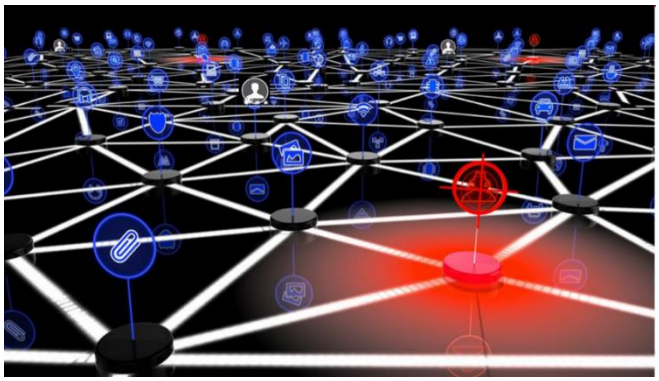
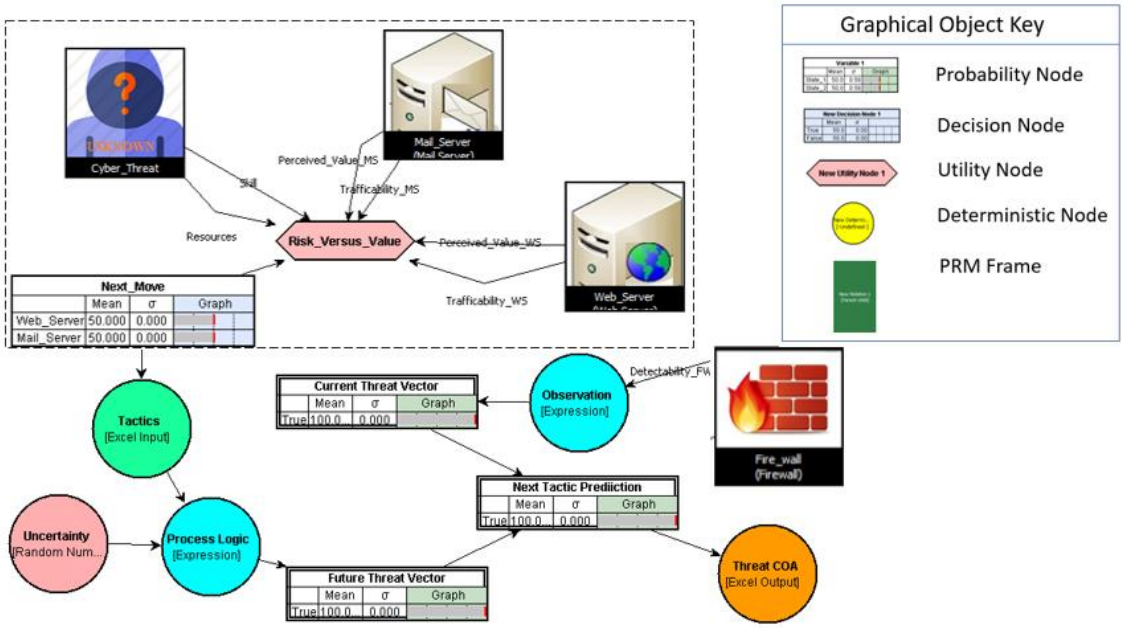
# Cyber Attack Forecasting System (CAFS)

Under USAF and DOE contracts, GCAS and its subcontractors Lockheed Martin, Applied Control Solutions, Carnegie Mellon University and Georgia Tech, have developed a prototype modelling approach to forecast a cyberthreat's maneuvers in compromised networks. The approach is based on techniques used by the DoD for ballistic missile attack warning and assessment, including probabilistic multi-model filters and Multi Hypothesis Method (MHM) within a Bayesian framework.






This proven technology has been leveraged to track and forecast future cyberthreat attack vectors for effective defense of organizational high value assets, and to neutralize those threats. Our framework models different classes of threat actors and their behaviors/capabilities in great detail. The result is the addition of a new dimension to cyber defense of predicting the potential next move in the attack vector.


GCAS LOCKHEED MARTIN ACS APPLIEDCONTROLSolutions Carnegie Mellon University Georgia Tech

1531 Grand Avenue, San Marcos, CA 92078; (760) 591-4227