Probabilistic terrorism risk assessment and risk acceptability for infrastructure protection[*]

MG Stewart[†], MD Netherton, Y Shi and M Grant
Centre for Infrastructure Performance and Reliability, The University of Newcastle, NSW, Australia

J Mueller
Mershon Center for International Security Studies, Ohio State University, USA

ABSTRACT: *In the decade since the events of 9/11 there has been renewed interest in understanding the risks of terrorism, and the effectiveness of counter-terrorism measures. Since there is uncertainty associated with terrorist threats, structural and system response, effectiveness of counter-terrorism and protective measures, and terrorists' ability to inflict damage, then there is clearly a need for probabilistic approaches to assessing and mitigating terrorism risks. The paper reviews research projects related to probabilistic terrorism risk assessment and risk acceptability for infrastructure protection currently underway at The University of Newcastle. The review of probabilistic risk assessments are given for: (i) IED design and initiation, and predicting variability of time-pressure load history on infrastructure; (ii) reinforced-concrete structural systems; (iii) full-body scanners used at airports in the United States; and (iv) buildings subject to a terrorist vehicle-borne improvised explosive device. The illustrative examples will highlight research capabilities at the University of Newcastle and identify research challenges to be faced in the future.*

KEYWORDS: Terrorism; risk; structural reliability; infrastructure; explosive blast loading.

REFERENCE: Stewart, M. G., Netherton, M. D., Shi, Y., Grant, M. & Mueller, J. 2012, "Probabilistic terrorism risk assessment and risk acceptability for infrastructure protection", *Australian Journal of Structural Engineering*, Vol. 13, No. 1, pp. 1-18, http://dx.doi.org/10.7158/S11-126.2012.13.1.

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 in 1992, 1993 and 1996; US Embassy in Kenya in 1998; Pentagon and World Trade Center in 2001; night clubs and restaurants in Bali in 2002 and 2005; Marriott Hotel in Jakarta in 2003; Australian Embassy in Indonesia in 2004; and "near misses" such as the recent Christmas Day Northwest Airlines aircraft suicide bombing attempt in 2009. The preferred method of attack is improvised explosive devices (IEDs), often through suicide tactics, against buildings and transport infrastructure (see figure 1).

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 two main threats are aircraft hijacking that could lead to 9/11 type attacks on buildings and other infrastructure, or a suicide bomber intent on destroying an aircraft in flight. The US 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

[*] Paper S11-126 submitted 12/09/11; accepted for publication after review and revision 7/12/11.

[†] Corresponding author Prof Mark Stewart can be contacted at mark.stewart@newcastle.edu.au.

© Institution of Engineers Australia, 2012

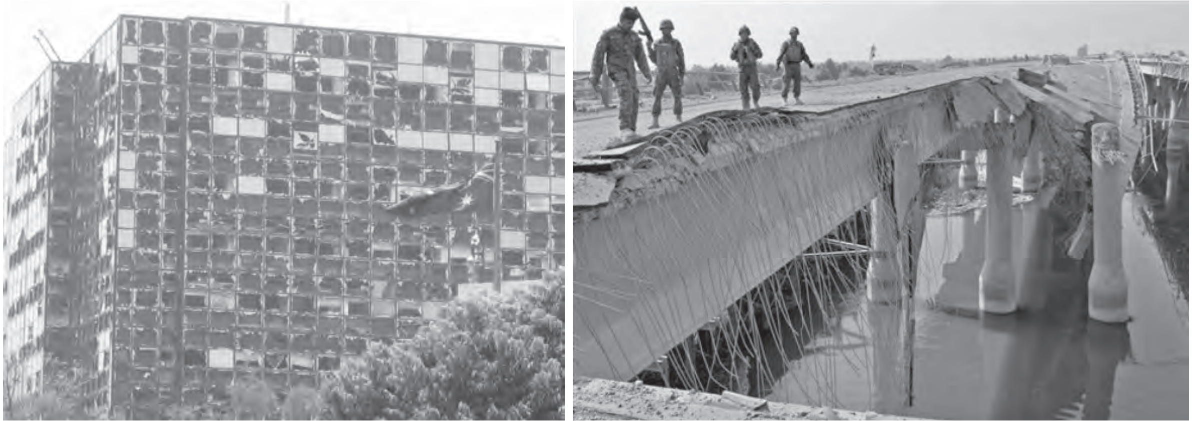

Figure 1: Vehicle-borne IED damage to building in Jakarta in 2004 (left) and bridge in Iraq in 2009 (right).

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 US 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 (eg. Twisdale et al, 1994; Low & 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 (eg. Stewart & 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 (eg. Stewart et al, 2006; Stewart & Netherton, 2008; Netherton & Stewart, 2009; Dillon et al, 2009; Cox, 2009; Stewart & Mueller, 2008a; 2008b; 2011), as well as recent life-cycle and cost-benefit analyses for infrastructure protective measures (Willis & LaTourette, 2008; von Winterfeldt & O'Sullivan, 2006; Stewart, 2008; 2010a; 2010b; 2011). Much of this work can be categorised as "probabilistic terrorism risk assessment".

Government spending on homeland security will reach $141.6 billion worldwide in 2009 and is projected to reach $300 billion by 2016. The cumulative increase in expenditures on US domestic homeland security over the decade since 9/11 exceeds one trillion dollars (Mueller & Stewart, 2011a; 2011b). 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 CT 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 11 September 2001 that there was a tendency to spend in haste on homeland security. For example, annual security costs for the US 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 US 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. 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.

The Centre for Infrastructure Performance and Reliability at the University of Newcastle has expertise in reliability and probabilistic risk assessment of physical infrastructure subject to deterioration, natural and man-made hazards, climate change, and other spatial and temporal effects. 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 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 for military planners
4. forensics to back-calculate charge weights.

