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 repre
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