A systems model for probabilistic risk assessment of improvised explosive device attacks

Matthew Grant* and Mark G. Stewart

Centre for Infrastructure Performance and Reliability,
The University of Newcastle,
New South Wales, 2308, Australia
E-mail: Matthew.J.Grant@uon.edu.au
E-mail: Mark.Stewart@newcastle.edu.au
*Corresponding author

Abstract: Due to their improvised nature, the variability in the design, manufacture and operation of most improvised explosive devices (IEDs) defy the traditional paradigms used to assess the effectiveness of conventional munitions. Thus, IEDs are complex socio-technical systems to model. To compensate for inadequacies in model design or data deficiencies, expert judgement and subjective probability assignments are often employed. The paper aims to reduce this reliance by developing an IED probabilistic risk assessment model using a systems model for IED attacks based on IED device reliability and characterising the human aspects of IED attack operational effectiveness from existing terrorism databases. This model can then be used to develop an automated model for IED probabilistic risk assessment that can be used towards informing military applications such as operations planning and war-gaming, and civil applications such as security risk management (including event planning), protective construction requirements, and insurance assessments. It was found that the risk of loss (fatalities, property damage) is influenced more by operational aspects (such as target selection, IED placement and attack timing) than the technical aspects of the device design and manufacture.

Keywords: improvised explosive device; IED; terrorism; probabilistic risk assessment; human performance assessment.

Reference to this paper should be made as follows: Grant, M. and Stewart, M.G. (2012) 'A systems model for probabilistic risk assessment of improvised explosive device attacks', *Int. J. Intelligent Defence Support Systems*, Vol. 5, No. 1, pp.75–93.

Biographical notes: Matthew Grant is a post-graduate student at the Centre for Infrastructure Performance and Reliability, The University of Newcastle in Australia. He has over 15 years experience within the Royal Australian Air Force as an Armament Engineer, including experience as a RAAF Improvised Explosive Device Disposal Officer. He is currently the Chief Engineer Munitions for the Australian Defence Force.

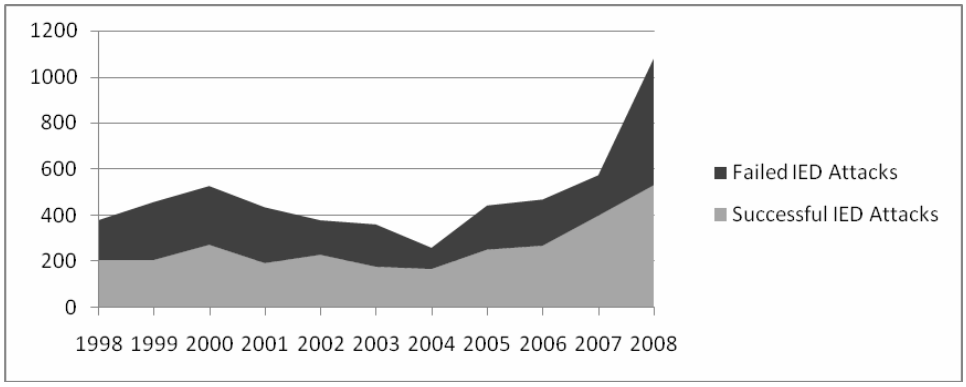
Mark G. Stewart is a Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. He is the author of *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (Oxford University Press, 2011), and more than 300 technical papers. He has received

extensive Australian Research Council (ARC) support to develop probabilistic risk-modelling techniques for infrastructure subject to explosive blasts and cost-benefit assessments for critical infrastructure counter-terrorism protective measures. In 2011, he received a five-year Australian Professorial Fellowship from the ARC to continue and extend that work.

1 Introduction

Terrorist threats against civilian and military infrastructure, particularly buildings, bridges, pipelines, energy distribution and aviation infrastructure, transcend national boundaries and appear to be an increasing threat to national sovereignty and international security and trade. This is evidenced by recent terrorist attacks including Manchester and London city centres (1992, 1993, 1996, 2005), US 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 aircraft suicide bombing attempt (2009). Improvised explosive devices (IEDs), often through the use of suicide tactics and vehicle borne improvised explosive devices (VBIEDs) against buildings and transport infrastructure, continue to be the terrorist weapon of choice with seemingly increasing frequency (see Figure 1).

Figure 1 Global IED attacks 1998–2008 (without Iraq and Afghanistan)



Source: Data derived from START (2010)

Research into improving the fidelity of models to inform decision makers for the optimal allocation of counter-terrorism funding has increased significantly. The utility of probabilistic risk assessment (PRA) was recognised early in this process, with formative research being conducted by Garrick et al (2004), and later system models being developed by Aven (2007), Dillon-Merrill et al. (2009), Stewart (2008, 2010), and Stewart and Mueller (2011). Our research will develop a PRA model for the specific threat of an IED attack.

2 PRA for IED attack

2.1 Challenges for PRA for IED attack

IEDs can be surprisingly simple devices to design and manufacture, ranging from a small pipe bomb, with potential to cause small numbers of casualties and minor damage to surrounding structures, to a large truck bomb capable of causing massive damage and loss of life (National Academies and the Department of Homeland Security 2010). However, since they are typically 'home made' and placed under imperfect conditions, their probability of initiation and subsequent success can be highly uncertain, as evidenced in the failed 21/7 London, 2007 Glasgow, 2009 Christmas Day Northwest Airlines aircraft and 2010 Times Square attempts. Indeed, when we consider IED incidents globally, we discover that 52% of incidents could be described as successful[1], however, rates of success vary significantly across regions (Western[2] 21%, Middle East and North Africa[3] 64%) and across perpetrator type (individual 27%, criminal 35%, terrorist organisations 53%, insurgent organisations 73%).[4]

These uncertainties will affect damage and fatality risk predictions and the utility of subsequent counter-terrorism decisions. Characterising these uncertainties using stochastic (probabilistic) methods is a logical step, which will lead to estimates of system reliability and risk. To date, the probabilistic and reliability analyses that have been carried out for infrastructure systems subject to explosive blast loading have been of very limited scope, have lacked realistic detail and relied upon expert opinion. This is in contrast to the approach that has been used very successfully for other man-made and natural hazards (e.g., Stewart and Melchers 1997, Stewart, 2010). 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 (e.g., Stewart, 2008, 2010; Stewart and Mueller, 2011).

