19th International Congress on Modelling and Simulation, Perth, Australia, 12–16 December 2011
http://mssanz.org.au/modsim2011

Terrorism and simulation of terrorist incidents across critical Infrastructure

Dave Birkett [a,b] **and Helena Mala-Jetmarova** [b,c]

[a] *Truscott Crisis Leaders, Wembley Downs, Western Australia 6019, Australia*
[b] *School of Science, Information Technology & Engineering, University of Ballarat, Mt Helen Campus, University Drive, Ballarat, Victoria 3353, Australia*
[c] *Grampians Wimmera Mallee Water (GWMWater), 11 McLachlan Street, Horsham, Victoria 3400, Australia*
Email: dbirkett@crisisleaders.com

Abstract: Terrorism has progressed to a global phenomenon as a terrorist attack has an immediate effect on society not only in the targeted area, but also across the rest of the world. Acts of terrorism are extremely difficult to predict or provide early warning in most cases. In consideration of Australia, which is to a certain extent insulated from the rest of the world by virtue of the sea barrier, there is a history of terrorist incidents reported back to the 1970s. Since the attack on New York in September 2001, the level of terrorism alert to Australia has increased significantly with a current 'Medium' national level of threat.

Critical Infrastructure (CI), which is considered essential for contemporary social human existence, has been impacted by multiple and variable external threats in modern times. The destruction at Chernobyl in 1986 and more recent events such as the terrorist incidents at Madrid in 2004, London in 2005, Moscow in 2011 and the tsunami in Japan in 2011 indicate the vulnerability of this infrastructure. Such events translate to threats from both natural disasters referred to as all hazard origin and human interventions such as terrorism.

Subsequently, some private and government organisations of CI now regularly rehearse and simulate models of both terrorist incidents and all hazard events as a proactive protection strategy and business continuity process. These models are implemented in a form of scripted Crisis Simulation Exercises (CSE) which simulate a crisis within an organisation in order to strengthen an organisation's ability to manage crisis situations. CI organisations which adopt these strategies are able to mitigate impact of these crises and therefore, are considered to reflect a more resilient organisation to the effects of external impact.

CSEs test plans, procedures, equipment and personnel to industry standards required. Within the spectrum of counter-terrorism in particular, the CSEs are becoming more sophisticated and reflective of reality with incorporation of live actions to ensure credibility and reality. The simulated scenario may include a variety of attack methodologies such as biological, chemical, cyber and conventional bombs/blasts and bullets to maintain exercise standards with continuously developing technology of terrorist attacks.

This paper defines the topic of terrorism with the profile of terrorists, and examines the terrorism concept and environment both in Australia and internationally including future considerations. It also provides an overview of the simulated framework for mitigation of crisis associated with CI protection with an Australian perspective, suitable for CI protection worldwide. Additionally, this paper examines the concept of terrorism simulation, illustrating a strong case for future simulation progression with some innovative ideas and futuristic predictions as to where terrorist simulations may advance to across the future.

Keywords: *Terrorism, terrorists, Critical Infrastructure (CI), Crisis Simulation Exercise (CSE*), *crisis*

1. INTRODUCTION

Australian CI is defined as those physical facilities, supply chains, information technology and communication networks, which if damaged or destroyed by a terrorist incident or all hazard event, would impact on the security, economy and social well being of the nation. Typical examples of CI are power, water, health, communications and banking sectors.

CI is considered as a primary target of fundamentalist terrorist groups as the attack has the immediate effect of engendering fear and panic not only in the targeted area, but also across the rest of the world. Moreover, the difficulty in predicting such incidents produces an additional element of fear across society. All hazard events tend to also contribute to significant impacts on CI, human life and national economies, although they may be predicted in selected instances. Preparedness for all hazard events, as described by Bennett (2007) from the United States Homeland Security Presidential Directive 8 as *"the term 'all – hazards preparedness' refers to preparedness for domestic terrorism attacks, major disasters, and other emergencies,"* can in reality surface under the guise of weather and geological occurrences, or infrastructure and asset life cycle failure.

2. BACKGROUND

2.1. What is Terrorism?

According to Silke (2004) the word 'terrorism' is one that invokes emotion and horror, often affecting opinions and judgements, which have led to misconceptions and prejudices, affecting official attitudes and policies. However, Bennett (2007) has identified that the word 'terrorism' is derived from the Latin word *'terrere'* which translated to English means to tremble, possibly from the fear invoked amongst populations directly affected by the randomness, and lack of predictability related to terrorist acts. Indeed, Silke (2004) outlines that previous researchers Schmid and Jongman (1988) had identified 109 differing definitions relating to the highly emotive topic of terrorism.

