Behavioral Influence Assessment (BIA) Method for Anticipating Behavior in Cyber Security Applications

Current Work and Potential Future Directions

PI: Asmeret Bier, PhD

abier@sandia.gov
505-845-3247

Cognitive Modeling Department

Sandia National Laboratories

Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2011-4701P.

Organizational Cooperation in Cyber Defense: Current Environment

Little is known about the decision-making among organizations that face cyber threats:

- **Country-sponsored espionage, identity theft, and attacks on critical infrastructure**
- **Organized hacker communities**

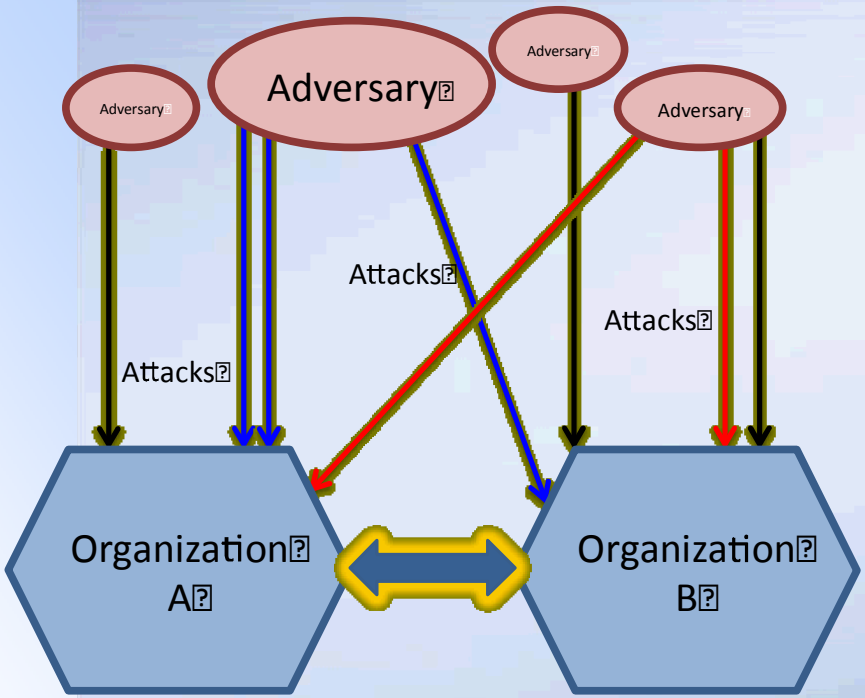
Focus of this effort:

- Develop a computational model for researching the psychological, social, and economic factors underlying decision-making in cyber defense
- Incorporate cultural, cognitive, and institutional constraints and conditions to simulate how cognition and environmental circumstances determine cyber defense strategies and behaviors
- Create a dynamic representation of the decision-making process that incorporates:
  1. individual cognition
  2. the effects of social interaction on individual cognition
  3. interactions between individuals

Current Effort:
Developing Models to Assess Adversary / Cyber Defender Interactions

How to Enhance Cyber Security Effectiveness?

- The **effectiveness of cyber defense might be enhanced** if information and resources were shared among organizations that face similar threats
  - Information about threats
  - Effective defense strategies
  - Personnel with particular expertise

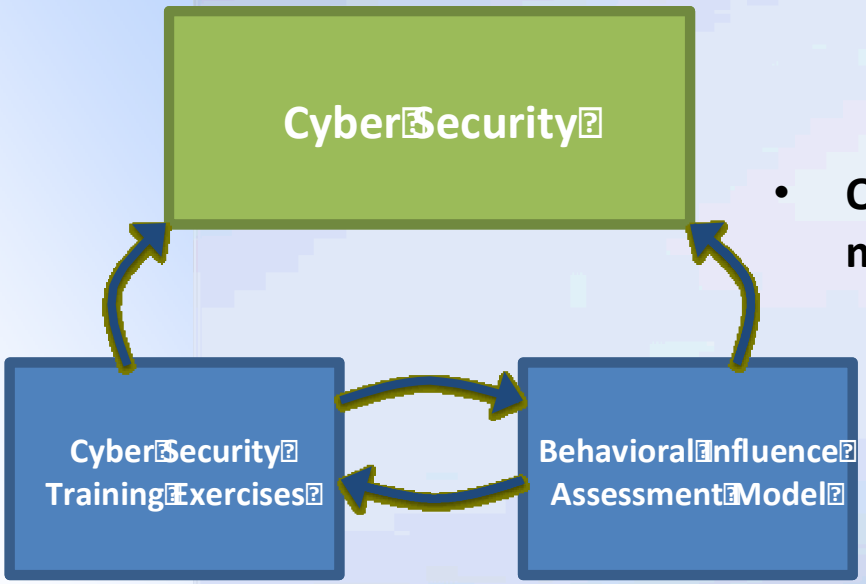


- Motivations to cooperate:
  - Improve security without increasing resources
- Motivations not to cooperate:
  - Potential for embarrassment
  - Group inertia
  - Competitive strategy