Expert opinion is often used where there remains a paucity of data to generate quantitative conclusions. Many factors associated with IED threats and vulnerability are grouped into this category, primarily because of their diversity – of motive, design, manufacture and response – and that they are derived from issues pertaining to human factors. The utility, and also the flaw, regarding the use of expert opinion is that you gain the experience of the individual – something of limited utility in an environment depending on the preferences of an unpredictable adversary (Levine, 2012). Assuming that the experience and information that an expert retains is relevant to the case under consideration, all expert opinion remains subjective (Taylor-Adams and Kirwan, 1997) introducing the opportunity for bias and prejudice into assessments (Forester et al., 2003; Koblentz, 2011) in addition to significant variability between experts (Firmino et al., 2006; Park and Lee, 2008). Forester et al. (2003) cite research indicating that humans perceptions of information are selective, making us poor at estimating probability and uncertainty, particularly as problems become more complex. Our research aims to develop a quantitative reliability paradigm to establish the materiel response of an IED to a suitable initiation impetus without resorting to expert opinion.

The likelihood and extent of an IED creating a damage effect (that is, generation of a thermal effect, blast effect, fragmentation effect or combination of these effects capable of inflicting casualties or damaging property/infrastructure) and subsequent success requires systems modelling techniques where each task is identified and its influence on subsequent tasks represented by logic diagrams. Reliability data needed includes the

mean and variance of components and successful task performance. As the tasks required to manufacture and initiate an IED often take place under stressful and imperfect conditions then it can be expected that task performance will not always be 100% reliable. Indeed, Stewart and Melchers (1997) report that human errors can cause up to 90% of failures for engineering systems.

This paper builds on our previous research (Grant and Stewart, 2011; noting that this paper provides a significant revision of our original model) which investigated the likelihood of an IED creating a damage effect, using functional flow block diagrams (FFBDs) to model an IED design and its manufacture for simple (pipe bomb), medium (mobile phone initiated VBIED) and complex (improvised mortar) IEDs. This paper concentrates on developing the PRA framework and modelling the operational aspects of an IED attack (such as planning for the attack, target selection, IED selection, placement of the IED, and timing the initiation of the IED). These functions can later be used to develop an automated model for IED PRA that can be used towards informing military applications such as operations planning and war-gaming, and civil applications such as security risk management (including event planning), protective construction requirements, and insurance assessments.

2.2 IED PRA model

The PRA for an IED attack can be facilitated through tailoring of a general terrorism PRA model. Modification of the PRA model developed by Stewart (2010) to address the IED attack context provides for the modelling of risk (or expected losses) as:

$$Risk = \sum_{T}\sum_{H}\sum_{L} \Pr(T)\Pr(H \mid T)\Pr(L \mid H)L \tag{1}$$

where

- $\Pr(T)$ is the annual threat probability, that is the probability that a particular target is attacked by a particular terrorist/criminal organisation with a particular type/size of IED.
- $\Pr(H|T)$ is the conditional probability of a hazard given occurrence of the threat. That is, it is a representation of the efforts of the attacker, the probability that a specific IED creates a specific damage effect of a specific yield.
- $\Pr(L|H)$ is the conditional probability of a loss given occurrence of the hazard. This is a respresentation of the combination of target characteristics that influence the result of an IED attack, for example, building construction/hardening, population density and the effectiveness of security measures.
- L is the loss or consequence that is the measurement of casualties and infrastructure damage and exposure arising from realisation of a particular hazard.
- The summation signs in equation (1) refer to the number of possible threat scenarios, hazard levels[5] and losses. If an attack is completely successful then $\Pr(H|T)\Pr(L|H) = 1.0$.

Risk as expressed in equation (1) thus consists of the product of likelihood of a successful attack against a target and the loss or consequence if a that target is attacked. Risk may also be expressed as the product of threat Pr(T), hazard Pr($H|T$), vulnerability Pr($L|H$), and impact L. No matter the precise formulation, the development of likelihood and consequence are a difficult proposition due to the diversity of motive and opportunity for the use of IEDs. However, these aspects of the model lend themselves to quantitative analysis through a multi-disciplinary approach, including consideration of soft aspects such as the cultural influences, personnel proficiencies and organisational maturity, along with technical aspects related to the IED design, its manufacture and reliability – the topic of the present paper – and the characteristics of the target.

2.3 Modelling hazard likelihood Pr(H|T)

Whatever their purpose and complexity, an IED is largely constructed from commonly available components. In principle, the reliability of an IED can be computed from the known reliabilities of their components, such as those identified in MIL-HDBK-217 (Department of Defence, 1995) and DEF STAN 00-42 (Ministry of Defence, 2008). However, unlike conventional military hardware, the reliability of IEDs cannot be calculated through such standard philosophies because you cannot assume that IEDs have been designed, manufactured and utilised in accordance with standard systems engineering practices by competent military personnel. As a result, component reliability can only be a partial contributor towards any model to be used for the PRA of IED threats.

The variability in IED effectiveness is thought to be caused by the disparate nature of improvised munitions development and their deployment. Some terrorists and insurgents are supported by a large para-military organisation having reach-back to knowledge and experience, whilst others are effectively self-starters relying upon their individual knowledge and experience supported by open-source media (Kenney, 2010; Speckhard, 2011; Brooks, 2011). This, combined with a disparate range of objectives, makes reliability/success predictions very complex and challenging to quantify.

The threat of IED attack, and hence development of a PRA, needs to be treated through a systems model, using an alternate paradigm to conventional munitions reliability. The effects of design, environment, manufacturing and operational considerations can be independently considered and overlaid as performance shaping functions (PSFs) that introduce additional variability in traditional reliability functions to optimise their fidelity. This is particularly pertinent as PSFs primarily introduce the effects of human interaction within the system and these influences cannot be derived from engineering standards alone. To identify potential PSFs a systems engineering approach using FFBDs has been adopted. The PSFs can then be used to influence the reliability function resulting from the integration of IED components.

Our model for Pr($H|T$) considers the combination of:

1 the reliability of the IED

2 the human factors affecting the design and manufacture of the IED

3 the human factors encompassing the operational proficiency of the attacker.

These aspects are all within the power of the attacker to influence. The combination of these considerations results in:

$$\Pr(H|T) = PSF_{D\&M} \times R \times PSF_{Ops} \quad (2)$$

where

- $PSF_{D\&M}$ is the PSF for design and manufacture of an IED
- R is the baseline reliability of the IED (i.e., IED design and manufacture to military standards)
- PSF_{Ops} is the PSF for the operational aspects of the IED attack.