For the purposes of this paper, the definition of terrorism, as identified by Bennett (2007) from the U.S. Department of State in the United States Code, Title 22, Section 2656f (d), is *"premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience."* Bennett (2007) also states that there are four key distinguishing elements of terrorism:

- It is premeditated – planned in advance and not conducted as an impulsive act of rage,
- It is political – designed to change the existing political order,
- It is aimed at civilians – not military personnel or facilities,
- It is carried out by sub-national groups – not a country's army.

In most cases, acts of terrorism are extremely difficult to predict or provide early warning with any accuracy. This is, despite the electronic and human intelligence, gathered and analysed by western intelligence agencies. Typical of these unpredictable and terrifying incidents were the Twin Towers attack in New York in 2001, the suicide bombing at Bali in 2002, and the Madrid and London transport attacks on both rail and bus transport in 2004 and 2005, respectively (Department of Prime Minister & Cabinet, 2010).

2.2. What are Terrorists?

In the global community, there appears to be a certain functional sociological thought that terrorists display and terrorist incidents reflect some commonality in profile or personal terrorist attributes. Indeed, Horgan (2007) considers that it is a 'fundamental attribution error' to cognitively understand the concept of the grouping of terrorists. This may be interpreted as displaying a profile considered as 'terrorist behaviour' or death destruction and social disturbance as an observed commonality. However, this tends to ignore the variable nature related to ideology, objectives, leadership, geographical spread and organisational context which more accurately defines the specific groups and patterns of group behaviour.

In consideration of the goals of terrorism, Bennett (2007) suggests five defined common goals which clearly translate to the individual terrorist. This is despite of operating individually or in large groups, and attacking in various ways for disparate goals. Bennett (2007) includes the following commonalities across global terrorist groups:

- Causing casualties (injuries and fatalities),

- Damaging or destroying CI,
- Disrupting the economy,
- Harassing, weakening or embarrassing the government,
- Discouraging tourism or investments due to perceived insecurity.

Bennett (2007) raises the issue that the development of more sophisticated weapons in the 21st century has allowed terrorists to kill increased numbers of people over larger distances. Bennett (2007) also informs that terrorists have maintained their technological expertise and linkages, and are utilising the Internet to formulate plans, gather information, recruit members, raise funds and spread propaganda. Illustrations of increased use of technology by some terrorist groups are highlighted by Bennett (2007) with examples selected from the South American Terrorist Group, Revolutionary Armed Forces of Colombia (FARC). This includes the identified use of remote controlled automobiles which have been observed to deliver car bombs. Another example by Bennett (2007) is the Tamil Tigers in Sri Lanka, where stealth technology has been used to mask suicide speedboats.

It has been reported that the Al-Qaida terrorist group is steadily increasing its utilisation of technology. This includes techniques to reach a larger audience via broadcast anchors in periodic announcements, improving video technological quality, increasing availability of recruitment literature on the Internet, increasing dual use of Arabic and English as international communication languages for propaganda purposes with some speeches in French and Urdu. Consequently, the propaganda campaigns continue to recruit and expose listeners to the ideology for terrorism.

3. TERRORISM CONTEXT AND ENVIRONMENT

3.1. Australia

Although Australia is to a certain extent insulated from the rest of the world by virtue of the sea barrier around the continent, there are 9 international airports with multiple daily flights from all areas of the globe, and multiple sea ports, with people entering and leaving the country on a daily basis. People entering and leaving Australia are monitored by the Australia's Customs and Border Protection Department (ACBPD) through a screening process. The ACBPD appears to be proactive in the area of the detection of any illicit movement of explosives and weapons.

However, terrorist incidents have occurred in Australia. The first observed terrorist incident was the bombing of the Yugoslav General Trade Agency in Sydney in 1972, followed by the Sydney Hilton Hotel bombing in February 1978 at the venue for the meeting of the Commonwealth Heads of Government Regional Meeting (CHOGRM). Subsequently, there was the assassination of the Turkish Consul General also in Sydney in 1980 (Crown, 1986) and the bombing of the Israeli Consulate and Hakoah Club in Sydney (Department of Prime Minister & Cabinet, 2010). These incidents provided an alert message to Australia, which previously appeared immune from the global effects of terrorism occurring in other countries. Crown (1986) indicates a state of political confusion and overreaction related to the CHOGRM incident. Although the media were warned with two anonymous phone calls as to the location prior to the blast, no person or group has claimed responsibility and no arrests or convictions occurred in relation to this incident. Crown (1986) also refers to the assassination of the Turkish Consul, Sarik Ariyak, in Sydney in December 1980, and the Gelignite bomb which blasted the Woolworth's store in Liverpool west of Sydney in May 1982.

