charles river analytics

Cyber Behavior Modeling and Inverse Cognition

Mr. Sean Guarino
Principal Scientist, Director
Human-Centered Artificial Intelligence
Charles River Analytics

About Charles River Analytics

Employee-owned Small Business
Founded in 1983

HQ: Cambridge, MA
Second office: Point Judith, RI

170+ employees and associates

- Established track-record of leading and performing on IARPA and DARPA programs, including leading programs in novel AI techniques and cyber technology development
  - IARPA CAUSE, HIATUS, FOCUS, SHARP, SCITE
  - DARPA SAIL ON, ASIST, CAML, SCEPTER, EDGE, CASE, VET, EA
- Interdisciplinary team bringing expertise in leading-edge AI approaches:
  - Machine learning, symbolic AI, and human-machine interactions
  - Probabilistic programming and deep reinforcement learning
  - Symbolic, probabilistic, and deep learning technologies to push next-generation hybrid AI
  - Intelligent, adaptive behavior modeling and interpretation
  - Innovative user experiences across diverse platforms
- Extensive experience applying AI to support cyber defense
  - Cyber human behavior modeling to support proactive cyber defense and automated cyber OPFOR for training
  - Inverse cognition to interpret observed behavior in the context of cyber behavior profiles, and probabilistically predict how interventions can impact those behaviors
  - Hybrid ensemble approaches to predicting adversary attacks

Cyber Behavior Modeling & Prediction (CyMod)

OBJECTIVE

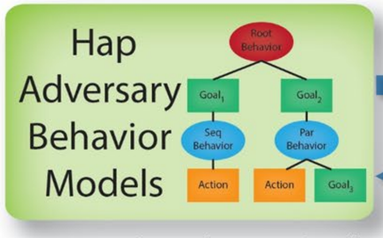
- Use reactive agents to simulate intelligent cyber adversaries, predict likely attack vectors, and prepare proactive defenses against those attacks

TECHNICAL APPROACH

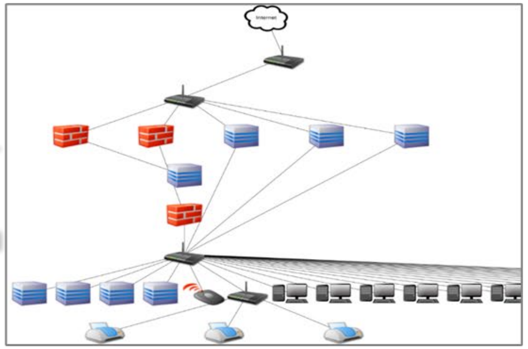
- **Hybrid models of adversary profiles:**
  - Flexible models of cyber adversaries for use in simulation and adversary understanding, including goals, motivations, skill levels, and attacks they execute
  - Flexible attack generation, using systemic functional grammars to capture attack details
- **Agent-Based wargaming** to realistically and intelligently model the pursuit of goals by adversaries
- **Decision aid** that provides insight I not adversaries based on complex cyber data

BENEFIT TO ReSCIND

- CyMod wargaming enables assessment of vulnerabilities and evaluation of defensive options, enabling the identification of high-impact proactive defenses



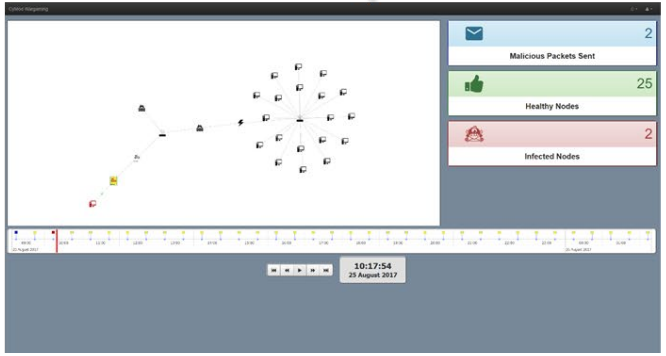
Behaviors/ Queries



Observed Effects

Hap engine dynamically executes behavior in response to simulation environment

How will adversary behaviors react to different defensive postures? What is the best option for proactive defense?



CUSTOMER

- ONR, DARPA, Army RDECOM

Cyber Adversary Discovery Engine (CADE)