Sandia National Laboratories

Organizational Cooperation in Cyber Defense: Potential Outcomes

- **Potential improvements to cyber defense capabilities**
  - May uncover leverage points and management alternatives that could improve cyber defense
    - Examples: resource allocation, allocation and recruitment of people with needed skills, bottlenecks
- **Potential improvements to cyber defense training program**
  - A model will be used to design collaborative challenges that could increase cooperative behavior
- **Opportunity for rigorous validation of a model of human behavior**
  - Using Tracer FIRE exercises as a source of validation data could help to improve accuracy of future models

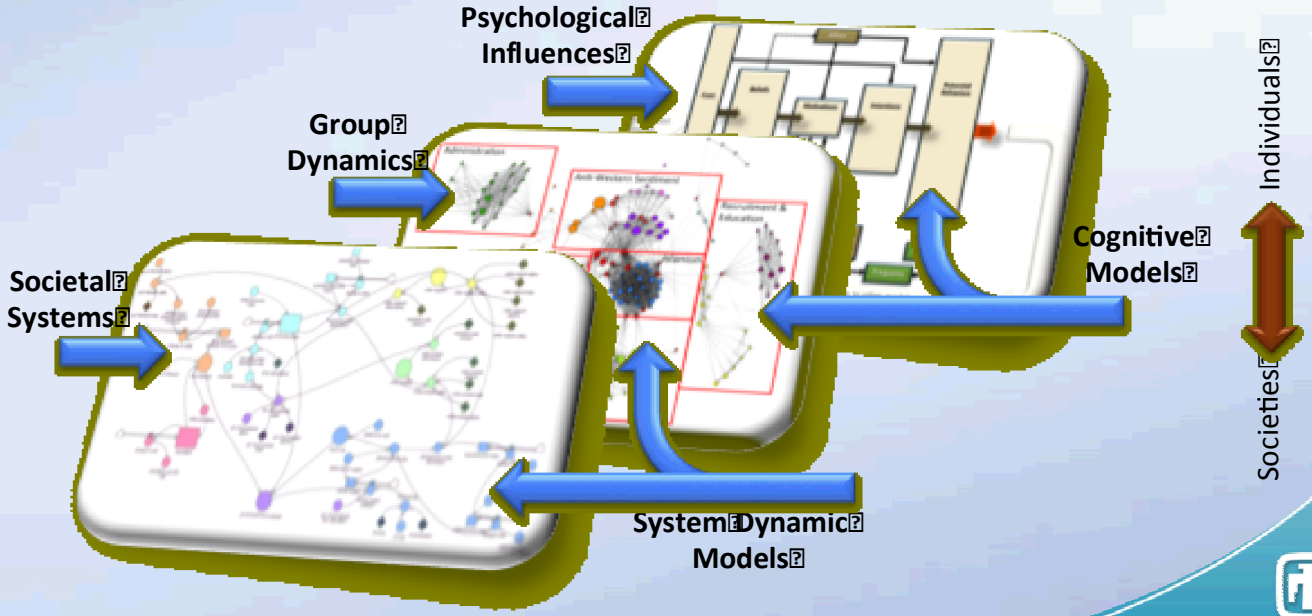


Sandia National Laboratories

Behavioral Influence Assessment (BIA)

The system is founded on established psychological, social, cultural and economic models

- To understand the potential for cooperation in cyber defense, we are using a modified **Behavioral Influence Assessment (BIA)** method
  - Used to improve understanding of the human dimension in order to better anticipate behaviors in response to potential events
  - **Human behavior needs to be examined at multiple scales**
    - Theory domains: psychological, social, historical, anthropological
    - Computational domains: agent-based (cognitive) and system dynamics modeling

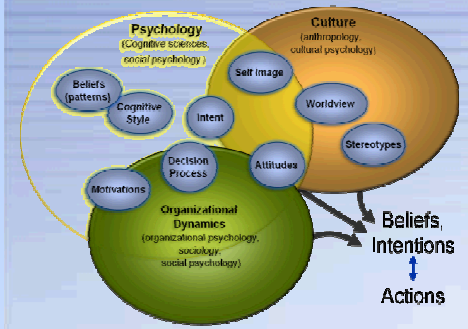


Sandia National Laboratories

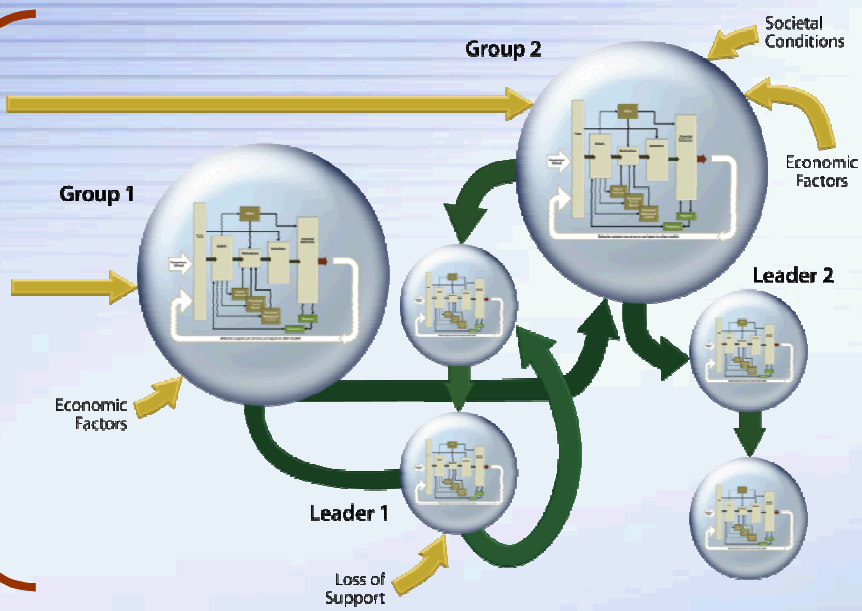
Behavioral Influence Assessment (BIA)