The level of terrorism alert to Australia has increased significantly since the attack on New York in September 2001 (Commonwealth of Australia, 2010). Currently, the national threat level for a terrorist act within Australia is designated as a 'Medium' level of threat. In other words, a terrorist act may occur anywhere in Australia at any time. The threat levels are calculated by various federal organisations and intelligence agencies, in consideration of the information available and Australia's political, economic and military activities elsewhere with a global perspective.

3.2. International

Within the international terrorism research sphere, some experts such as Sinai (2007) consider that there are the following three basic types of terrorism warfare conducted by terrorist groups:

- Conventional Low Impact (CLI), where conventional means are applied by terrorist groups with minimal casualties to highlight specific issues or causes,

- Conventional High Impact (CHI), where conventional means are used to create and maximise catastrophic damage, such as the impact of the airliners into the Twin Towers in New York in 2001,
- Chemical, Biological, Radiological or Nuclear (CBRN) warfare, where unconventional methodologies are applied by terrorist groups to inflict maximum casualties.

The various preparations and mitigations to reduce the effects and impacts of a terrorist attack tend to follow the progress and developments of the changing and evolving face of terrorism over time. Intelligence and law enforcement presently tend to provide a framework of mitigations catering for CLI and CHI.

3.3. Future Considerations

Terrorism has progressed and developed relative to the global reaction to counteract the various terrorist incidents. In the 1970s, subsequent to the Munich terrorist incident, plane hijackings were observed as a tool for terrorists. As airlines tightened security, the displacement effect appeared to move terrorists into kidnappings, bombings and suicide bombing attacks. In consideration of this progression, there may well be a new wave of terrorist attacks under a new umbrella in the future.

Terrorism is the new face of world unresolved conflict, and for the majority of terrorist groups, has made the quantum permanent leap from the parliament to the streets. It is unlikely that the world will experience traditional warfare that complies with the Geneva Convention in the future. The rules of warfare have now been by-passed with terrorism exhibiting no rules, no identifiable country of origin and no predictability as to what will occur, where and when? This new mode of warfare produces a dilemma for western intelligence agencies, which may have to modify and restructure the standard intelligence approach in order to combat this new violent international order.

With the global progression for remote access in all businesses, particularly in the areas of the designated CI, 'a soft underbelly' is possibly developing to become a future terrorist target. These industry advances have been developed to reduce labour costs and increase efficiency across the world, but may well have increased the potential risk exposure to CI. For example, the increasing use of remote control and Supervisory Control and Data Acquisition (SCADA) in the power, water and other sectors may increase the risk of external cyber intervention. Also the banking network moving vast sums of money across cyberspace may be at risk.

There is an awareness of this issue amongst various government organisations. The government considers the issue as a shared responsibility (Commonwealth of Australia, 2010) from domestic users to private and government organisations. In consideration of the recent focus on international 'cyber warfare' subsequent to a recent alleged attack on United States cyber infrastructure (Rogin, 2010), owners of infrastructure are becoming increasingly aware of potential risks and are examining mitigation strategies.

4. CRISIS SIMULATION EXERCISES (CSEs)

4.1. Current Practice

CSE is a process which models or simulates a crisis within an organisation in order to develop and strengthen an organisation's ability to manage and control a crisis situation. The CSE may focus on testing crisis plans, procedures, equipment or personnel to the appropriate levels of necessary exposure. A modelled crisis represents either a terrorist incident or an all hazard event. There are four types of CSEs, which differ especially from the exercise objectives, timeframe and stakeholders involved, such as:

- Tabletop exercises,
- Incident/emergency exercises,
- Live exercises,
- Business continuity exercises.

Similar to a real crisis situation, exercise stakeholders include both the organisational personnel and external organisations. The organisational personnel represent the Crisis Management Team (CMT) and the Incident Management Team (IMT) which would normally manage a real crisis. For the purpose of the CSE, the CMT and IMT consists of personnel from throughout the organisation representing a cross section from operations to management. Organisational personnel are also represented as counter players who provide exercise input. External organisations represent exercise assessors and observers, and support the exercise manager as

required. Unlike a real crisis, the CSE includes the role of an exercise manager and an exercise controller to assure that the exercise is managed effectively.

