



# A Cyber Awareness Framework for Attack Analysis, Prediction, and Visualization

University of California Santa Barbara, Berkeley, Georgia Institute of Technology



MURI, Sept., 2009

Email: kemm@cs.ucsb.edu

WWW: <http://www.cs.ucsb.edu/~seclab/cybaware>

October 2009

## MURI Objective

Development of novel situation awareness theories and techniques to obtain an accurate view of the available cyber-assets and to automatically determine the assets required to carry out each mission task

Automatic assessment of attack damage and determination of possible next moves and mission impact

Modeling adversary behavior to predict the threat of future attacks to the success of a mission

A semantically rich presentation environment

## Payoff

- The models, theories, techniques, and tools developed will provide the DoD with a supporting foundation for building a more effective defense against cyber-attacks, especially state-sponsored attacks
- By automating the process of extracting the dependencies between cyber-missions and the needed assets, it will be possible to prioritize attack remediation and optimize human-intensive tasks
- A game-theoretical analysis of attacker actions will enable the construction of forecasts on the nature of the developing threat
- Tailored immersive visualization will enable the efficient evaluation of different courses of action (COAs)

## Scientific/Technical Approaches

- Develop theoretically sound yet practical techniques to automatically analyze network event data to get an up-to-date view of the available cyber-assets
- Develop comprehensive analysis techniques to automatically extract dependency relationships between cyber-missions and cyber-assets
- Extend previous correlation work to associate ongoing attacks and affected cyber-assets to get an accurate understanding of the impact of cyber-attacks
- Develop adversary behavior models to help predict the effects of future attacks launched to prevent successful mission completion
- Leverage novel cognitive science techniques to produce a semantically-rich, easy-to-grasp view of the cyber-mission status