Integration of Cognitive and System Models

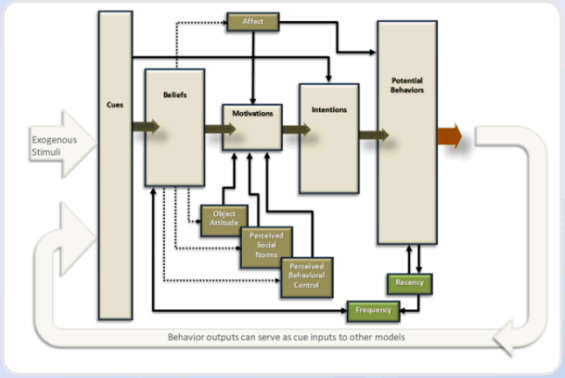
The system is addressing both individual and system-level decision making



System Level



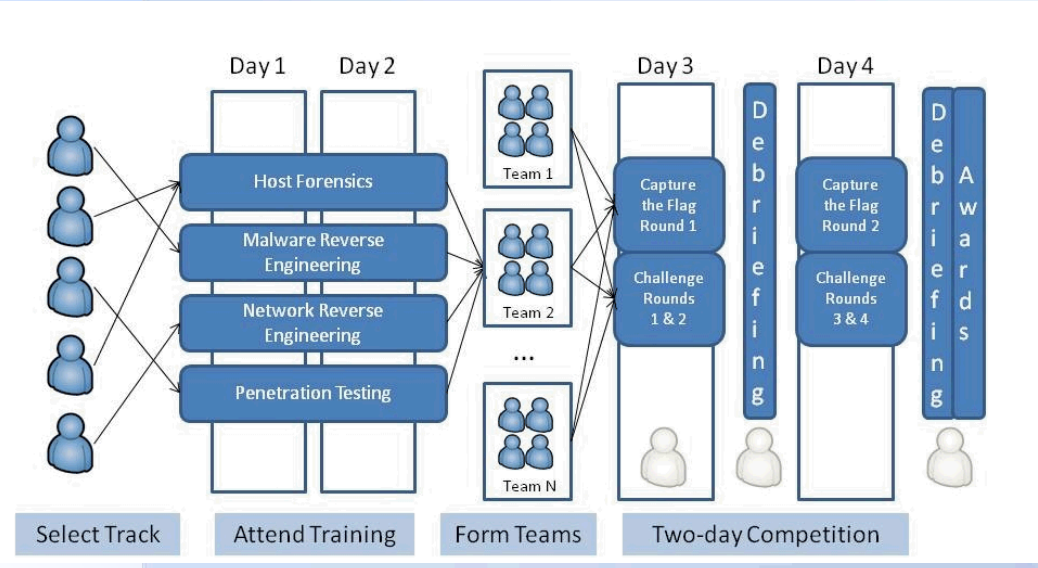
Cognitive Level



Sandia National Laboratories

Tracer FIRE

- Will used data from Sandia's **Tracer FIRE exercises**
  - Training program for cyber defenders
    - Includes competitive cyber defense simulation exercises
    - Organizers are interested in using the training to improve cooperation between participants and organizations
- Tracer FIRE presents **opportunities for the Cyber BIA project**
  - Potential source of data on cognition, interactions, and scenario outcomes
  - Potential for model to improve exercises, and vice versa



Sandia National Laboratories

Potential Future Directions for BIA-related Cyber Research

- How **international relations**, treaties, etc. might affect the character of cyber threats
- **Insider threat**
- Understanding **cyber defenders** and leverage points that might make them more effective
  - Improving team performance in the cyber domain
- **Validating** models of human behavior in the cyber realm

Planned Research: Organizational Cooperation in Cyber Defense

- Phase 1: **Design collaborative challenges for Tracer FIRE**
  - A dynamic simulation model will be created and used to design a true multi-team collaborative challenge to be implemented at Tracer FIRE
    - The model will be conceptual, not strongly validated
    - The exercise will mimic a real life scenario, and will be designed to teach desired skills
- Phase 2: **Model Tracer FIRE exercises**
  - Data collected from Tracer FIRE exercises will create an opportunity for rigorous validation
  - Cooperative and competitive exercises may be compared
- Phase 3: **Model organizational cooperation**
  - Validation data from phase 2 will be scaled up where possible
  - The model will be used to locate leverage points and management alternatives to increase cyber effectiveness