancy, so it is assumed herein that the number of occupants (L_2) is modelled as a normal distribution with mean = 250 people and COV = 0.17 so that there is a 10% probability than occupancy will be higher than 319 occupants in the event of a terrorist attack. The value of a single life (VSL) is \$6.5 million (Robinson 2010), hence, mean L_2 = \$1.6 billion.

A literature review by Stewart (2011) found that the minimum cost of protective measures ($C_{security}$) needed for substantial risk reduction for an existing building is at least 10% of building costs. If we assume that the budget time period for providing protective measures to the building is five years, then if the 10% increase in costs is annualised over five years with a discount rate of 3% then this equates to a present value cost of $C_{security} \approx$ \$450,000 pa.

The net benefit is calculated from Eqn. (10) using Monte-Carlo simulation analysis for a range of attack probabilities. Figure 5 shows the simulation histogram of net benefit for three attack probabilities: $p_{attack} = 10^{-2}$, 10^{-3} and 10^{-4} /building/year. As there is random variability with many of the input parameters then net benefit is variable as shown in Figure 5. With reference to Figure 5 it is clear that if $p_{attack} = 10^{-2}$ per building per year then there is near 100% confidence that the net benefit is positive so near 100% sure that the protective measures are cost-effective. On the other hand, if $p_{attack} = 10^{-4}$/building/year then there is near 100% certainty that protective measures are not cost-effective. If $p_{attack} = 10^{-3}$/building/year then Figure 5 shows that there is only a 35% probability that protective measures are cost-effective (i.e., $Pr(E_b) > 0$). Figure 6 shows another way to present results and this shows the mean and lower and upper bounds (5th and 95th percentiles) of net benefit for various attack probabilities. The threshold threat probability is 5.6×10^{-4}/building/year so if an attack probability exceeds this threshold (or break-even) value then the protective measure is likely to be cost-effective. Note that Ellingwood (2006) suggests that the minimum attack probability be at least 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 may be high, the probability that any particular item of infrastructure will be attacked is very low. If the annual attack probability is 10^{-4}/building/year then the protective costs outweigh the benefits ($E_b < 0$) and so protective measures would not be cost-effective. Clearly, due to the uncertainties inherent in such an analysis, a sensitivity analysis is recommended, see Stewart (2010a) for further details and analysis.

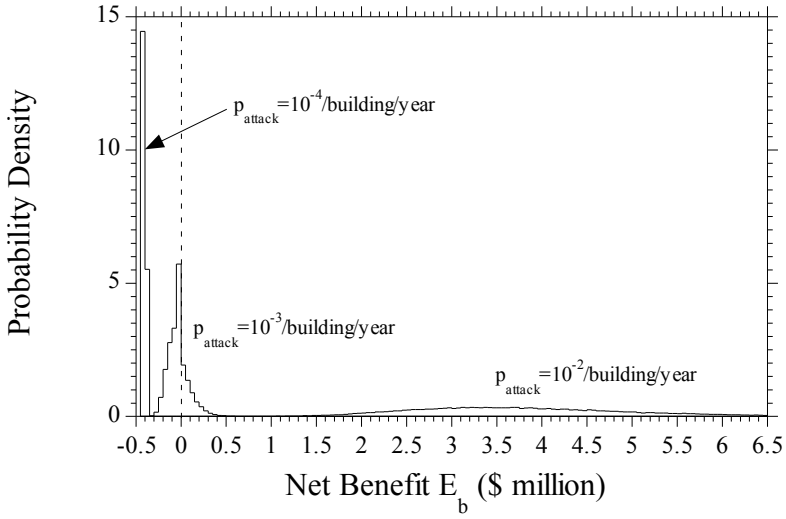

Figure 5. Histograms of Annual Net Benefit (E_b) for Institutional Building, for Attack Probabilities of 10^{-2}, 10^{-3} and 10^{-4} per year.

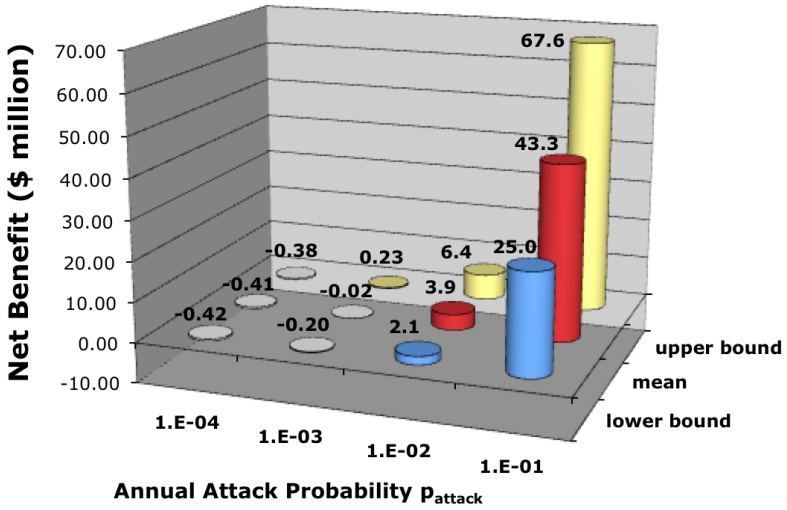

Figure 6. Annual Net Benefit (E_b) for Institutional Building.