Current research has focused on usage number 1. Discussions with the Australian Federal Police, Australian Defence Force, and other emergency response and security agencies have highlighted the importance of the other uses.

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 (RC) structural systems; (iii) full-body scanners used at airports in the US; and (iv) buildings subject to a terrorist vehicle-borne IED (VBIED). The illustrative examples will highlight research capabilities at The University of Newcastle, and identify research challenges to be faced in the future. 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 6) 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.

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 trade-offs 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:

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

where $E(C_B)$ is the expected benefit from the security measure not directly related to mitigating terrorist threats (eg. 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, terrorist access to flight deck, 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 (ie. 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 equation (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 (eg. Stewart, 2010a; 2010b; 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 (eg. Sunstein, 2002; Ellingwood, 2006). This is confirmed by the US Office of Management and Budget, 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, equation (1) can be generalised for expected utility incorporating risk aversion (eg. Stewart et al, 2011a). 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 & 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 & 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 (ie. 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 equation (1) provides an alternative decision-making criteria based on expected costs. A comparison of expected costs will provide information about relative performance levels of alternative CT protective measures. 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.

3 PROBABILISTIC BLAST LOAD MODELLING

3.1 Reliability of improvised explosive devices

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:

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

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, UK and US, and representative mobile phone data, to inform component reliabilities, is:

$$\begin{aligned} R = {} & 0.9994 \times 0.999 \times 0.98 \times 0.97 \\ & \times 0.97 \times 0.999 = 0.920 \end{aligned} \tag{3}$$

Table 1 provides a summary of baseline IED reliabilities derived from conventional munitions' representative component reliability data for common IED designs (Grant & Stewart, 2011). The baseline reliability assumes there are no errors in connecting

Table 1: 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

components, and assumes statistical independence of component reliabilities. Hence, R reflects the reliability of an IED designed and manufactured to military specifications and standards.

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

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

where PSF_i is the PSF 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 2).

Table 2 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 2 imply that IED initiation rates for criminal, terrorist and insurgent organisations equal that of their conventional equivalents used by western militaries (ie. 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 & Stewart, 2011).

3.2 Time-pressure load history of explosives

It is readily observed from field testing that the blast load experienced by a target structure – for apparently similar circumstances – will not always be the same. The variability in blast loading can be traced to:

- parameter uncertainty
- inherent variability – natural, intrinsic, irreducible uncertainty of a situation
- model error – measure of accuracy of predictive model.

Table 2: PSFs for IEDs in regions of interest.

Organisational culture	Device complexity	Global	Western	Middle East and 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	Simple	0.981	0.855	0.990
	Medium	0.980	0.928	0.953
	Complex	0.905	0.761	1
Insurgent	Simple	→1	NA	1
	Medium	→1	NA	1
	Complex	→1	NA	1

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

- user factor for mass of explosive (W_{user})
- net equivalent quantity (NEQ) of an explosive in terms of a mass of TNT (W_{NEQ})
- the range (R) and angle of incidence (AOI)
- 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 & Bulmash (1984) have been incorporated into widely-used and well-respected blast load design models, such as ConWep (Hyde, 1991), TM5-1300 (US Department of the Army, 1990) and LS-DYNA (Livermore Software Technology Corporation, 2011). Given such wide acceptance, the polynomials of Kingery & 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 CT 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 3, for a VBIED that uses ANFO as the explosive. For more details of the probabilistic blast load model see Netherton & 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.

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 (eg. Ellingwood et

Table 3: Statistical parameters for blast loading model (Netherton & Stewart, 2010). Note $C_0 = 0.6267$, $C_1 = -0.3510$, $C_2 = 0.0713$, $C_3 = -0.0048$, Z is scaled distance (m/kg$^{1/3}$).

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	$x = 0$	$\sigma = 3.06$ m	Normal
	$y = \mathrm{R}$	$\sigma = 1.53$ m	Normal
	$z = 0$	$\sigma = 0$ m	Deterministic
Ambient air temperature (°C)	21.9 °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)			
$0.59 \le Z < 6.0$ m/kg$^{1/3}$	0.991	$0.178 - 0.0236Z$	Normal
$6.0 \le Z < 40.0$ m/kg$^{1/3}$	0.991	0.036	Normal
Time of positive phase duration (t_d)			
$0.59 \le Z < 6.0$ m/kg$^{1/3}$	$0.43 + 0.596\log_{10}Z$	$C_0 + C_1Z + C_2Z^2 + C_3Z^3$	Normal
$6.0 \le Z < 9.0$ m/kg$^{1/3}$	$0.43 + 0.596\log_{10}Z$	0.046	
$9.0 \le Z < 40.0$ m/kg$^{1/3}$	1.00	0.046	Normal

al, 1980; Stewart & Melchers, 1997). 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.