With reference to Figure 1, a clear comparison is demonstrated illustrating a terrorist incident as it would occur in reality with the simulated model. This model or CSE identifies the commonalities of an external influence which provides the primary 'trigger' and focus relating to either the 'reality' of a terrorist incident or all hazard event. Additionally, the CSE identifies the commonalities of an external influence, providing the primary focus and 'trigger,' which relates to the 'reality' of a crisis. Moreover, the defined targeted organisation is visualised within the model with a demonstration of the various forms of external monitoring which actually occurs in a real incident and which is simulated during a CSE. Additional and more detailed information about the CSEs can be found in Birkett et al. (2011).

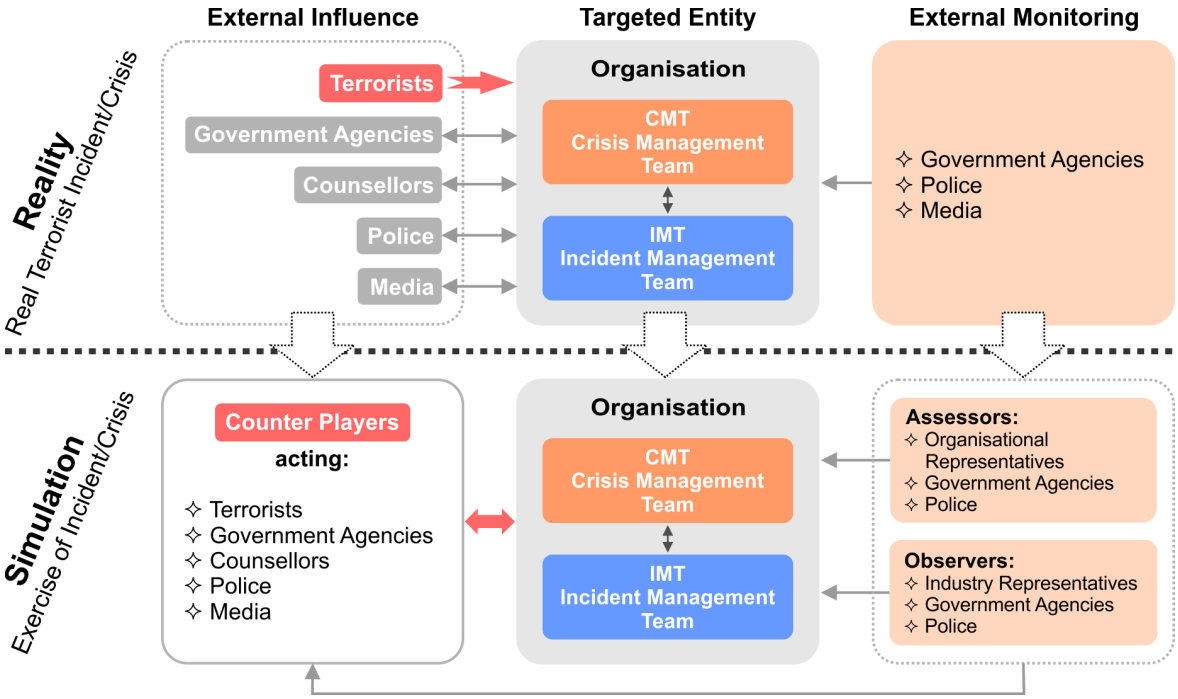

Figure 1. A Typical Model Displaying Linkage between a Terrorist Incident as Reality and Simulation.

To answer the question 'Why CSEs require to be considered in relation to terrorist incidents and all hazard events?', it should be understood that the occurrences and timing of these events are not always predictable or convenient, and CI organisations need to be prepared for these crises. In order to mitigate the impact of these events, it is appropriate to create a credible CSE for the purpose of operational rehearsal. According to Birkett et al. (2011), this rehearsal experience provides significant training for the various operational and management personnel within potentially impacted CI organisations, prior to the incident which may occur in reality. CI organisations which adopt the CSEs strategies reflect a more resilient organisation to the effects of both terrorist incidents and all hazard events.