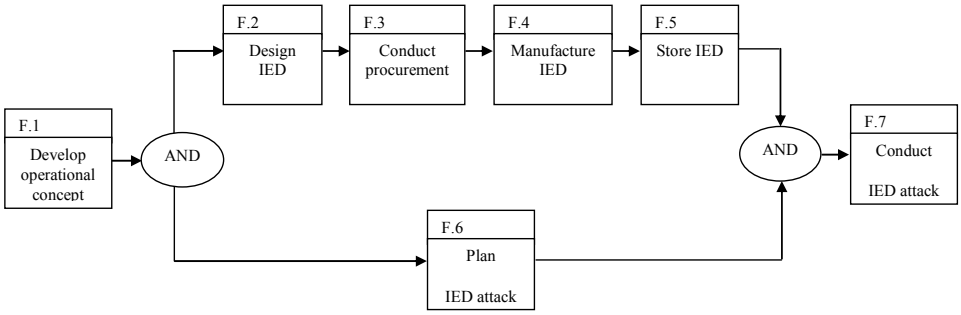
2.4 Developing PSFs using FFBDs

A FFBD was developed for a typical IED attack. FFBDs were chosen as they are a basic tool that is commonly used in systems engineering applications (Faulconbridge and Ryan, 2005), particularly in the aviation industry and for defence major capital acquisitions. FFBDs provide a visual representation of functional flow, being a multi-tier, time-sequenced, step-by-step diagram of a system's functional flow – in our case for the creation of a terminal effect (i.e., initiation) by an IED which defines the hazard and so Pr(H|T). In our context, the functional flow steps may include combinations of hardware, software, personnel, facilities and procedures. Each function is shown with respect to its logical relationship to the execution and completion of other functions (Faulconbridge and Ryan, 2005).

The highest level function *Create Damage Effect (F.0)*, describing the process towards achieving IED initiation at an appropriate time and place (i.e., the target), is depicted in Figure 2. It was developed using the US Federal Aviation Administration's standard Functional Symbology with minor modification to suit the application (ATO Operations Planning, 2006). The first authors' experience as an IED Disposal Officer and a professional engineer were used to establish this highest level function such that it would maintain utility for a diverse range of multi-layer modelling scenarios, an example of such a model being that proposed by Weiss et al. (2011). Subsequent devolution provides a functional hierarchy which can be used to develop PSFs (and their derivative influences) and identify where we can employ probability density functions (PDFs) to represent $PSF_{D\&M}$ and PSF_{Ops}, contributing to our model for Pr(H|T). Within the functional hierarchy we can group the key factors affecting functional blocks, those that contribute to the successful function of an IED and creation of a damage effect, into broad categories. It is these factors that are generally very difficult to appreciate and assess in contributing to the context of threat success, usually resulting in the use of expert opinion and judgement – particularly as significant aspects of these key factors concern human performance and are affected by attributes such as culture, education, training and experience.

From Figure 2, we can identify aspects that contribute towards our total model at equation (1). Design and manufacture $PSF_{D\&M}$ is aligned primarily with the uppermost (F.2, F.3, F.4 and F.5) functional flow of Figure 2, the design, manufacture and storage of an IED in preparation for an attack. Operational aspects PSF_{Ops} can be associated primarily to F.1, F.6 and F.7. Previous work (Grant and Stewart, 2011) concentrated on devolving F.2 to F.5, and identifying PSFs relating to $PSF_{D\&M}$.

Figure 2 FFBD – *F.0 Create Damage Effect*



This paper focuses on the human factors influencing the operational aspects of an IED Attack, although a summary of the results from Grant and Stewart (2011) are provided below. This provides the reader with an awareness of the research conducted to date, and how these have been built upon to create our IED systems model.

2.5 The global terrorism database

In order to progress our model we require a large body of IED incident data, however, access to such data is an acknowledged inhibitor to progressing research into IEDs and their deployment due to security classification constraints (Dietz, 2011). One open source database from which data is available, the global terrorism database (GTD), is collated by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland (START, 2010). The GTD is an open-source database including information on terrorist events around the world from 1970 through 2010. For each of the more than 98,000 GTD incidents, information is available on the date and location of the incident, the weapons used and nature of the target, the number of casualties, and any known groups or individuals responsible. As identified by Barker (2011) and Sheehan (2012), media reporting in particular is a problematic source of IED incident data as it generally relies upon eyewitness or journalist reports with little expertise in IED operations. Additionally, there is the potential for under-reporting of incidents (particularly device failures) either through censorship, lack of newsworthiness or lack of discovery; and it is difficult to attribute attack success criteria, particularly considering the diversity of motive and inability to accurately assess indirect costs (Enders and Olson, 2011).

It was noticed that GTD reporting was very sensitive in areas of high conflict, particularly Iraq and Afghanistan where there were significant discrepancies between GTD reporting and reporting from the US Military (Joint Improvised Explosive Defeat Organization, 2008). As a result, all incidents relating to Iraq and Afghanistan were removed from the database for analysis as they were considered a significant source of bias.

Additionally, conventional munitions using their fuzing system as designed were removed to ensure that these items did not bias the data and that only IEDs were incorporated into the dataset. The dataset was re-characterised based on our criteria for success (victim casualties, assassination victims killed and/or greater than USD$1 million

property damage), categorisation of the device, its operation, and the loss sustained from the incident.

Our results have been calculated using our system model, populated with data from the GTD.

2.6 Quantifying influence of IED design, manufacture and $PSF_{D\&M}$

Investigation of IED design and manufacture (F.2 to F.5 of Figure 2) were devolved into a function of the following PSFs (Grant and Stewart, 2011):

- design quality
- design education, training and experience
- manufacturing quality
- national culture
- manufacturing education, training and experience.

The hazard likelihood (damage effect) Pr($H|T$) was determined to be a product of the IED baseline reliability (R) (estimated as a single point estimate from assessed device complexity) and these PSFs. The GTD was used to provide the data necessary to identify the significance of PSFs towards influencing Pr($H|T$). Although the GTD does not have sufficient fidelity to assess the impacts of the discrete PSFs identified, there was sufficient fidelity to investigate Pr($H|T$) – noting that PSF_{Ops} was considered to be 1 due to data filtering ensuring that only devices that were appropriately placed being considered – as:

$$\Pr(\text{Initiation}) = f_{Cult} f_{Org} f_{DC} R = PSF_{D\&M} \times R \tag{3}$$

$$PSF_{D\&M} = f_{Cult} f_{Org} f_{DC} = \Pr(\text{Initiation}) / R \tag{4}$$

where

- Pr(Initiation) is the probability that an IED will initiate, a measure of its reliability
- f_{Cult} is the PSF associated with region, an indicator towards national culture
- f_{Org} is the PSF associated with organisational culture, an indicator towards design and manufacture quality
- f_{DC} is the PSF associated with design complexity, an indicator towards education, training and experience
- $PSF_{D\&M}$ is the PSF for design and manufacture of an IED
- R is the baseline reliability of the IED.