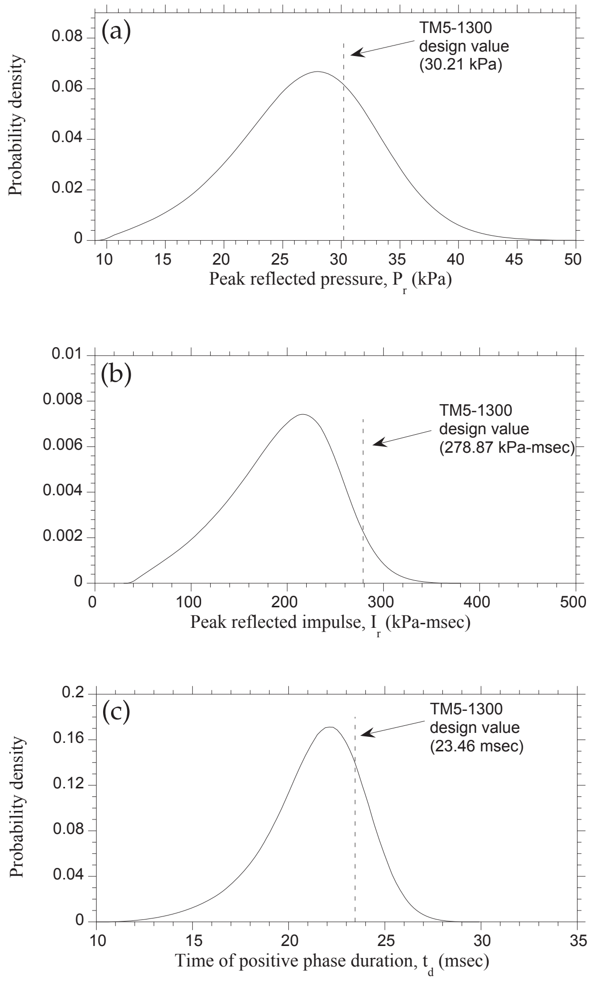

Figure 2: Probability distributions of blast load parameters and comparison with TM5-1300 design values (adapted from Netherton & Stewart, 2010).

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:

$$\Pr(H\,|\,T) = \Pr[G(\mathbf{X}) \leq 0] \tag{5}$$

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 façades) 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 & Netherton, 2008; Netherton & 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 4 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 finite element modelling 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):

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

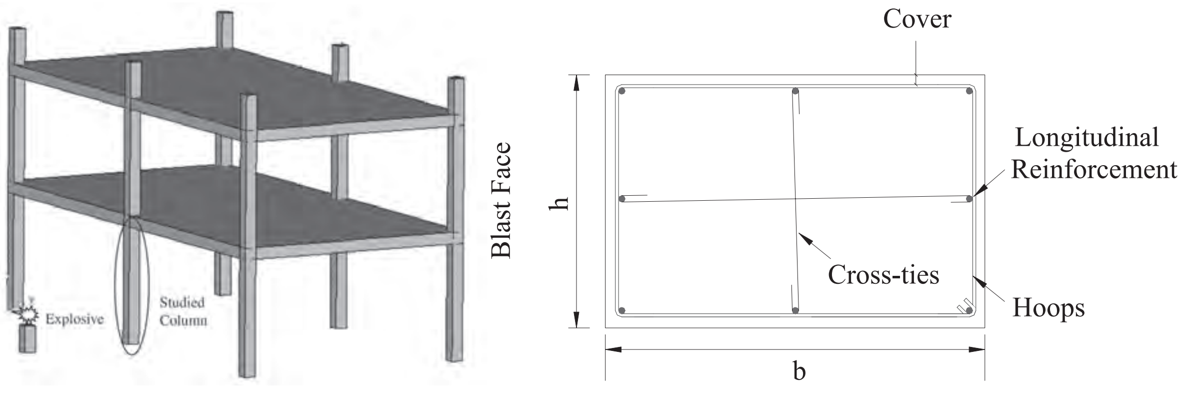

Figure 3: Location and cross-section of RC column.

Table 4: 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)
Fracture strain of longitudinal steel	18%
Hoops/cross-ties	10 mm at 200 mm spacing
Yield strength of hoops and cross-ties	275.8 MPa (Grade 40)
Fracture strain of hoops and cross-ties	18%
Cover	25 mm
Concrete compressive strength (f'_c)	42 MPa

Table 5: Statistical parameters for RC column (adapted from Stewart et al, 2011b).

Parameter	Mean	COV	Distribution
Cover (mm)	$C_{nom} + 6.4 + 0.004b$	$\sigma = 24.9$ mm	Normal#
Yield strength (MPa)	$1.145f_y$	0.05	Normal^
Concrete compressive strength	$f'_c + 7.5$ MPa	$\sigma = 6$ MPa	Lognormal
Note # truncated at stirrup diameter (10 mm), ^ truncated at zero.			

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 equal to:

$$P_{design} = 0.85f'_c(A - A_{st}) + f_y A_{st} \quad (7)$$

where f'_c is the compressive strength of concrete, A is the cross-sectional area of the RC column, A_{st} is the cross-sectional area of longitudinal reinforcement, and f_y is the yield strength of longitudinal reinforcement.

Shi et al (2008) defined 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).

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

$$\begin{aligned}
\Pr(\text{low damage}|T) &= \frac{n[D<0.2]}{N} \\
\Pr(\text{medium damage}|T) &= \frac{n[0.2 \le D \le 0.5]}{N} \\
\Pr(\text{high damage}|T) &= \frac{n[0.5 < D \le 0.8]}{N} \\
\Pr(\text{collapse}|T) &= \frac{n[D>0.8]}{N}
\end{aligned} \quad (8)$$

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 to 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 3. The statistical parameters for cover, concrete compressive strength and yield strength of reinforcement are given in table 5. These statistics are representative of new RC columns constructed in the US. 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.

The simulation histogram of load-carry capacity of the undamaged (P_{design}) and damaged ($P_{residual}$) columns when R = 10 m are shown in figure 4. It is observed that the COV is 0.13 and 0.32 for P_{design} and $P_{residual}$, respectively. Clearly, there is increased variability for a damaged structural element. Blast reliability curves (BRCs) are shown in figure 5. The 90% confidence bounds are also shown; more simulation runs would reduce the 90% confidence intervals, but those shown in figure 5 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

