JDiBrief – Security

Scenario based risk assessment for critical infrastructures: SUMMARY (1 of 5)

Author: Dr Tanya Le Sage, UCL Department of Security & Crime Science

In recent years democratic countries have witnessed an increase in attempted terrorist attacks, with violent extremists often targeting symbolic buildings (i.e. key government departments or historic landmarks) or critical infrastructures (such as transport networks or energy-grids). Within the risk management environment, risk assessment is one of the main methods used to prevent terrorist attacks from happening. It is a critical aspect of security and crime control, and forms the core of many risk management frameworks.

Terrorism risk assessment is usually performed by security professionals, and involves estimation of the probability and consequences of hypothetical attacks against a target. Such estimates are derived through a mix of experience and historical evidence.

At present, one of the key issues with risk assessment models is that they often lack the ability to integrate new security measures with existing ones. This means that the assessment of the effectiveness of the inclusion of new technologies is inaccurate, or at best, time consuming.

The innumerable threats to security mean that risk assessment of infrastructure can be a complex process. It is important to consider a wide range of scenarios when considering the effectiveness of the implementation of different security measures. These can identify the extent to which proposed measures mitigate the identified risks, and fit within their operational context. Scenarios are commonly used in risk assessments to represent ordinary situations corresponding to normal states, and extraordinary situations corresponding to potential risky deviations. This approach has been used by decision-makers to subject specific ecosystems to numerous fictional scenarios. By doing so, they are able to assess how these ecosystems react to the scenarios, and decide whether the systems proposed to be implemented were suitable.

Led by Dr. Borrion, the UCL Resilience of Infrastructure and Building Security (RIBS) team is developing a computing engine that can simulate hundreds of attack scenarios, and evaluate their consequences against specific evaluation criteria. The computing engine the team has built can, for example, determine the multiple paths that a terrorist may take through a synthetic environment. It can also account for the numerous actions that they can complete at each step of their attack.

RIBS
Resilient Infrastructure and Building Security

SEVENTH FRAMEWORK PROGRAMME

Within the simulation environment each path that the offender (i.e. the player) can take is determined as a dynamic crime script. Crime scripts – borrowed from Environmental Criminology – represent a chronological sequence of causal events. For example, a suicide bomber may enter a building, move to a location where he wishes to explode the bomb, get the bomb into a state such that it is ready to explode, and then trigger it to cause an explosion.

Once this script has been simulated, and the likelihood of proceeding along the path has been determined, experts in explosion analysis carry out simulation based analysis to determine the consequences of the attack using criteria such as the number of fatalities, number of injuries, and corporate outcomes such as business continuity and reputation.

JDiBrief – Security

Scenario based risk assessment for critical infrastructures: TOPIC OVERVIEW (2 of 5)

Author: Dr Tanya Le Sage, UCL Department of Security & Crime Science

Since the turn of the millennium democratic countries have seen increased attempts by violent extremists to commit terrorist attacks. The primary targets of these attacks are often symbolic buildings (i.e. key government departments or historic landmarks) or critical infrastructure (such as transport networks or energy-grids). When successful, these attacks have a major impact on society, causing death, serious injury, damage and disruption on an unprecedented scale. To mitigate these threats to national security a variety of strategies and tactics are adopted by politicians, private sector organisations and security companies. Within the risk management environment, risk assessment is often a prerequisite step for the prevention of terrorist attacks. It is is a critical aspect of security and crime control, and forms the core of many risk management frameworks.

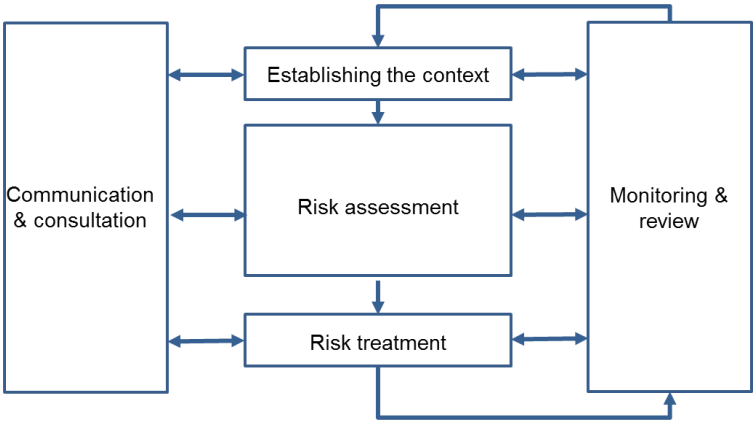

Figure 1 – a representaion of the ISO 31000 risk management framework

Probabilistic risk assessment is a practical approach for assessing the capabilities of security systems.