Given the broad nature of IED designs and implementations, Grant and Stewart (2011) used several typical IED configurations of differing design complexities – simple (pipe bomb), medium (mobile phone initiated VBIED) and complex (improvised mortar) – to represent R and for use in further calculations. 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 (Department of Defence, 2007), the UK (Ministry of Defence, 2008) and the USA (Reliability Information Analysis Centre & Data and Analysis Centre for Software and Defense Science Board, 2005), and representative mobile phone data (Cinque et al., 2007), to inform component reliabilities, is:

$$R = 0.9994 \times 0.999 \times 0.98 \times 0.97 \times 0.97 \times 0.999 = 0.92$$

Table 1 provides a summary of baseline IED reliabilities derived from conventional munitions' representative component reliability data for common IED designs. The baseline reliability assumes there are no errors in connecting components, storage of components, the device does not degrade with time through environmental factors, and assumes statistical independence of component reliabilities. Hence, R reflects the reliability of an IED designed and manufactured to military specifications and standards.

Table 1 also shows the probability that an IED of representative complexity will initiate (Pr(Initiation)) obtained from statistical analysis of the GTD. The $PSF_{D\&M}$ is obtained from equation (4) by dividing the Pr($H|T$) with baseline reliability R, see Table 2 for Global, Western and Middle East and North Africa regions.

Table 1 Global device complexity comparison to GTD and baseline IED reliability estimates

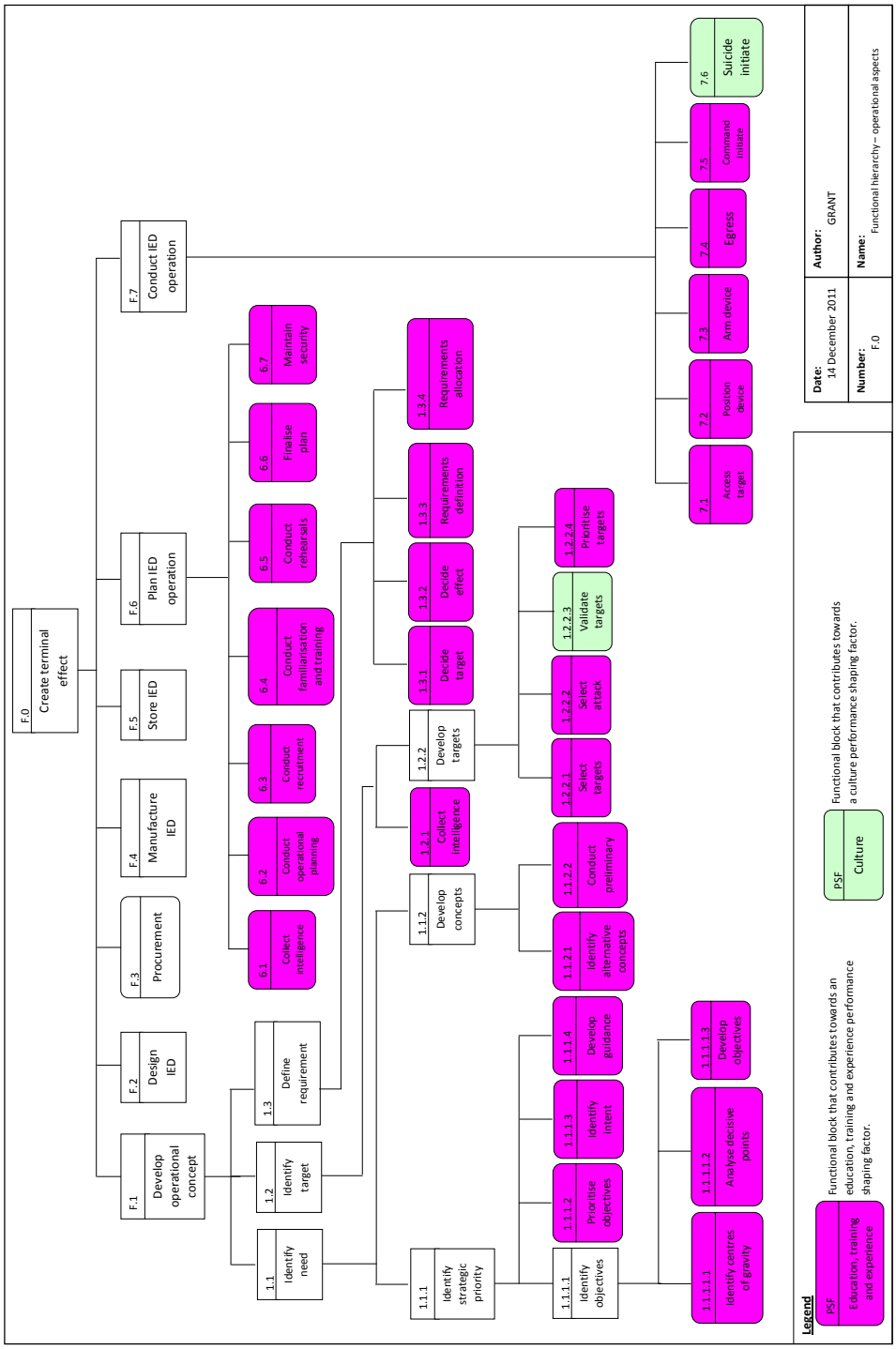
Device complexity	*Representative IED design*	*Probability of IED initiation Pr(Initiation)*[1]	*Baseline reliability R*
Unknown		0.97	-
Simple	Pipe bomb	0.92	0.93
Medium	Mobile phone initiated VBIED	0.95	0.92
Complex	Improvised mortar	0.78	0.91

Note: [1]Statistical analysis from GTD

Table 2 Derived $PSF_{D\&M}$ for regions of interest

Organisation	*Device complexity*	*Global $PSF_{D\&M}$*	*Western $PSF_{D\&M}$*	*Middle East and Nth Africa $PSF_{D\&M}$*
Individual	Simple	0.59	0.54	0.61
	Medium	0.70	0.52	-
	Complex	-	-	-
Criminal	Simple	→1	0.99	1
	Medium	0.97	0.96	1
	Complex	0.55	-	-
Terrorist organisation	Simple	0.98	0.86	0.99
	Medium	0.98	0.93	0.95
	Complex	0.91	0.76	1
Insurgent organisation	Simple	→1	-	1
	Medium	→1	-	1
	Complex	→1	-	1

Figure 3 Functional hierarchy – operational aspects of IED attack (see online version for colours)



There is considerable variability in IED Success between different regions, organisational types and device complexities. results given in Tables 1 and 2 suggest that, except in situations where lone perpetrators are involved or complex designs are attempted, $PSF_{D\&M}$ is a comparatively minor source of variability towards the probability of loss from an IED attack. For more details, including probabilistic estimates of loss (damage, casualties) due to IED initiation, see Grant and Stewart (2011). An objective of further research is to develop the single point estimates for IED reliability into probability distribution functions to ensure that appropriate assessments of variability for Pr($H|T$) can be achieved within the PRA model.