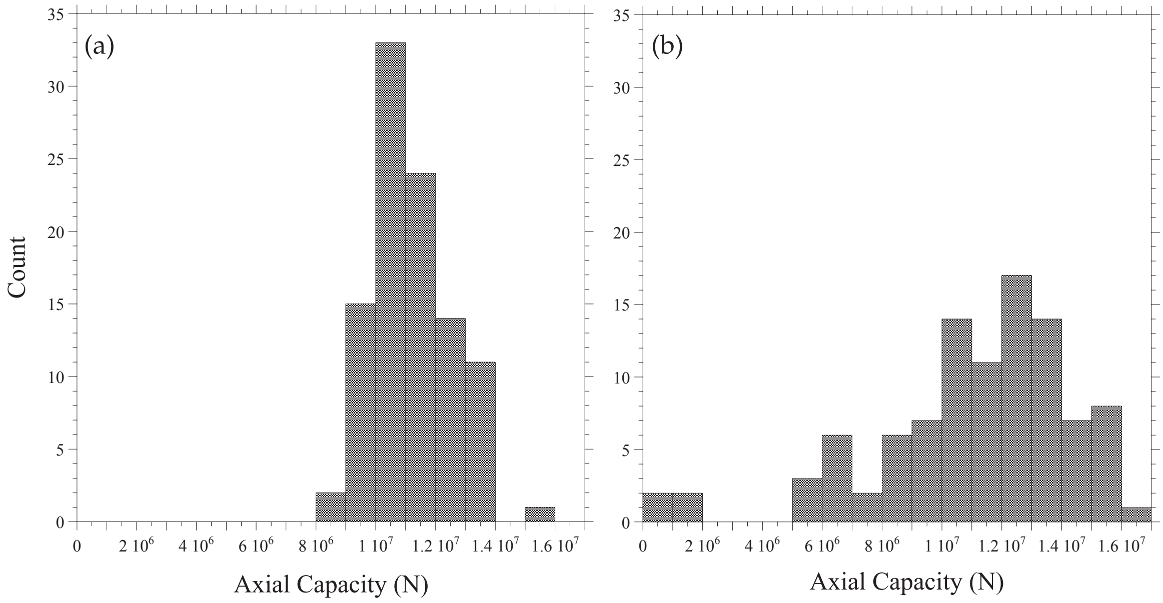

Figure 4: Simulation histograms for (a) undamaged (P_{design}) and (b) damaged ($P_{residual}$) RC columns for R = 10 m.

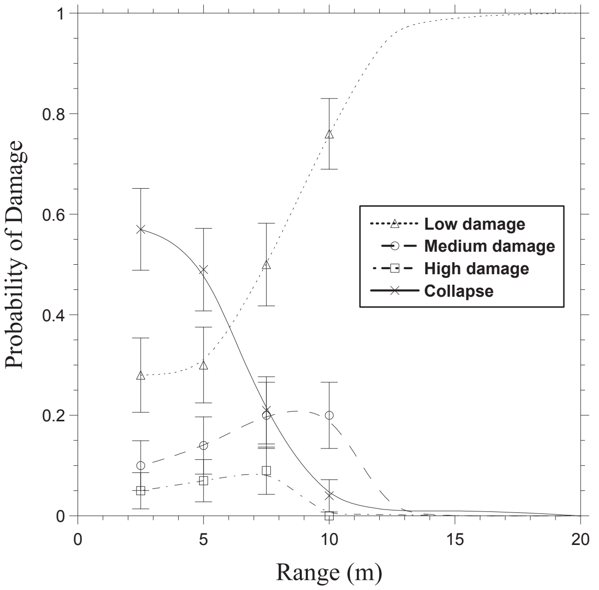

Figure 5: Blast reliability curves for RC column.

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 (2011b).

5 SYSTEM MODELLING AND RELIABILITY ANALYSIS FOR HOMELAND SECURITY MEASURES

Homeland security requires a systems and reliability approach not unlike engineering systems (see recent book by Mueller & Stewart, 2011a). Aviation security is a particular concern to policy-makers, where each layer of aviation security provides a CT measure that is inter-related to other security measures: some will be complementary, while some will be "stand-alone" measures. System modelling techniques can be used to represent all security measures, their inter-dependencies and time-critical influences (Stewart, 2010a; 2010b). To illustrate this concept, the reliability of aviation security measures is considered, with risk reduction estimated for advanced imaging technologies (AITs) that are full-body scanners to inspect a passenger's body for concealed weapons and explosives.

The United States TSA has been deploying AITs since 2010 and the cost of this technology will reach $1.2 billion per year by 2014. AITs are being trialled or deployed in the UK, France, Netherlands, Italy, Canada, Australia and elsewhere, which will cost billions of dollars if they are also used for primary screening in those countries. The terrorist threat that AITs are primarily dedicated to is preventing the downing of a commercial airliner by an IED smuggled on board by a passenger. Since AITs operated by the TSA are effective only for passengers leaving the US, the risk reduction applies for a suicide bomber who attempts to board an aircraft at a US airport.

The TSA has arrayed "21 Layers of Security" to "strengthen security through a layered approach". The risk reduction (ΔR) is the additional risk reduction achieved by the presence of AITs when compared to the overall risk reductions achieved by the presence, absence and/or effectiveness of all other security measures. We start assessing risk reduction by developing a simple systems model of existing and new (AITs) aviation security measures. For a suicide bomber to succeed in downing a commercial airliner requires that all stages of the planning, recruiting and implementation of the plot go undetected. We will focus on three steps linked to aviation security:

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

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

1. success in boarding aircraft undetected – 10 layers of TSA security
2. success in detonating IED – trained flight crew and passengers
3. location and size of IED is sufficiently powerful to down the aircraft – aircraft resilience.

If any one of these security measures are effective, or the capabilities of the terrorist are lacking, then the terrorist will not be successful. We do not include all "layers" of TSA security such as checked baggage or canines, only those likely to stop a suicide bomber.

