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.

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.

ISSN 2050-4853