2.7 Developing operational PSF_{Ops}

The PSF_{Ops} is primarily dependent upon the operational aspects of an IED attack, the ability to plan an IED attack without drawing the attention of security elements, and subsequently conducting the IED attack effectively. Hence, PSF_{Ops} is primarily reliant upon F.1, F.6 and F.7 from Figure 2, the operational functions which provide for a successful IED attack.

The operational functions of the FFBD in Figure 2 were devolved to between Level 1 and Level 4, depending on the security implications of further devolving these functions, thus creating the functional hierarchy at Figure 3. F.1 Develop Operational Concept was developed using the Australian *Defence Capability Development Manual* (Department of Defence, 2006), the US *Joint Doctrine for Targeting* (Department of Defence, 2002) and Driels (2004). F.6 Plan IED attack was developed with the assistance of the US *Joint Doctrine for Targeting* and Kenney (2010), and F.7 Conduct IED attack was developed from the authors' knowledge and experience.

From the subsequent functional hierarchy (Figure 3) we could identify key PSFs affecting each functional block, and group these into broad categories. The major PSFs that influence the operational aspects of an IED attack were identified as:

1 education, training and experience

2 culture.

There is some inter-relationship between the PSFs identified – culture [national culture, organisation type (Minkov and Hofstede, 2011)] and education, training and experience (Yorks and Sauquet, 2003). In particular, organisational culture is expected to have a large impact on education, training and experience – the more proficient the organisation is at IED attacks, the greater experience is available to the organisation and the better equipped it is to train personnel.

3 Results – IED 'success' and estimation of probability of hazard Pr(H|T)

IED 'success' for this paper has been defined as an IED attack that causes victim casualties and/or USD$1 million or greater in property damage. Pr($H|T$) was quantified using the results from Grant and Stewart (2011) to describe $PSF_{D\&M}$. These results have been used with minor modification to account for an increase in fidelity to IED attack Success criteria for instances where IEDs were utilised to attempt assassination. In these

instances, IEDs were only considered successful if the intended victim were killed. Table 3 shows that $PSF_{D\&M} \times R$ remains very high.

As PSF_{Ops} relies upon the IED having the potential to create, or having created a damage effect, all incidences of IED failure due to technical problems were removed from consideration – these pertain to influencing $PSF_{D\&M}$. Other aspects, such as device detection and render safe by authorities, poor device selection or placement or accidental initiation of the IED were considered to be a normal part of an IED attack and were included within the dataset.

The limitations associated with the GTD constrained the fidelity of our model, however, we have been able to consider:

1 national culture

2 organisational culture as they impact PSF_{Ops}.

As discussed earlier, our PSFs have a good deal of interdependency, however, given the data limitations of the GTD this is the optimum fidelity that can be achieved without a dedicated database of incidents structured to the research. The quantification of PSF_{Ops} from the GTD for regions of interest is presented at Table 3. These regions were selected for investigation due to their similarity in casualty averages per incident where casualties arose (Global 20, Western 21.1, Middle East and North Africa 19.4, South America 16.1 and Russia and NIS 20.5).

The operational aspects PSF_{Ops} can be effectively estimated through filtering the data within the GTD. Effectively, given the GTD dataset and its reduction, we can consider that Pr($H|T$) is equivalent to the probability of IED Success for further discussion and conditional on Pr(T) = 1. These results are provided at Table 3 for both casualty and property losses.

Table 3 PSFs and IED success Pr($H|T$) for regions of interest, for all IED devices and organisational types

Region	*Pr(Initiation)* $(PSF_{D\&M}R)$	PSF_{Ops}		*Probability of hazard (IED success) Pr(H|T)*	
		Casualties	*Property*	*Casualties*	*Property*
Global	0.97	0.53	0.04	0.52	0.04
Western	0.89	0.21	0.06	0.19	0.05
Middle East and Nth Africa	0.99	0.66	0.04	0.65	0.04
South America	0.98	0.41	0.13	0.40	0.13
Russia and NIS	0.98	0.61	0.04	0.59	0.04

As discussed earlier, casualties arising from IED attack and property/infrastructure damage need to be considered independently to develop an appropriate assessment of losses. Categorisation of incidents from the GTD allowed us to identify the frequency of casualties arising from incidents to generate distributions for loss (Figures 4 and 5) correlated to Pr($H|T$). We did not discriminate between casualties (dead or wounded), although this could be achieved to provide an additional level of fidelity. Additionally, further fidelity could be achieved through investigating distributions for loss across different PSFs, an example is provided in Figure 6 comparing loss distributions for criminal and terrorist organisations.

Figure 4 Relationship between Pr($H|T$) and Pr($L|H$)L for casualties arising from IED attack (see online version for colours)

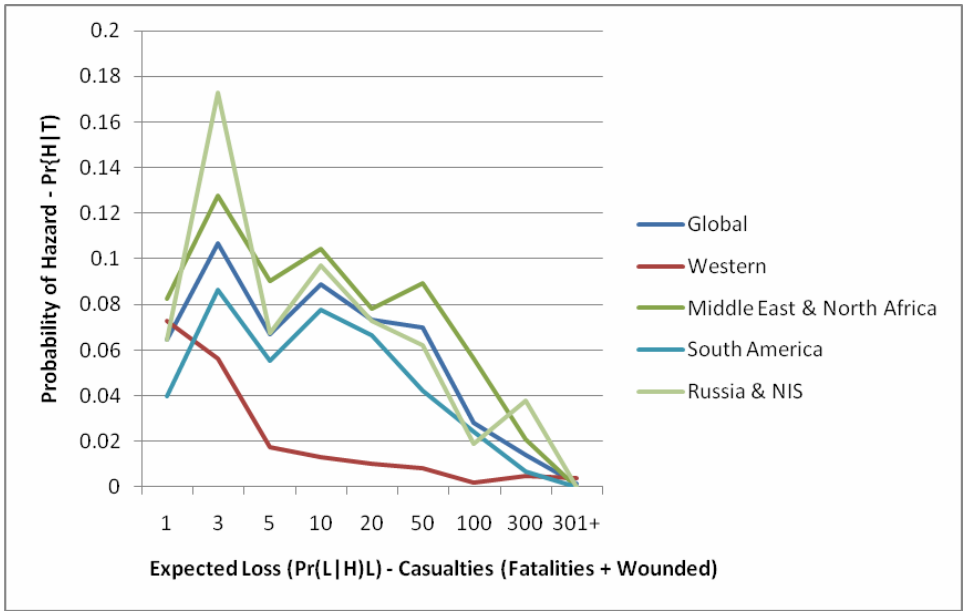


Figure 5 Relationship between Pr($H|T$) and Pr($L|H$)L for value of property damages arising from IED attack (see online version for colours)

