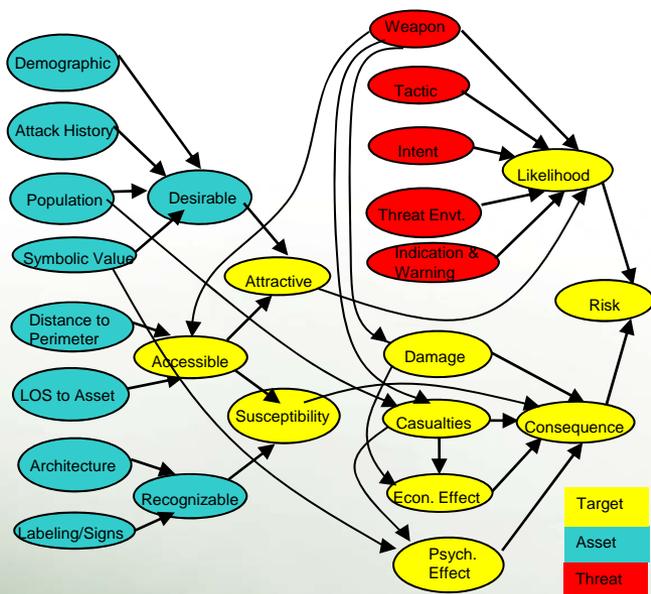


Threat Anticipation and Deceptive Reasoning Based on Bayesian Belief Networks

Modeling and Simulation Group

Computational Sciences & Engineering Division



Problem Statement:

- Threat anticipation requires that we understand the likelihood of an event and the consequences if that event were to occur so that mitigation efforts can be optimally employed. This anticipation requires integrating disparate data sources that are almost impossible for one person to grasp. Anticipating the threat of terrorist attack requires combining information from multiple different sources such as analytic models, simulations, historical data, and user judgments, most of which involve uncertainties.

Technical Approach:

- While threat anticipation can be implemented using several methods, Bayesian Belief Networks (BBNs) have advantages over other methods because they employ consistent reasoning and have representations of uncertainty that are compatible with the more efficient tracking and data fusion algorithms.

Benefit:

- By utilizing network engineering processes that treat the probability distributions of BBN nodes within the broader context of a system development effort as a whole, and not in isolation, we are capable of developing a general threat anticipatory framework that can be used to model a multitude of threat scenarios.

Point of Contact:

Glenn Allgood
(865) 574-5673
allgoodgo@ornl.gov