OBJECTIVE

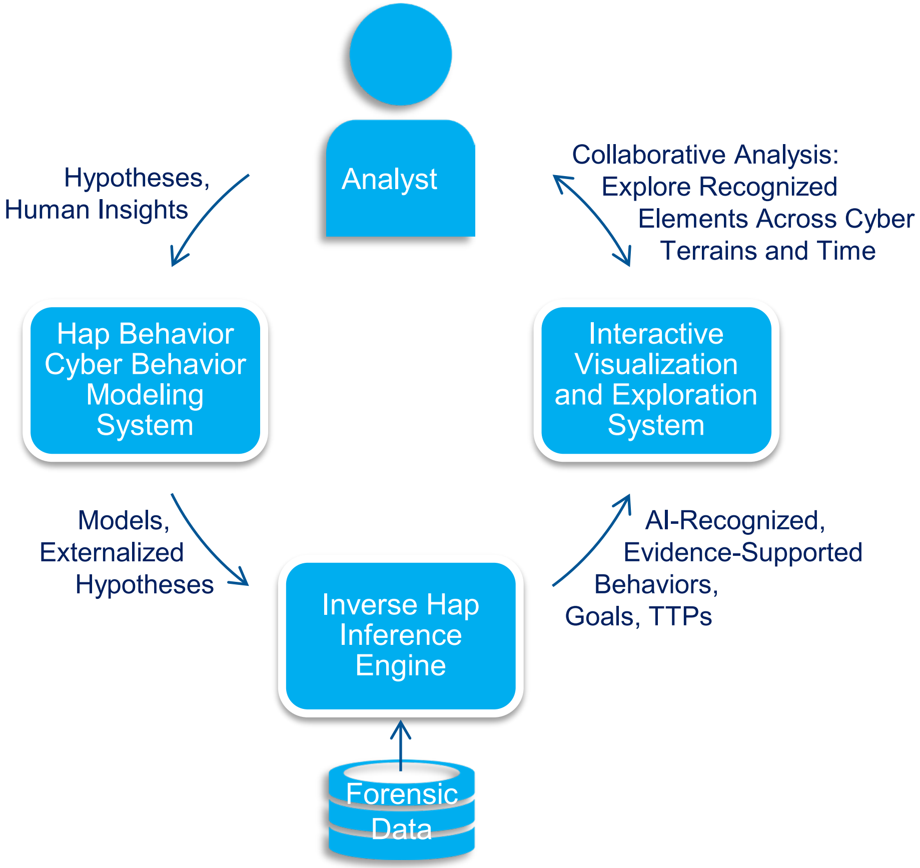
- Perform cyber forensic analysis to understand what approaches and strategies adversaries are using in attacks

TECHNICAL APPROACH

- **Behavior Modeling System:** Uses scalable models to capture complex and multi-tiered adversary behaviors
- **Inverse Cognition:** Combines probabilistic programming and machine learning to recognize and interpret attacker behaviors in data
- **Visualization and Exploration:** Compactly visualizes activity, intuitively organizes it by logical terrain and time, allows interactive exploration with multiple views

BENEFIT to ReSCIND

- CADE provides a thought accelerator for identifying the behavioral tendencies of adversaries based on forensic data, enabling analysts to understand and visualize the behaviors and goals of cyber attacks


Analyst
Hypotheses, Human Insights
Collaborative Analysis: Explore Recognized Elements Across Cyber Terrains and Time
Hap Behavior Cyber Behavior Modeling System
Interactive Visualization and Exploration System
Models, Externalized Hypotheses
AI-Recognized, Evidence-Supported Behaviors, Goals, TTPs
Inverse Hap Inference Engine
Forensic Data

CUSTOMER

- ONR

ReSCIND Contributions and Needs

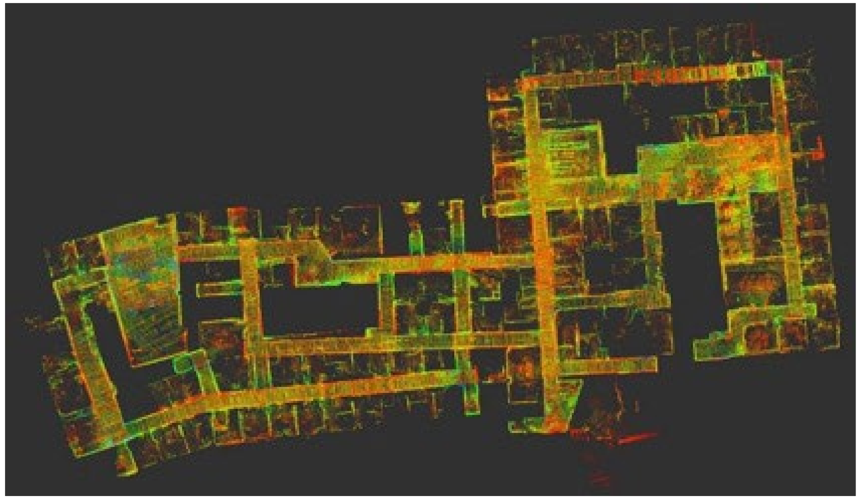
Charles River Analytics provides:

- Cyber adversary behavior modeling
- Inverse cognition to interpret adversary behavior
- Deep learning to adapt to novel behaviors
- Wargaming to predict impacts of interventions
- UX design and development
- Program leadership experience & track record

Seeking partners with experience in:

- Psychology/biases of cyber adversaries & criminals
- Low-level manipulation of cyber defense systems

Contact Information



Charles River Analytics

ReSCIND Contact: Sean Guarino,
sguarino@cra.com
625 Mount Auburn St.
Cambridge, MA 02138
617.491.3474
www.cra.com