Security systems can take many forms – for example, CCTV networks, air ventilation systems or biometric technologies – and are designed to protect assets from being altered in an undesirable manner.

Terrorism risk assessment is usually performed by security professionals, and involves estimation of the probability and consequences of hypothetical attacks against a target. Such estimates are derived through a mix of experience and historical evidence. Risk assessments will also commonly look to anticipate future and emergent threats to security. The results of the risk assessment help formulate and implement a suitable security strategy.

In response to the heightened risks, the past decade has seen the security technology industry grow substantially. Many security products and measures are now available for the purposes of protecting critical infrastructure. Security managers have to decide between different measures (i.e. technologies or policies), often using cost-benefit analysis to substantiate their decision. Such costs and benefits are sometimes directly in conflict though (i.e. a 'perfect' system may be prohibitively expensive) and decisions are made with a view to finding the optimal balance between the two.

At present, one of the key issues with computer based risk models is that they often lack the ability to integrate new security measures. This means that the assessment of the effectiveness of the inclusion of new technologies is inaccurate, or at best, time consuming. The approach outlined in the subsequent page of this JDiBrief permits the impact of new technologies to be evaluated, and further allows the impact of a malfunctioning security system to be assessed.

JDiBrief – Security

Scenario based risk assessment for critical infrastructures: ANALYSIS (3 of 5)

Author: Dr Tanya Le Sage, UCL Department of Security & Crime Science

The innumerable threats to security mean that risk assessment of infrastructure can be a complex process. It is important to consider a wide range of scenarios when considering the effectiveness of the implementation of different security measures. These can identify the extent to which proposed measures mitigate the identified risks, and fit within their operational context. Scenarios are commonly used in risk assessments to represent 'as planned' situations corresponding to normal states, and risk situations corresponding to potential deviations. This approach has been used by decision-makers who subject an ecosystem to numerous fictional scenarios. By doing so, they are able to assess how the ecosystem reacts to the scenario, and can determine the resulting outcomes against evaluation criteria.

Security-related evaluation criteria often correspond to the changes made to an asset as the result of an attack. *Information security* predominantly categorises the evaluation criteria into three categories:

- Confidentiality (the extent to which other users know about the properties of some entities, and their relationships to other elements in the ecosystem),
- Integrity (including injuries or fatalities) and
- Accessibility (by certain users).

For *physical security* although the categories are well defined, they are not so compartmentalised.

Previous research has considered using agent-based models to simulate terrorist attacks. Such models allow the roles of the offender and defender (i.e. the security measures) to be played out step by step, allowing each agent to assess its situation and make decisions based on a set of rules. This technique has been used to assess the effect of biological attacks and chemical attacks on a city. The models allow analysts to simulate many scenarios over a broad range of conditions. However they are computationally intensive and the effects of interactions between the agents are uncertain, meaning that it is difficult to make predictions about the system's future states.

Further work has considered modelling the implementation of security systems as discrete event systems, allowing sequences to be generated which characterise a system's behaviour. A combination and extension of these two approaches forms the basis of the computational tool developed at UCL, outlined in the next brief in this series.

JDiBrief – Security

Scenario based risk assessment for critical infrastructures: NEW KNOWLEDGE AND APPLICATIONS (4 of 5)

Author: Dr Tanya Le Sage, UCL Department of Security & Crime Science

The UCL Resilience of Infrastructure and Building Security (RIBS) team is developing a computing engine that can simulate hundreds of attack scenarios, and evaluate their consequences. The computing engine the team has built can, for example, determine the multiple paths that a terrorist may take through a synthetic environment. It can also account for the numerous actions that they can complete at each step of their attack.

Within the simulation environment each path that the offender (i.e. the player) can take is determined as a dynamic crime script. Crime scripts – borrowed from Environmental Criminology – represent a chronological sequence of causal events. For example, a suicide bomber may enter a building, move to a location where he wishes to explode the bomb, get the bomb into a state such that it is ready to explode, and then trigger it to cause an explosion.

Once this script has been simulated, and the likelihood of proceeding along the path has been determined, experts in explosion analysis carry out simulation based analysis to determine the consequences of the attack using criteria such as the number of fatalities, number of injuries, and corporate outcomes such as business continuity and reputation.

