

## OUR EXPERTISE AND PROVEN CAPABILITIES

**AUTONOMY**

**ADAPTATION**

**HUMAN/SYSTEM INTERFACE**

## DECISION SUPPORT

### Multi-Future Probabilistic Forecasting

Multiple agents search alternative paths through complex behavior models in parallel

Any-time forecast adjusts in real time to incoming data; runs 10<sup>4</sup>x faster than real time

Yields probability distribution over alternative futures to support ACH and mitigate cognitive anchoring

## BEHAVIOR MODELING

### Cognitive Red-Team Agents

Enables scalable, repeatable wargaming and testing of security and network infrastructure

Learned behavior model exposes novel attack vectors

Agents acting as virtual assistants allow human experts to focus on high level goals

## CYBER SIMULATION

### Cyber Sandbox for Attack & Defense Training

Agent-based cyber ecology provides autonomous adversaries and legitimate users

Dynamic Tailoring adapts adversaries and environment to maximize learning

Constructive sims are readily available for continuous training and evaluation

## Relevant Research to be Leveraged:

## Research Area of Interest:

Current approaches to detecting cyber attacks are *reactive* and *shallow*:

- *reactive* because they focus on what adversaries have done in the past, rather than anticipating what they may do in the future.
- *shallow* because they focus on cyber observables without reasoning about adversaries' goals and objectives.

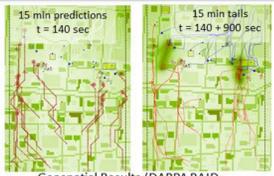
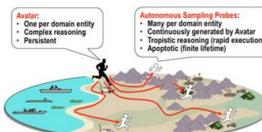
SoarTech combines innovative analytics on observables with sophisticated behavioral models of cyber actors that can support both:

- cognitive reasoning (extending the model through experience and explaining reasoning to humans) and
- Monte Carlo exploration (for probabilistic forecasting over multiple possible futures).

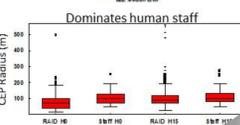
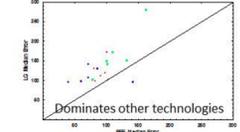
## ENHANCING CYBERSPACE DEFENSE THROUGH BIDIRECTIONAL BEHAVIORAL MODELS

### Probabilistic Forecasting

Mechanism: Monte Carlo search of structured environment (cf. MCTS)



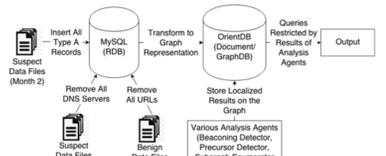
Demonstrated on HTN behavior models (e.g., cyber-attack models)



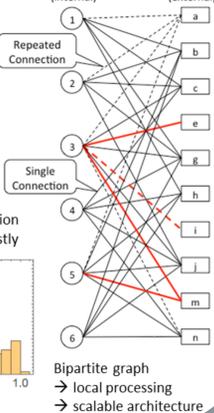
- 10<sup>4</sup>x faster than real time on conventional hardware; parallelizable for further gains
- Generates distribution over possible futures
- Any-time algorithm supports real-time data updates from cyber sensors

### Dynamic Understanding of DNS Data

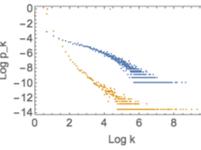
Problem: detect IPTs from DNS Type A records



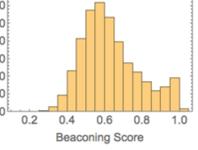
21,250 IPs (internal), 1,638,439 Edges, 782,575 URLs (external)



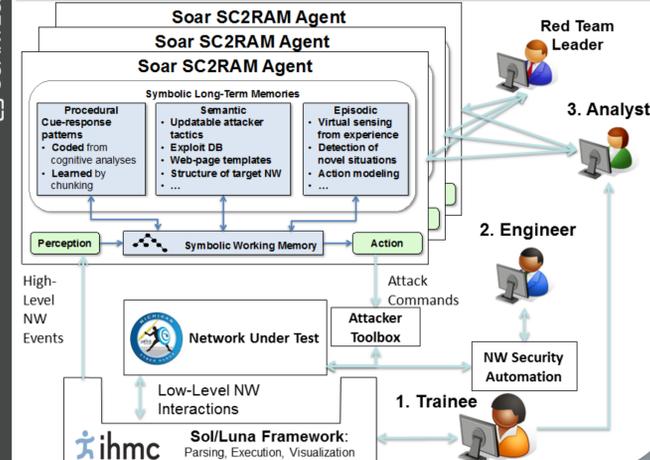
Resulting graph: IP degree (top, blue) and URL degree (bottom, yellow)



Innovative scoring function detects beaconing robustly



### Simulated Cognitive Cyber Red-team Attacker Model



SOARTECH POCs

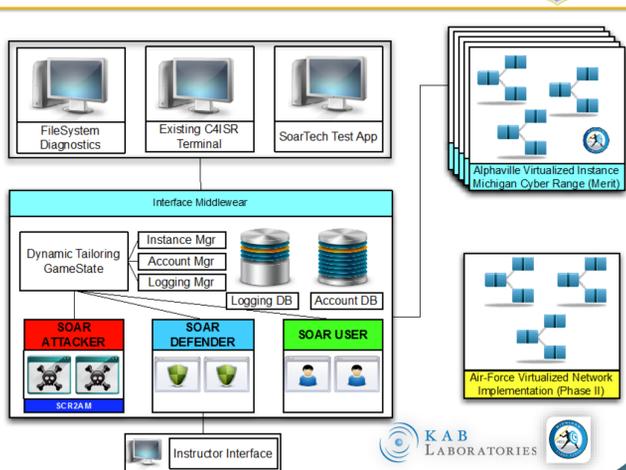
Dylan Schmorow, Ph.D.

Chief Scientist

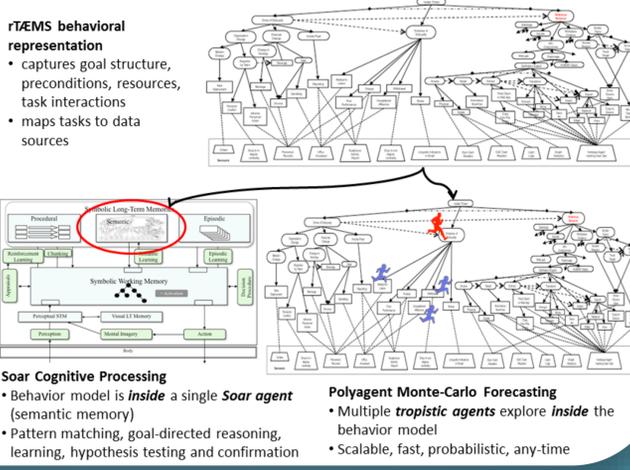
703.424.3138

[dylan.schmorow@soartech.com](mailto:dylan.schmorow@soartech.com)

### Cyber SecurITy INstruction Environment



### Bidirectional Behavior Models



Denise Nicholson, Ph.D., CMSP

Director of X

407.616.7651

[denise.nicholson@soartech.com](mailto:denise.nicholson@soartech.com)

H. Van Dyke Parunak, Ph.D.

Senior Scientist

734.395.3253

[van.parunak@soartech.com](mailto:van.parunak@soartech.com)