Cyber Security Econometrics

Cyberspace Sciences & Information Intelligence Research (CSIIR) Group

Goal: Placing a System in the Cone (i.e., operating envelope) and changing its position dynamically to meet mission requirements and to certify operational capability.

- **Problem**
  - Network defense requires layers of strategic thinking
  - Cyber attacks are constantly evolving and increasingly sophisticated

- **Technical Approach**
  - Identify IA controls (e.g., within Defense In Depth levels) and mitigation costs as an investment toward assuring mission success
  - Comprehends different organizational mission needs for all stakeholders
  - Uses comprehensive computational models for stake estimation, Bayesian of dependency relationships and threat analysis

- **Benefit**
  - Comprehensive basis for choosing courses of action that have the highest risk reduction return on investment
  - Reduce the most risks for the lowest cost

POCs: Frederick T. Sheldon Ph.D., 865-576-1339 sft@ornl.gov
Robert K. Abercrombie, Ph.D., 865-241-6537 abe@ornl.gov

IA risk/costs: due to key indicators are available to demonstrate status and potential improvement in the vulnerability profiles of the enterprise.