Figure 6 shows a reliability block diagram used to represent the system of foiling, deterring or disrupting an IED terrorist attack on a commercial airplane. If a terrorist attack is foiled by any one of these layers of security, then this is viewed as a series system. Assume:

- probability that a terrorist is successful in avoiding detection by any one of the 10 layers of pre-boarding TSA security is a high 90%
- passengers and trained flight crew have a low 50/50 chance of foiling a terrorist attempting to assemble or detonate an IED
- imperfect bomb-making training results in high 75% chance of IED detonating successfully
- aircraft resilience – a 75% chance of an airliner crashing if a bomb is successfully detonated.

For a series system where each event probability is statistically independent the probability of airliner loss is as in equation (9), next page.

The probability then that the plot is foiled, deterred or disrupted is 1 – Pr(airline loss) = 90.2% assuming existing security measures. Now, if the additional security measure is AITs, then we assume the probability of this technology in preventing:

- a suicide bomber boarding an aircraft is five times higher than any existing layer of TSA pre-boarding security, ie. 50%

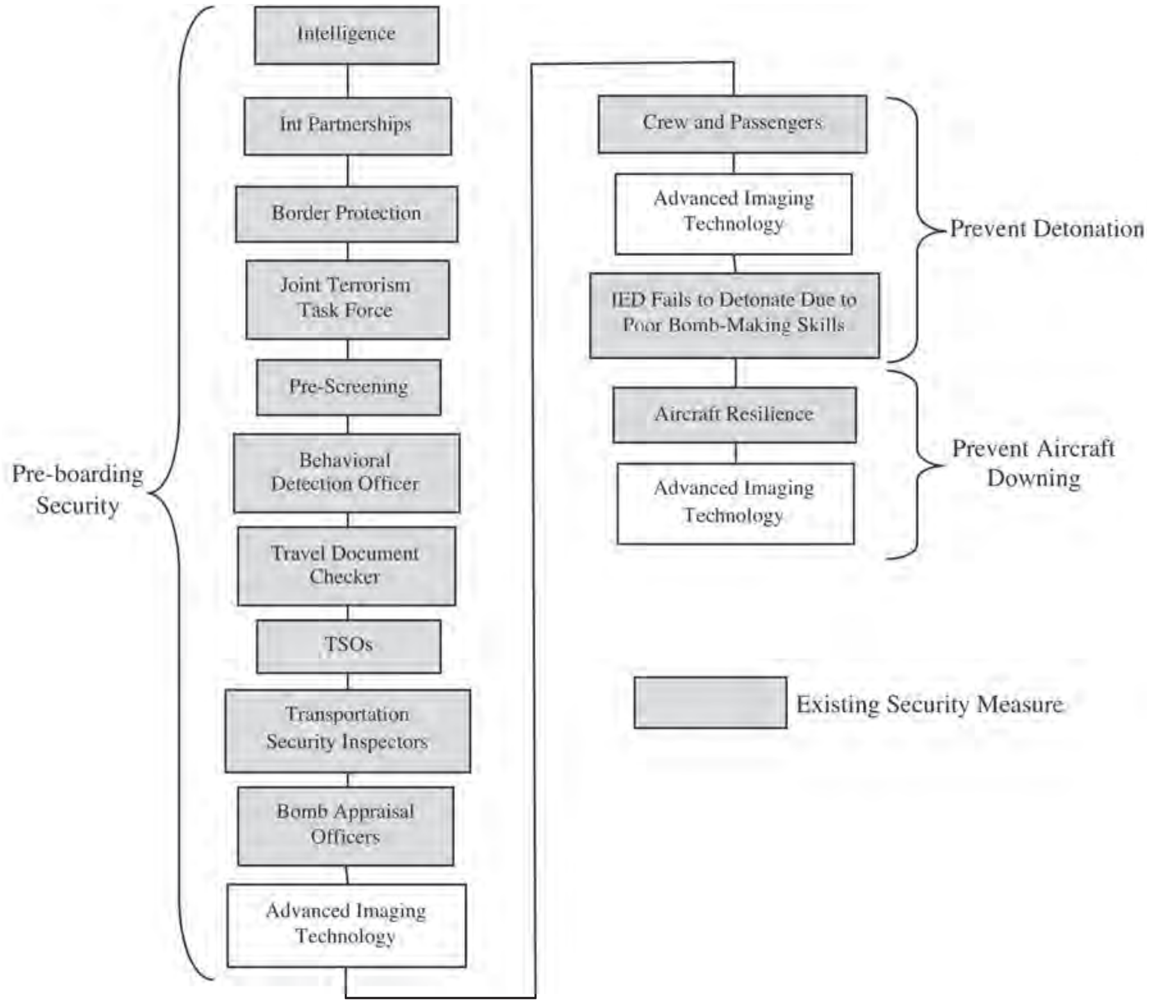
Pre-boarding Security
Intelligence
Int Partnerships
Border Protection
Joint Terrorism Task Force
Pre-Screening
Behavioral Detection Officer
Travel Document Checker
TSOs
Transportation Security Inspectors
Bomb Appraisal Officers
Advanced Imaging Technology
Crew and Passengers
Advanced Imaging Technology
IED Fails to Detonate Due to Poor Bomb-Making Skills
Prevent Detonation
Aircraft Resilience
Advanced Imaging Technology
Prevent Aircraft Downing
▨ Existing Security Measure

Figure 6: Reliability block diagram of existing (shaded) and enhanced aviation security measures with advanced imaging technology.

$$\begin{aligned}\Pr(\text{airliner loss}) = \prod_{i=1}^{10} &\Pr(\text{non-detection for preboarding security measure } i)\\ &\times\Pr(\text{Passengers/Crew non-detection})\\ &\times\Pr(\text{IED detonates successfully})\\ &\times\Pr(\text{aircraft downed by IED detonation})\\ &=(0.9)^{10}\times 0.5\times 0.75\times 0.75 = 9.8\%\end{aligned} \qquad (9)$$

- a suicide bomber from successfully detonating an IED is 50% because AITs may deter a terrorist from using more reliable, but more detectable, detonator
- in preventing an IED from being sufficiently large to down the aircraft is 50%.