4.2. Future Perceptions

The requirement for the CSEs may escalate in the future. Due to the rapid advances in technology within the international global community, it can be anticipated that there will be new progress in this area within the next two to three years. In consideration of existing communications and virtual technology, it is feasible that the following predictive methodologies and tools may be available and utilised to support the CSEs:

- A possible system of recorded and stored holographic images to add realism to the CSE, complete with sound, visual effects and odour in a CD format or another medium, which may take its place to be used in a computer or its successor,
- The CSEs for terrorist attacks across the future should also incorporate some realistic and credible aspects of CBRN and SCADA cyber penetration to remain proactive in lieu of the current reactive stance,
- CSEs may be available in a series of adjustable script packs, complete with interactive scripts with a variety of sounds, visual effects and odour,

- There may be a fast growth of private sector groups specialising in this futuristic high technology simulation area,
- A variety of quality CSEs may be available on-line for a fee or annual membership to private organisations specialising in this area,
- There will potentially be a 'one stop' shop for all CSEs, again in cyber space to cater for the needs of any organisation wishing to test plans,
- CSEs may well be a legislated compliance activity for private organisations listed on the stock exchange and government organisations to provide evidence and assurance that their plans have been independently tested on an annual basis,
- There may be a virtual reality package to temporarily relocate the 'corporate warrior' from the second commercial battlefield into the first battlefield of the terrorist to provide some exposure and realism.

All the above are merely projections for the future in consideration of the rapid advances in technology over the past 20 years. It is not inconceivable that some of the above may occur, and that some readers of this paper may well convert these perceptions into reality.

5. CONCLUSION

The paper has introduced CI as a target of both terrorist incidents and all hazard events, highlighting the difficulty in predicting these crisis situations. Terrorism was defined and analysis provided related to terrorists and their behavioural patterns.

The situation in Australia relating to terrorism was broadly discussed. It was demonstrated that although Australia has a distinct 'advantage' of isolation from the rest of the world, terrorist incidents have occurred in the past. Internationally, types of terrorist warfare were evaluated, with the future path of terrorism and its environment also examined. It was concluded that there is an increased awareness of terrorist progression and sophistication in terms of technologies used, which may result in an increasing requirement for examination and implementation of mitigation strategies.

These strategies include CSEs which were described in the broad context of their application to CI protection. It was demonstrated how a real crisis within an organisation translates to the simulated model with participants involved. It was suggested that CSEs are a beneficial tool to increase the resilience of the organisation in the case of crisis from both terrorist incidents and all hazard events. Various future perceptions were also introduced for future considerations of paper readers.

REFERENCES

Bennett, B. T. (2007). Understanding, Assessing and Responding to Terrorism – Protecting Critical Infrastructure and Personnel. John Wiley & Sons, New Jersey.

Birkett, D., Truscott, J., Mala-Jetmarova, H., and Barton, A. (2011). Vulnerability of Water and Wastewater Infrastructure and its Protection from Acts of Terrorism: A Business Perspective. In: *Handbook of Water and Wastewater Systems Protection, Series Protecting Critical Infrastructures,* Clark, Robert M., Hakim, Simon, Ostfeld, Avi, eds., Springer, USA.

Commonwealth of Australia (2010). Critical Infrastructure Resilience: Whose Responsibility Is It? Fact Sheet. Trusted Information Sharing Network (TISN). Available on http://tisn.gov.au/www/tisn/content.nsf/Page/Publications_PublicationsA-Z (accessed on 22 September 2011).

Crown, J. (1986). Australia: The Terrorist Connection. The MacMillan Company of Australia Pty Ltd, Melbourne.

Department of Prime Minister & Cabinet (2010). Securing Australia - Protecting Our Community. Canberra, Australia, ISBN: 978-1-921385-99-5.

Horgan, J. (2007). Understanding Terrorist Motivation: A Socio-Psychological Perspective. In: *Mapping Terrorism Research,* M. Ranstorp, ed., Routledge, Abingdon.

Rogin, J. (2010). The Top 10 Chinese Cyber Attacks (That We Know of). Available on http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of (accessed on 22 September 2011).

Schmid, A., and Jongman, A. (1988). Political Terrorism, second edition. North-Holland Publishing Company, Oxford.

Silke, A. (2004). Research on Terrorism - Trends, Achievements and Failures. Routledge, Abingdon, Oxon.

Sinai, J. (2007). New Trends in Terrorism Studies: Strengths and Weaknesses. In: *Mapping Terrorism Research,* M. Ranstorp, ed., Routledge, Abingdon.