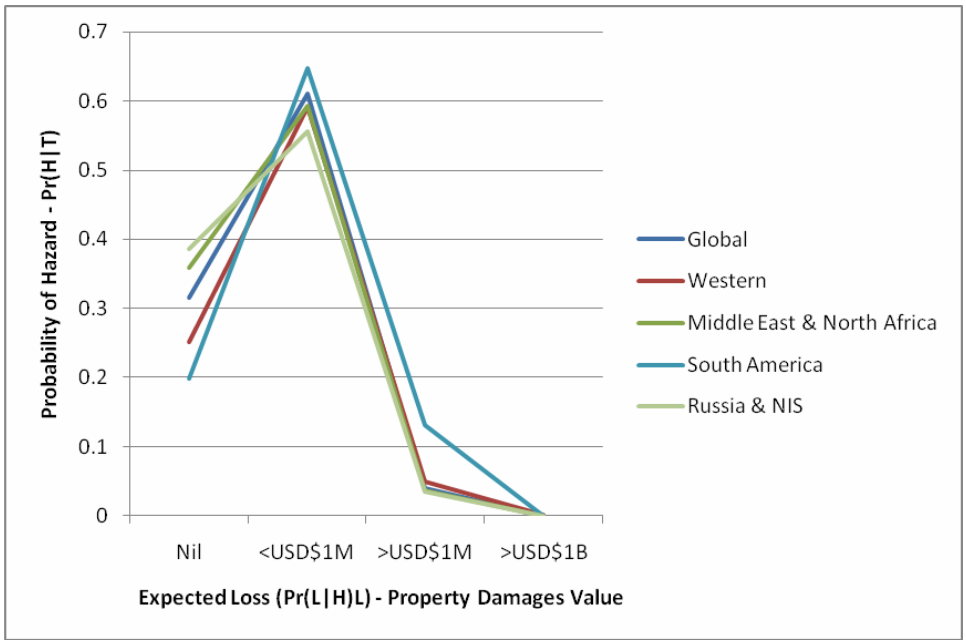
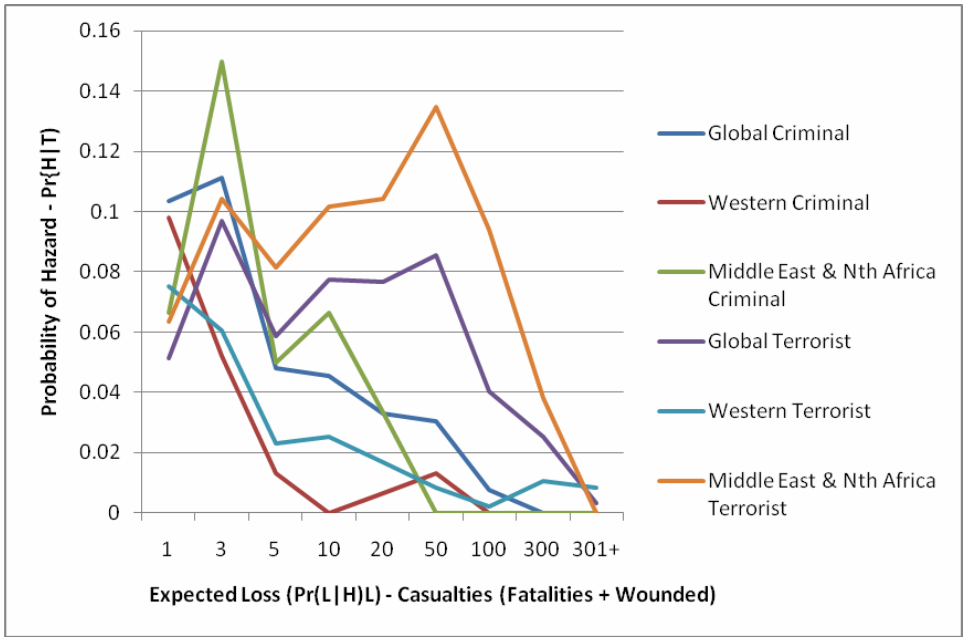


Figure 6 Relationship between Pr($H|T$) and Pr($L|H$)L – casualties (see online version for colours)



4 Discussion

The limitations of using the GTD as a dataset precluded detailed investigation and devolution of the identified PSFs further than depicted in Table 3, however, a dedicated IED database, well informed by post-incident forensics and intelligence, would provide further insight into how each PSF contributes to the probability of success for IED attacks. Despite this, Pr($H|T$) was able to be quantified in a more general sense and several observations can be made regarding IED success and the factors that contribute towards it.

4.1 IED success

Table 3 displays the comparison of $PSF_{D\&M}R$ and PSF_{Ops}, indicating that the probability of IED success is affected more by operational aspects (PSF_{Ops}) than IED design and manufacture ($PSF_{D\&M}R$). It would appear that if an IED is emplaced, then without intervention by authorities, the IED will most probably initiate as designed and create a damage effect. Despite this, creation of a damage effect does not imply a high probability of IED success in terms of casualties and damage as indicated in Table 3.

4.2 Regional and national culture influences

National culture affects personnel relationships and interactions, communication, learning and the conduct of tasks (Hofstede, 1980). One such aspect of note for this study is that national culture is an indicator for non-compliance behaviours (Park and Jung, 2007) –

the ability for personnel to follow directions, procedures and instructions. The results in Table 3 demonstrate that national culture [as correlated to region and noting that Vidino (2011) indicates that only a small proportion of terrorist plots arise from external regions] has a demonstrable impact on Pr($H|T$). In particular, IED attacks in the West are less likely to generate casualties than those in the Middle East, although there is greater probability of infrastructure damage (Table 3) and mass casualties (300+) (Figure 4) arising from attacks occurring in the West. These mass casualty events significantly impact the overall average of Western casualty averages per incident where casualties arose. There are several possible causes for these results, these being the motivation of the personnel involved, their access to education and training, and the security measures (discussed later) in place to combat IED attacks.