Again assuming a series system, and since Pr(AIT effectiveness) is 50%, the probability that a terrorist plot will not be foiled, disrupted or deterred by AITs is [1 – Pr(AIT effectiveness)]^3 = (1 – 0.5)^3 = 12.5% and so probability of airliner loss is now calculated as 9.8 × 12.5% = 1.2%. Hence, the probability of preventing a terrorist attack and the downing of an airliner is now 100 – 1.2 = 98.8% due to AITs. The additional risk reduction from this single security measure is ΔR = 98.8 – 90.2 = 8.6%. This is the risk reduction in stopping a suicide bomber boarding a plane in the US, detonating it successfully or the explosive energy is insufficient to down the aircraft.

While we have tried to err on the generous side – ie. towards improving the cost-effectiveness of full-body scanners – we recognise that the probability estimates for effectiveness of security measures are uncertain. Since there are uncertainties with quantifying risk reduction a sensitivity analysis is needed to assess robustness of results. For example, using the figures above, the best case scenario is that AITs are 100% effective in eliminating this remaining risk then the best case risk reduction is ΔR = 9.8%. If AITs are less effective than assumed above, but still twice as effective than any existing layer of TSA pre-boarding security [Pr(AIT effectiveness) = 20%], then risk reduction is reduced to 4.8%. Lower and upper bound risk reductions may thus be 5% and 10%, respectively, with a mean of ΔR = 7.5%.

Using this data, Stewart & Mueller (2011) utilised equation (1) to assess the cost-effectiveness of AITs. An expected value cost-benefit analysis showed that the minimum attack probability for full body scanners to be cost-effective is Pr(T) = 61.5% per year. A full probabilistic analysis then found that the mean rate of attack needs to exceed 1.6 to 3.3 attacks per year to be 90% certain that AITs are cost-effective. See Stewart & Mueller (2011) for further details, and Stewart & Mueller (2008a; 2008b) for cost-benefit studies of air marshals (unlikely to be cost-effective) and hardening of cockpit doors (highly cost-effective) for US and Australian aviation security.

6 PRACTICAL IMPLEMENTATION: BUILDING PROTECTION FROM VBIED

To illustrate the benefits of probabilistic terrorism risk assessment models an institutional building subject to a terrorist VBIED is considered (Stewart, 2010a). The illustrative example will show under what combination of risk reduction, and fatality and damage costs the fatality and failure risks the protective measures would be cost-effective.

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 (Lakamp & McCarthy, 2003). In this case, measures to protect the building from VBIEDs 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), 2 (medium) and 3 (high terrorist threats), and two types of loss attributes j = 1 (direct physical damage) and 2 (fatalities). The net benefit from equation (1) is rewritten for this example as:

$$E_b = \sum_{i=1}^{3}\sum_{j=1}^{2}\Pr(T_i)\Pr(H_i|T_i)\Pr(L_j|H_i)L_j\Delta R_i - C_{security} \qquad (10)$$

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), and ΔR_i is the percentage reduction in risk due to CT protective measures for the ith threat. We assume that C_B = 0 and Pr(H_i | T_i) = 1.0.

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 threat probability Pr(T_i) is the product of probability of a terrorist attack (p_{attack}) and the relative threat probability given an attack Pr(T_i | attack). 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 6). Stewart (2011)

Table 6: Probabilistic models for hypothetical threats and losses (Stewart, 2010b). Note, probability distributions censored at 0.0 and 1.0.

Threat i	**Relative threat probability $\Pr(T_i \mid \text{attack})$**	**Probability of physical damage $\Pr(L_1 \mid H_i)$**			**Probability of fatalities $\Pr(L_2 \mid H_i)$**		
		Mean	**COV**	**Distribution**	**Mean**	**COV**	**Distribution**
1 (low)	0.6	0.25	0.1	Lognormal	0.10	0.25	Lognormal
2 (medium)	0.3	0.80	0.1	Lognormal	0.25	0.25	Lognormal
3 (high)	0.1	1.00	–	–	0.50	0.25	Lognormal

Table 7: Probabilistic models for hypothetical risk reduction (Stewart, 2010b).

Threat i	**Risk reduction ΔR_i**		
	Mean	**COV**	**Distribution**
1 (low)	90%	0.064	Uniform [80-100]
2 (medium)	65%	0.089	Uniform [55-75]
3 (high)	50%	0.115	Uniform [40-60]

has shown that the probability of building occupant fatality given a terrorist attack $\Pr(L_2 \mid H_i)$ varies from 0.0003 to 0.45 and so $\Pr(L_2 \mid H_i)$ 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 6 shows their assumed statistical parameters and probability distributions. Note that a COV of 0.25 represents a 95% confidence interval of approximately ±50% about the mean value.

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 random variables; see table 7, where it is assumed that the risk reduction is accurate to ±10%.

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 & 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 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 et al, 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 per year.

The net benefit is calculated from equation (10) using MCS analysis for a range of attack probabilities. Figure 7 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 7. With reference to figure 7 it is clear that if p_{attack} = 10^{-2}/building/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 7 shows that there is only a 35% probability that protective measures are cost-effective (ie. $\Pr(E_b) > 0$). Figure 8 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

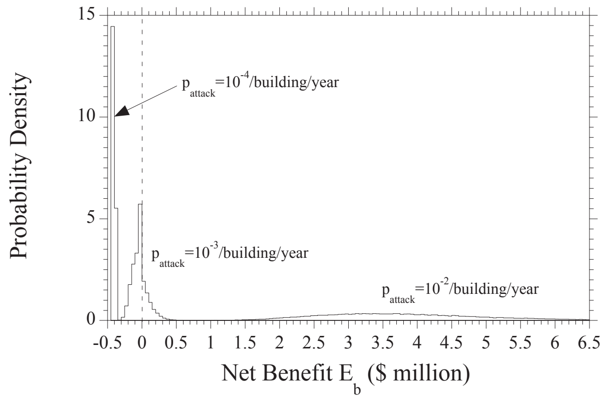

Figure 7: Histograms of annual net benefit (E_b) for institutional building, for attack probabilities of 10^{-2}, 10^{-3} and 10^{-4} per year.