6. Risk Transfer

An important consideration in critical infrastructure protection is the displacement effect, a transfer of risk. Terrorists can choose, and change, their targets, depending on local and immediate circumstances. This

process, of course, does not hold in the case of natural disasters: a tornado bearing down on Kansas does not decide to divert to Oklahoma if it finds Kansans too well protected. In contrast, if the protection of one target merely causes the terrorist to seek out another from among the near-infinite set at hand, it is not clear how society has gained by expending effort and treasure to protect the first. The people who were saved in the first locale are gainers, of course, but their grief is simply transferred to others.

For example, there is a program to protect bridges in the United States, and a list of something like 200 of the most important bridges has been drawn up. There seems to be no evidence terrorists have any particular desire to blow up a bridge, due in part, perhaps, to the facts that it is an exceedingly difficult task under the best of circumstances and that the number of casualties is likely to be much lower than for many other targets.

The apparent hope of the protectors in this case is that, after security is improved for all these targets, any terrorists who happen to have bridges on their hit list will become disillusioned. If so, however, they might become inclined to move on to the 201st bridge or, more likely perhaps, to another kind of bridge: the highway overpass, of which there are some 600,000 in the United States. If the terrorists' attention is drawn, further, to any one of a wide array of multiple overpass bridge networks, they might be inclined to destroy one of those. The financial and human consequence, not to mention the devastating traffic inconvenience, that could result from such an explosion might well surpass the destructive consequences of one directed at one of those 200 bridges. The issue, then, is: how has society been benefited by the protection of the bridges?

The 2011 suicide bombing at Moscow's Domodedovo airport took place in the arrivals area, well away from the passenger security screening. Accordingly, any risk reduction passengers gained by being in the secure zone of the airport was simply transferred to those outside, as the attackers targeted a place of public assembly for which there are few countermeasures.

Or there is the case of the installation of sensors to measure chemical, biological, or radiological levels in New York. Presumably, any terrorists clever enough to engineer the relevant weapons are likely to be able to learn where the sensors have been put in place, and there is no gain to society if they simply choose to move to Newark or Washington or Columbus. However, this elemental consideration does not appear to have been part of the decision process.

7. Assessing 'Critical' Infrastructure

There is no doubt that a terrorist attack on many infrastructure elements could cause considerable damage and significant loss of life. However, while such targets as buildings, bridges, highways, pipelines, mass transit, water supplies, and communications may be essential to the economy and well-being of society, damage to one or even several of these, with few exceptions, will not be "critical" to the economy, or to the state.

In part, this is because infrastructure designers and operators place much effort on systems modelling to ensure that a failure of one node will not keep the network from operating, even if at reduced efficiency. This is done routinely: for example, it is necessary to close many bridges from time to time for maintenance or repair, and therefore traffic is redirected so that the network is not interrupted. Other failures routinely planned for include traffic accidents, severe weather, earthquakes, and equipment malfunctions. In other

words, as a matter of course, infrastructure is designed with built-in redundancies and backup systems to ensure resilience in the event of anticipated or unexpected hazards.

There is also a displacement effect, a transfer of risk. Terrorists can choose, and change, their targets, depending on local and immediate circumstances. If the protection of one target merely causes the terrorist to seek out another from among the near-infinite set at hand, it is not clear how society has gained by expending effort and treasure to protect the first.

Relying on standard evaluative measures accepted for decades by analysts, governments, regulators, and risk managers, efforts to protect people and structures from the effects of a terrorist attack are unlikely in general to be cost-effective because of the multiplicity of targets, the ability of terrorists to shift targets as needed, the capacity in many cases to quickly rebuild, the exceedingly low likelihood of an attack on a specific target, the limited capability of most terrorist groups, and the difficulty of predicting which targets are most appealing to them. If the terrorists' goal is to kill people, lucrative targets are essentially everywhere. If their goal is to destroy property, protection measures may be able to deter, inconvenience, or complicate, but only to the point where the terrorists seek something comparable among a vast—or even effectively infinite—array of potential unprotected targets.

Our cost-benefit assessment suggests, then, that many individual items of infrastructure, including airports and buildings, require no protective measures unless, perhaps, there is a very specific threat to them.

Finally, we are not arguing that much of homeland security spending is wasteful because we believe there will be no more terrorist attacks. Like crime and vandalism, terrorism will always be a feature of life, and a condition of zero vulnerability is impossible to achieve. However, future attacks might not be as devastating as 9/11, as evidenced by the attacks on Western targets in the ten years since 9/11 that, although tragic, each have claimed victims numbering in the tens to a few hundred. The frequency and severity of terrorist attacks are low, very low in fact, which makes the benefits of enhanced counterterrorism expenditures challenging to justify by any rational and accepted standard of cost-benefit analysis.