4.3 Organisational culture and education, training and experience influences

Organisational culture drives many of the aspects surrounding IED operations. Through knowledge management, processes and procedures an organisation can avoid mistakes, share best practices, solve problems faster, and complete faster development (Skyrme, 2002). Our results indicate that the knowledge resident in teams of personnel are better equipped for planning and conducting IED attacks than individuals, as demonstrated by the results obtained in Table 2. The failure rates identified within the global column of Table 2 are consistent with the failure rates associated with human error identified by Stewart and Melchers (1997) for individuals and teams.

We can clearly discriminate the differences between organisational groups through the use of these methods. For example, criminal and terrorist use of IED attacks where casualties are concerned (Figure 6), with criminal IED attacks likely to cause less casualties per incident than attacks by terrorist organisations.

Additionally, we can conclude that training is more important for IED operations than education given the comparative lack of success for Western IED attacks when compared to those in other regions, since educational standards are likely to be higher in Western countries. This is consistent with Barker's (2011) observations whilst studying the use of IEDs in Iraq and Afghanistan-Pakistan. He concluded that the evolution of technique is a local affair, shaped by local knowledge (including unarticulated expertise and experience resident in individuals) combined with tactical success or failure, and concerted efforts to respond to these experiences.

4.4 Efficacy of security measures

There are several areas where the GTD dataset maintains sufficient fidelity to make broad assessments of the efficacy of security measures and arrangements. These security measures include those that are preventative (dissuade, detect, neutralise, respond) or contain (detect, alert, limit, manage, search, evacuate) the situation (Nunes-Vaz et al., 2011). Such measures include IED disposal response, security check points, security patrols, policing activities and effective community awareness and response (e.g., evacuation) processes. The GTD dataset usefulness is constrained, however, we can derive whether an IED attack has been detected (i.e., the IED discovered), whether an appropriate response to the discovered threat was enacted, and whether this response

prevented IED success (i.e., prevented casualties/assassination or property damage > USD$1 million).

Other aspects of security measures undoubtedly contribute to IED attack failures through making it more difficult for the attacker to achieve a successful result. However, in this study, these aspects are considered to be failures on the part of the attacker – a result of inadequate planning, poor selection of the IED or inadequate education and training – hence affecting PSF_{Ops}.

A breakdown of IED attack detection and response success (no casualties arising from the attack) is provided in Table 4. With 11% of IED attacks being discovered, a credible security response remains important in combating terrorism. Almost 98% of these instances result in no casualties, with this proportion being higher if we were to discount casualties arising from security personnel responding to the IED attack (e.g., disarming an IED < evacuating the public). Further, if we consider the specific cases where credible threats are received, the probability that an IED attack causing casualties reduces from 52% to 6%.

One interesting case study into IED attacks against Thai educators and students reveals that an active security presence reduces target casualties from 1.7 casualties per incident to 0.2 casualties per incident (calculated from START 2010 data). This, however, comes at a cost to security personnel (an average of 3.3 security casualties per incident), posing an interesting ethical dilemma as to the value of the security element's lives versus the value of those they protect.

Table 4 Breakdown of IED attack detection and response success

Region	*Total incidents*	*Total incidents detected*		*Successful response given incident is detected*	
		No.	*%*	*No.*	*%*
Western	961	205	21	205	100
M.E. and N. Africa	907	77	8	73	95
Sub-Saharan Africa	182	10	5	10	100
South America	449	32	7	32	100
South Asia	1536	116	8	110	95
East Asia	50	3	6	3	100
Eastern Europe	118	5	4	5	100
Russia and NIS	370	66	18	64	97
Southeast Asia	731	83	11	82	99
Central America and Caribbean	7	1	14	1	100
Global	*5,339*	*598*	*11*	*585*	*98*

4.5 Future research

Future research shall investigate the feasibility of providing a level of quantitative analysis towards threat probability Pr(T), broadening the modelling of Pr($H|T$) to incorporate probability distribution functions more reflective of the reliability of IEDs, and quantifying Pr($L|H$)L through considering the quantification of target characteristics (for example, target vulnerability, population densities and target topology). This shall

facilitate further development of our model to provide a level of quantitative prediction for the risks arising from IED attacks. This model can then be automated to develop a PRA tool to estimate the risks associated with IED attacks. The model can then be employed to inform military operations planning and civil threat planning, including PRA and security risk management activities. This will include cost-benefit analysis for the efficacy of security measures intended to minimise the hazards associated with IED attack.

5 Conclusions

A PRA framework is described to assess the reliability and effectiveness of IEDs. To be sure, IEDs are complex socio-technical systems to model. If an IED is emplaced, then without intervention by authorities, the IED will most probably initiate and create a damage effect as designed – although this does not imply that the perpetrator's intent or target losses shall also be high. Despite this, there remains considerable variability in IED success between different geographic regions and organisational types. The major contributor to risk is the reliability and effectiveness of operational and planning aspects of IED attacks, and not the systems engineering and technical aspects relating to IED design and manufacture.

References

ATO Operations Planning (2006) *National Airspace System – Systems Engineering Manual*, Federal Aviation Administration [online] http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/operations/sysengsaf/seman/ (accessed 3 March 2011).

Aven, T. (2007) 'A unified framework for risk and vulnerability analysis covering both safety and security', *Reliability Engineering and System Safety*, Vol. 92, No. 6, pp.745–754.

Barker, A.D. (2011) 'Improvised explosive devices in Southern Afghanistan and Western Pakistan, 2002–2009', *Studies in Conflict & Terrorism*, Vol. 34, No. 8, pp.600–620.

Brooks, R.A. (2011) 'Muslim 'homegrown' terrorism in the United States – how serious is the threat?', *International Security*, Vol. 36, No. 2, pp.7–47.

Cinque, M. et al. (2007) 'How do mobile phones fail? A failure data analysis of Symbian OS Smart Phones', *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, IEEE.

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

Department of Defence (2002) *Joint Publication 3-60 Joint Doctrine for Targeting*, Joint Chiefs of Staff, USA.

Department of Defence (2006) *Defence Capability Development Manual*, Commonwealth of Australia, Canberra.

Department of Defence (2007) *Defence Explosive Ordnance Publication 105 (AM1) – Explosive Ordnance Life Management and Surveillance (Draft)*, Commonwealth of Australia, Canberra.