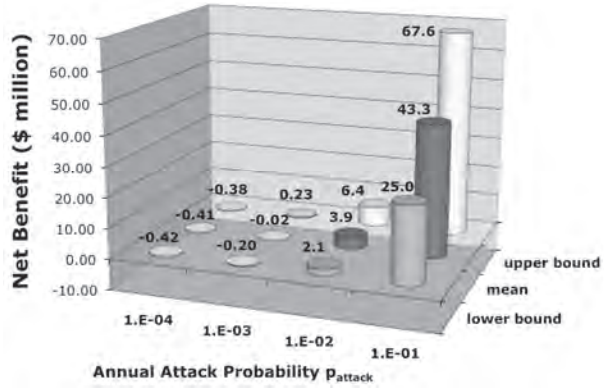

Figure 8: Annual net benefit (E_b) for institutional building.

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) suggested 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).

7 CONCLUSIONS

Since there is uncertainty associated with terrorist threats, structural and system response, effectiveness of CT 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) RC structural systems; (iii) full-body scanners used at airports in the United States; and (iv) buildings subject to a terrorist VBIED. The illustrative examples highlighted the research capabilities at the University of Newcastle, and identified research challenges to be faced in the future.

ACKNOWLEDGEMENTS

The support of the Australian Research Council is gratefully acknowledged. Yufeng Shi appreciates the financial support provided by the China Scholarship Council and the University of Newcastle. Matthew Grant appreciates the support of the Royal Australian Air Force and the University of Newcastle. 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.

Cox, L. A. 2009, "Improving Risk-Based Decision-Making for Terrorism Applications", *Risk Analysis*, Vol. 29, No. 3, pp. 336-341.

Department of Defense, 1995, "MIL-HDBK-217F Reliability Prediction of Electronic Equipment Notice 2", Washington, DC.

Department of Homeland Security (DHS), 2011, "FY2011 Budget in Brief", Washington, DC.

Dillon, R. L., Liebe, R. & Bestafka, T. 2009, "Risk-based Decision Making for Terrorism Applications", *Risk Analysis*, Vol. 29, No. 3, pp. 321-335.

Eamon, E. 2007, "Reliability of concrete masonry unit walls subjected to explosive loads", *Journal of Structural Engineering*, ASCE, Vol. 133, No. 7, pp. 935-944.

Ellingwood, B. R. 2006, "Mitigating Risk from Abnormal Loads and Progressive Collapse", *Journal of Performance of Constructed Facilities*, Vol. 20, No. 4, pp. 315-323.

Ellingwood, B., Galambos, T. V., MacGregor, J. G. & Cornell, C. A. 1980, *Development of a Probability Based Load Criterion for American National Standard A58*, NBS Special Publication 577, US Govt. Printing Office, Wash., DC.

Grant, M. & Stewart, M. G. 2011, "System and Reliability Modelling of Improvised Explosive

Devices", *PARARI 2011 – 10th Australian Explosive Ordnance Symposium*, Brisbane, 8-9 November.

Hao, H., Stewart, M. G., Li, Z.-X. & Shi, Y. 2010, "RC Column Failure Probabilities to Blast Loads", *International Journal of Protective Structures*, Vol. 1, No. 4, pp. 571-591.

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

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

Kingery, C. N. & 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. & McCarthy, G. H. 2003, *A Cost-Benefit Analysis of Security at the Naval Postgraduate School*, MBA Professional Report, Naval Postgraduate School, Monterey, California.

Livermore Software Technology Corporation, 2011, *LS-DYNA (Version 971) Finite element software for nonlinear dynamic analysis of inelastic structures*, Livermore, CA, USA, www.lstc.com/lsdyna.htm.

Low, H. Y. & Hao, H. 2001, "Reliability analysis of reinforced concrete slabs under explosive loading", *Structural Safety*, Vol. 23, No. 2, pp. 157-178.

Low, H. Y. & Hao, H. 2002, "Reliability analysis of direct shear and flexural failure modes of RC slabs under explosive loading", *Engineering Structures*, Vol. 24, pp. 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. & Stewart, M. G. 2011a, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*, Oxford University Press, New York and Oxford, UK, September.

Mueller, J. & Stewart, M. G. 2011b, "The Price is Not Right: The U.S. spends too much money to fight terrorism", *Playboy,* Vol. 58, No. 10, pp. 149-150.

Netherton, M. D. & 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*, Vol. 36, No. 12, pp. 1346-1354.

Netherton, M. D. & Stewart, M. G. 2010, "Blast Load Variability and Accuracy of Blast Load Prediction Models", *International Journal of Protective Structures*, Vol. 1, No. 4, pp. 543-570.

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

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

Robinson, L. A., Hammitt, J. K., Aldy, J. E., Krupnick, A. & Baxter, J. 2010, "Valuing the Risk of Death from Terrorist Attacks", *Journal of Homeland Security and Emergency Management*, Vol. 7, No. 1.

Shi, Y., Hao, H. & Li, Z.-X. 2008, "Numerical Derivation of Pressure-Impulse Diagrams for Prediction of RC Column Damage to Blast Loads", *International Journal of Impact Engineering*, Vol. 35, No. 11, pp. 1213-1227.

