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.

ISSN 2050-4853