Dietz, A.S. (2011) 'Countering the effects of IED systems in Afghanistan: an integral approach', *Small Wars & Insurgencies*, Vol. 22, No. 2, pp.385–401.

Dillon-Merrill, R.L., Parnell, G. and Buckshaw, D. (2009) 'Logic trees: fault, success, attack, event, probability, and decision trees', *Wiley Handbook of Science and Technology for Homeland Security*, pp.1–22, Wiley.

Driels, M.R. (2004) *Weaponeering: Conventional Weapon System Effectiveness*, American Institute of Aeronautics and Astronautics, USA.

Enders, W. and Olson, E. (2011) 'Measuring the economic costs of terrorism', *Oxford Handbook of the Economics of Peace and Conflict* [online] http://www.socsci.uci.edu/~mrgarfin/OUP/papers/Enders.pdf (accessed 20 Jul 2011).

Faulconbridge, R.I. and Ryan, M.J. (2005) *Engineering a System: Managing Complex Technical Projects*, Argos Press, Canberra.

Firmino, P.R.A. et al. (2006) 'Eliciting engineering judgments in human reliability assessment', *Reliability and Maintainability Symposium*, IEEE, pp.512–519.

Forester, J. et al. (2003) 'Expert elicitation approach for performing ATHEANA quantification', *Reliability Engineering and System Safety*, Vol. 83, No. 2, pp.207–220.

Garrick, B.J. et al. (2004) 'Confronting the risks of terrorism: making the right decisions', *Reliability Engineering and System Safety*, Vol. 86, No. 2, pp.129–176.

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.

Hofstede, G. (1980) 'Motivation, leadership, and organization: do American theories apply abroad?', *Organizational Dynamics*, Vol. 9, No. 1, pp.42–63.

Joint Improvised Explosive Defeat Organization (2008) *Annual Report – FY 2008*, US Department of Defense [online] https://www.jieddo.dod.mil/content/docs/20090625_FULL_2008_Annual_Report_Unclassified_v4.pdf (accessed 21 July 2011).

Kenney, M. (2010) ''Dumb' yet deadly: local knowledge and poor tradecraft among Islamist Militants in Britain and Spain', *Studies in Conflict & Terrorism*, Vol. 33, No. 10, pp.911–932.

Koblentz, G.D. (2011) 'Predicting peril or the peril of prediction? Assessing the risk of CBRN terrorism', *Terrorism and Political Violence*, Vol. 23, No. 4, pp.501–520.

Levine, E.S. (2012) 'Estimating conditional probabilities of terrorist attacks: modeling adversaries with uncertain value tradeoffs', *Risk Analysis*, Vol. 32, No. 2, pp.294–303.

Ministry of Defence (2008) Defence Standard 00-42 Part 1 Issue 2, Reliability and Maintainability (R&M) Assurance Activity Part 1 One-Shot Devices/Systems, UK.

Minkov, M. and Hofstede, G. (2011) 'The evolution of Hofstede's doctrine', *Cross Cultural Management: An International Journal*, Vol. 18, No. 1, pp.10–20.

National Academies and the Department of Homeland Security (2010) *News and Terrorism – Communicating in a Crisis* [online] http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf (accessed 26 February 2010).

National Consortium for the Study of Terrorism and Responses to Terrorism (START) (2010) Global Terrorism Database [Data file], University of Maryland, USA, May 2010 [online] http://www.start.umd.edu/gtd (accessed 14 June 2011).

Nunes-Vaz, R., Lord, S. and Ciuk, J. (2011) 'A more rigorous framework for security-in-depth', *Journal of Applied Security Research*, Vol. 6, No. 3, pp.372–393.

Park, J. and Jung, W. (2007) 'OPERA – a human performance database under simulated emergencies of nuclear power plants', *Reliability Engineering and System Safety*, Vol. 92, No. 4, pp.503–519.

Park, K.S. and Lee, J. (2008) 'A new method for estimating human error probabilities: AHP–SLIM', *Reliability Engineering and System Safety*, Vol. 93, No. 4, pp.578–587.

Reliability Information Analysis Centre & Data and Analysis Centre for Software and Defense Science Board (2005) *System Reliability Toolkit*, Defense Technical Information Centre, USA.

Sheehan, I.S. (2012) 'Assessing and comparing data sources for terrorism research', *Evidence-Based Counterterrorism Policy*, Springer Science + Business Media, New York.

Skyrme, D.J. (2002) 'Developing a knowledge strategy: from management to leadership', in Morey, D. et al. (Eds.): *Knowledge Management: Classic and Contemporary Works*, MIT Press, London.

Speckhard, A. (2011) 'Battling the 'University of Jihad:' an evidence based ideological program to Counter Militant Jihadi Groups active on the internet', *Countering Violent Extremism: Scientific Methods & Strategies*, Air Force Research Laboratory, USA.

Stewart, M.G. (2008) 'Cost-effectiveness of risk mitigation strategies for protection of buildings against terrorist attack', *Journal of Performance of Constructed Facilities*, Vol. 22, No. 2, pp.115–120, ASCE.

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

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

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*, Vol. 8, No. 1, Article 30, pp.1–18.

Taylor-Adams, S. and Kirwan, B. (1997) 'Human reliability data requirements', *Disaster Prevention and Management*, Vol. 6, No. 5, pp.318–335.

Vidino, L. (2011) *Radicalization, Linkage, and Diversity: Current Trends in Terrorism in Europe*, RAND Corporation, USA.

Weiss, L., Whitaker, E., Briscoe, E. and Trewhitt, E. (2011) 'Evaluating counter-IED strategies', *Defense & Security Analysis*, Vol. 27, No. 2, pp.135–147.

Yorks, L. and Sauquet, A. (2003) 'Team learning and national culture: framing the issues', *Advances in Developing Human Resources*, Vol. 5, No. 1, pp.7–25.

Notes

1 Based on success criteria of inflicting casualties (not the perpetrator or their associates), assassinating intended victims and/or greater than USD$1 million property damage.

2 Includes Western Europe, North America (including Mexico), Australia and New Zealand.

3 Includes Algeria, Bahrain, Cyprus, Egypt, Iran, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, North Yemen, Qatar, Saudi Arabia, South Yemen, Syria, Tunisia, Turkey, United Arab Emirates, West Bank and Gaza Strip, Western Sahara, Yemen

4 Revised from Grant and Stewart (2011).

5 The hazard arising from each device is a combination of the damage effect (that is, a thermal effect, blast effect, fragmentation effect or combination of these effects) and the yield of the IED. This is a function of the type and size of the IED and the proficiency of its manufacturer.