Stewart, M. G. 2008, "Cost-Effectiveness of Risk Mitigation Strategies For Protection of Buildings Against Terrorist Attack", *Journal of Performance of Constructed Facilities*, ASCE, Vol. 22, No. 2, pp. 115-120.

Stewart, M. G. 2010a, "Acceptable Risk Criteria for Infrastructure Protection", *International Journal of Protective Structures*, Vol. 1, No. 1, pp. 23-39.

Stewart, M. G. 2010b, "Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-Terrorism Protective Measures for Infrastructure", *International Journal of Critical Infrastructure Protection*, Vol. 3, No. 1, pp. 29-40.

Stewart, M. G. 2011, "Life Safety Risks and Optimisation of Protective Measures Against Terrorist Threats to Infrastructure", *Structure and Infrastructure Engineering*, Vol. 7, No. 6, pp. 431-440.

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

Stewart, M. G. & Mueller, J. 2008a, "A Risk and Cost-Benefit and Assessment of U.S. Aviation Security Measures", *Journal of Transportation Security*, Vol. 1, No. 3, pp. 143-159.

Stewart, M. G. & Mueller, J. 2008b, "A Cost-Benefit and Risk Assessment of Australian Aviation Security Measures", *Security Challenges*, Vol. 4, No. 3, pp. 45-61.

Stewart, M. G. & 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*, Vol. 8, No. 1, Article 30.

Stewart, M. G. & Netherton, M. D. 2008, "Security Risks And Probabilistic Risk Assessment of Glazing Subject to Explosive Blast Loading", *Reliability Engineering and System Safety*, Vol. 93, No. 4, pp. 627-638.

Stewart, M. G., Netherton, M. D. & Rosowsky, D. V. 2006, "Terrorism Risks and Blast Damage to Built Infrastructure", *Natural Hazards Review*, ASCE, Vol. 7, No. 3, pp. 114-122.

Stewart, M. G., Ellingwood, B. R. & Mueller, J. 2011a, "Homeland Security: A Case Study in Risk Aversion for Public Decision-Making", *International Journal of Risk Assessment and Management*, Vol. 15, No. 5/6, pp. 367-386.

Stewart, M. G., Shi, Y. & Zhi, X. 2011b, "Structural Reliability Analysis of Reinforced Concrete Columns Subject to Explosive Blast Loading", *9th International Conference on Shock & Impact Loads on Structures*, Fukuoka, 16-18 November.

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

Twisdale, L. A., Sues, R. H. & Lavelle, F. M. 1994, "Reliability-based design methods for protective structures", *Structural Safety*, Vol. 15, No. 1-2, pp. 17-33.

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

von Winterfeldt, D. & O'Sullivan, T. M. 2006, "Should WE Protect Commercial Airplanes Against Surface-to-Air Missile Attacks by Terrorists?", *Decision Analysis*, Vol. 3, No. 2, pp. 63-75.

Willis, H. & 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*, Vol. 28, No. 2, pp. 325-339.

Wolstenholme, L. C. 1999, *Reliability Modelling – A Statistical Approach*, Chapman & Hall/CRC, UK.

MARK STEWART

Professor Mark G. Stewart is Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. He is co-author of *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (Oxford University Press, 2011) and *Probabilistic Risk Assessment of Engineering Systems* (Chapman & Hall, 1997), as well as more than 300 technical papers and reports. He has more than 25 years of experience in probabilistic risk and vulnerability assessment of infrastructure and security systems that are subject to man-made and natural hazards. Since 2004, Mark has received extensive ARC support to develop probabilistic risk-modelling techniques for infrastructure subject to military and terrorist explosive blasts and cost-benefit assessments of counter-terrorism protective measures for critical infrastructure. In 2011, he received a five-year Australian Professorial Fellowship from the ARC to continue and to extend that work.

MICHAEL NETHERTON

Michael D. Netherton is a Lecturer in the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. He received his MSc (Weapons Effects on Structures) in 2000 from the Royal Military College of Science in the UK and is currently a part-time PhD candidate at the University of Newcastle. He served 23 years in the Royal Australian Air Force, retiring in 2004 as a Squadron Leader specialising in the provision of engineering advice for the targeting of enemy infrastructure and systems. He saw active service across the Middle East in 2003 where he was the Senior Australian Representative within the Combined (USA, UK and Australia) Weapons Effectiveness Assessment Team.

YUFENG SHI

Yufeng Shi is a research student in the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. His PhD topic is structure reliability analysis of reinforced concrete structures subject to explosive blast loading. He received his MSc (Structural Engineering) in 2010 from Hunan University in China. In 2008, he was a member of the study team for the 2008 Sichuan earthquake, which was organised by Hunan University.

MATTHEW GRANT

Matthew Grant is a Royal Australian Air Force Armament Engineer and postgraduate student at the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. Matthew has over 15 years' experience within the Royal Australian Air Force, including experience as a RAAF IEDDO. After graduating from Cranfield University's Masters of Science (Explosive Ordnance Engineering) program in 2006, Matthew became the Deputy Chief Engineer for the Australia Defence Force's Non-Guided Munitions inventory.

JOHN MUELLER

John Mueller is a Senior Research Scientist at the Mershon Center for International Security Studies and Professor of Political Science at Ohio State University, Columbus, Ohio. He is the author of over a dozen books, several of which have won prizes. Among the most recent of these are *The Remnants of War* (2004), *Overblown* (2006), *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda* (2010), and *War and Ideas* (2011). He has also edited the web-book *Terrorism Since 9/11: The American Cases* (2011). He has published numerous articles in scholarly journals and general magazines and newspapers, is a member of the American Academy of Arts and Sciences, and has been a John Simon Guggenheim Fellow. He is currently a Cato Senior Fellow at the Cato Institute in Washington, DC.