8. Conclusions

Since there is uncertainty associated with terrorist threats, structural and system response, effectiveness of counter-terrorism and protective measures, and their ability to inflict damage, then there is a need for probabilistic approaches to assessing and mitigating terrorism risks. The paper reviews probabilistic risk assessments for (i) IED design and detonation, and predicting variability of time-pressure load history on infrastructure, (ii) reinforced concrete structural systems, (iii) airport protection, and (iv) buildings subject to a terrorist Vehicle Borne Improvised Explosive Device (VBIED). The illustrative examples highlighted the recent research, and identified research challenges to be faced in the future. It was found that attack probabilities have to be very high for security and protective measures for buildings and airports to be cost-effective.

Acknowledgements

The support of the Australian Research Council is gratefully acknowledged. The assistance of PhD students Michael Netherton, Yufeng Shi, and Matt Grant is greatly appreciated. Professor Mueller appreciates the financial support of a Distinguished Scholar Award at Ohio State University.

References

Anderson, T. (2006), Terror May Be at Bay at Port: Shipping Hubs Too Vulnerable, *Daily News of Los Angeles*, 18 May.

CONWEP (1991), *Conventional Weapons Effects Program*. Prepared by D.W. Hyde, US Waterways Experimental Station, Vicksburg.

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

Department of Defense (1995), *MIL-HDBK-217F Reliability Prediction of Electronic Equipment Notice 2*, Washington, D.C.

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

DHS (2011), FY2011 Budget in Brief, Department of Homeland Security, Washington, D.C.

Eamon, E. (2007), Reliability of concrete masonry unit walls subjected to explosive loads. *Journal of Structural Engineering* ASCE, 133(7):935–44.

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

Grant, M. and Stewart, M.G. (2011), System and Reliability Modelling of Improvised Explosive Devices, *PARARI 2011 - 10th Australian Explosive Ordnance Symposium*, Brisbane, 8-9 November, 2011.

Hao, H., Stewart, M.G., Li, Z-X. and Shi, Y. (2010), RC Column Failure Probabilities to Blast Loads, *International Journal of Protective Structures*. 1(4):571-591.

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

Kingery, C.N. and Bulmash, G. (1984), *Airblast Parameters From TNT Spherical Air Burst and Hemispherical Surface Burst*. Technical Report ARBRL-TR-02555. US Army Armament Research and Development Centre, Maryland, USA.

Lakamp, D.J. and McCarthy, G.H. (2003), *A Cost-Benefit Analysis of Security at the Naval Postgraduate School*, MBA Professional Report, Naval Postgraduate School, Monterey, California.

Low, H.Y. and Hao, H. (2001), Reliability analysis of reinforced concrete slabs under explosive loading, *Structural Safety*, 23(2):157–178.

Low, H.Y. and Hao, H. (2002), Reliability analysis of direct shear and flexural failure modes of RC slabs under explosive loading, *Engineering Structures*, 24:189–198.

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

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

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

Netherton, M.D. and Stewart, M.G. (2009), The Effects of Explosive Blast Load Variability on Safety Hazard and Damage Risks for Monolithic Window Glazing, *International Journal of Impact Engineering*, 36(12): 1346-1354.

Netherton, M.D. and Stewart, M.G. (2010), Blast Load Variability and Accuracy of Blast Load Prediction Models, *International Journal of Protective Structures*. 1(4):543-570.

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

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

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

Shi, Y., Hao, H. and Li, Z-X. (2008), Numerical Derivation of Pressure-Impulse Diagrams for Prediction of RC Column Damage to Blast Loads, *International Journal of Impact Engineering,* 35(11): 1213-1227.

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

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

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

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

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

Stewart, M.G. and Mueller, J. (2008b), A Cost-Benefit and Risk Assessment of Australian Aviation Security Measures, *Security Challenges,* 4(3): 45-61.

Stewart, M.G. (2010a), Acceptable Risk Criteria for Infrastructure Protection, *International Journal of Protective Structures*, 1(1):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*, 3(1):29-40.

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

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

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

Stewart, M.G., Shi, Y. and Zhi, X. (2011), Structural Reliability Analysis of Reinforced Concrete Columns Subject to Explosive Blast Loading, *9th International Conference on Shock & Impact Loads on Structures*, Y. Sonoda and T.S. Lok (eds), CI-Premier, 91-102.

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

TM5-1300 (1990), Design of Structures to Resist the Effects of Accidental Explosions, US Department of the Army Technical Manual TM5-1300, USA.

Twisdale, L.A., Sues, R.H. and Lavelle, F.M. (1994), Reliability-based design methods for protective structures. *Structural Safety*,15(1–2):17–33.

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

Willis, H. and LaTourette, T. (2008), Using Probabilistic Terrorism Risk-Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative in the Land Environment*, Risk Analysis* 28(2):325-339.

Wolstenholme, L.C. (1999), *Reliability Modelling – A Statistical Approach*, Chapman & Hall/CRC, U.K.