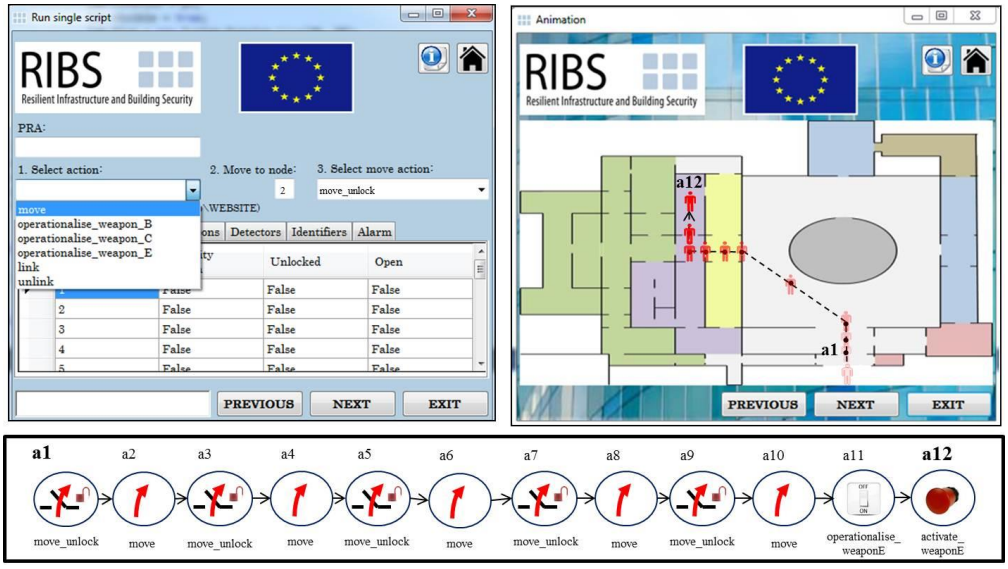

Figure 2 – a screenshot of the RIBS simulated terrorist script

Figure 2 illustrates where the RIBS software was used to model an attack script on a public target. The attack script described here shows an offender entering the building via the main entrance, and proceeding to move throughout the building until they reach a highly populated room. Once they have reached their destination, they attempt to trigger an explosive device. Upon the triggering of this device the consequences of the attack are estimated using simulation software. In this context, probabilistic risk analysis provides a useful framework to estimate the vulnerability of the facility to a terrorist attack, and identify areas where security should be enhanced.

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007- 2013) under grant agreement n° 242497.

JDiBrief – Security

Scenario based risk assessment for critical infrastructures: RESOURCES (5 of 5)

Author: Dr Tanya Le Sage, UCL Department of Security & Crime Science

GENERAL RESOURCES

- RIBS project website - Available at: http://www.ribs-project.eu/
- Clarke, R. V. and Eck, J. (2003) *Becoming a Problem-solving Crime Analyst*. London: Jill Dando Institute of Crime Science.
- Meade, C. and Molander, R. C. (2006). Considering the Effects of a Catastrophic Terrorist Attack. RAND Corporation, Santa Monica, California.
- Willis, H., Morral, A., Kelly, T., Medby, J. (2005). *Estimating terrorism risk*. RAND Corporation, Santa Monica, California.

A SELECTION OF ACADEMIC PAPERS AND BOOK CHAPTERS:

- Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Studies Prevention*, vol. 3
- Dillon, R. L., Liebe, R. M. and Bestafka, T. (2009) Risk-based decision making for terrorism applications, *Risk Anal*., vol. 29, no. 3, pp. 321–335.
- Ezell, B. C., Bennett, S. P., Winterfeldt, D. Von, Sokolowski, J. and Collins, A.J. (2010) Probabilistic Risk Analysis and Terrorism Risk, *Risk Anal*., vol. 30, no. 4, pp. 575–589.
- Taylor J. , Margaritis D. , Nasir Z. A., Borrion H. , Lai K.M., *The role of protection measures and their interaction in determining building vulnerability and resilience to bioterrorism*, J Bioterr. Biodef., 2013

CONFERENCE PROCEEDINGS

- Le Sage T., Borrion H., Toubaline S., *An Object-Oriented Approach for Modelling Security Scenarios*; Computer Modelling and Simulation, International Conference on - April 2013, Cambridge, UK
- Borrion, H., Bouhana, N. (2012). iCARE: A scenario-based method for the RIBS project. *European Intelligence and Security Informatics.* 22 August 2012, Odense, Denmark
- Le Sage, T., Borrion, H., Toubalne, S. (2012). A tool-target approach for simulating a terrorist attack. *IEEE Technologies for Homeland Security.* 14-16 November 2012, Boston, Massachusetts
- Toubaline, S., Borrion, H., Le Sage, T. (2012). Dynamic generation of event trees for risk modelling of terrorist attacks. *IEEE Technologies for Homeland Security.* 14-16 November 2012, Boston, Massachusetts