Game Theory and Cyber War: Paradigms for Understanding Human Decisions in Cyber Security

Coty Gonzalez (Carnegie Mellon University)

In collaboration with: Noam Ben-Asher, Ph.D.

Post-Doctoral Fellow – CMU; Now: Post-Doctoral Researcher – ARL

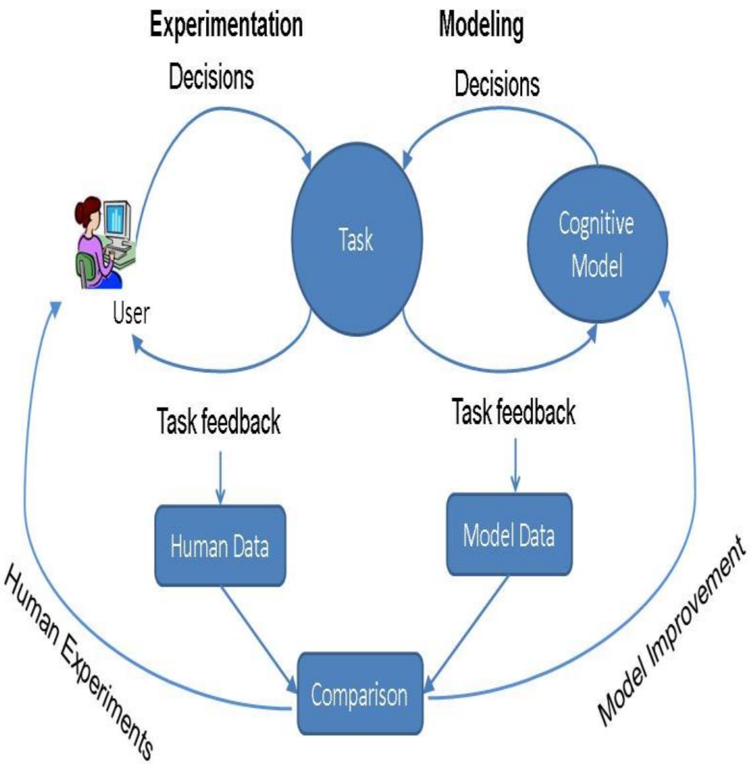
Research Objectives

- **To establish a theoretical model of decision making in cyber-security situations that answers questions such as:**
  - How do humans recognize and process possible threats?
  - How do humans recognize, process and accumulate information to make decisions regarding to cyber-defense?
  - How do human risk perception and tendencies to perceive rewards and losses influence their decisions in cyber-defense?
- **To provide a computational cognitive model of human decision making in cyber-security situations that:**
  - Addresses challenges of cyber-security while accounting for human cognitive limitations
  - Provide concrete measures of a human's decision making and behavior
  - Suggest approaches to investigate courses of action and the effectiveness of defense strategies according to the dynamics of cyber-security situations.

Research Approach

- **Laboratory Experiments:**
  – E.g., The "IDS security game": Study the dynamic process of decisions from experience
- **Cognitive Modeling:**
  – Computational representations of human experiential judgment and decision making process
  – Based on Instance-Based Learning Theory (IBLT, Gonzalez et al., 2003)
  – E.g., IBL models of stopping decisions: dynamic accumulation of evidence before an attack is declared

Involves comparison of data from: computational cognitive models and from humans, both performing the same task



From individual to network behavior

Modeling detection with Instance-Based Learning Theory (Dutt, Ahn, Gonzalez, 2011, 2012)

Defender

Individual (Defender).
Cognitive theories, Memory and individual behavior

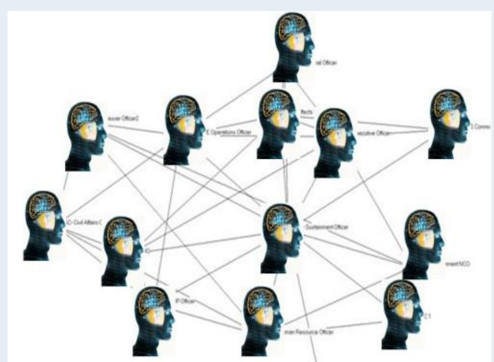
From Individual Decisions from Experience to Behavioral Game Theory: Lessons for Cyber Security (Gonzalez, 2013)

Defender Attacker

Pair (Defender and Attacker).
Interdependencies, Information, Behavioral Game Theory

Perspectives from Cognitive Engineering on Cyber Security. (Cooke et al., 2012).

The Cyber Warfare Simulation Environment and Multi-Agent Models (Ben-Asher, Rajivan, Cooke & Gonzalez, 2014; Ben-Asher & Gonzalez, in Prep).



Cyber War: multiple attackers Defenders

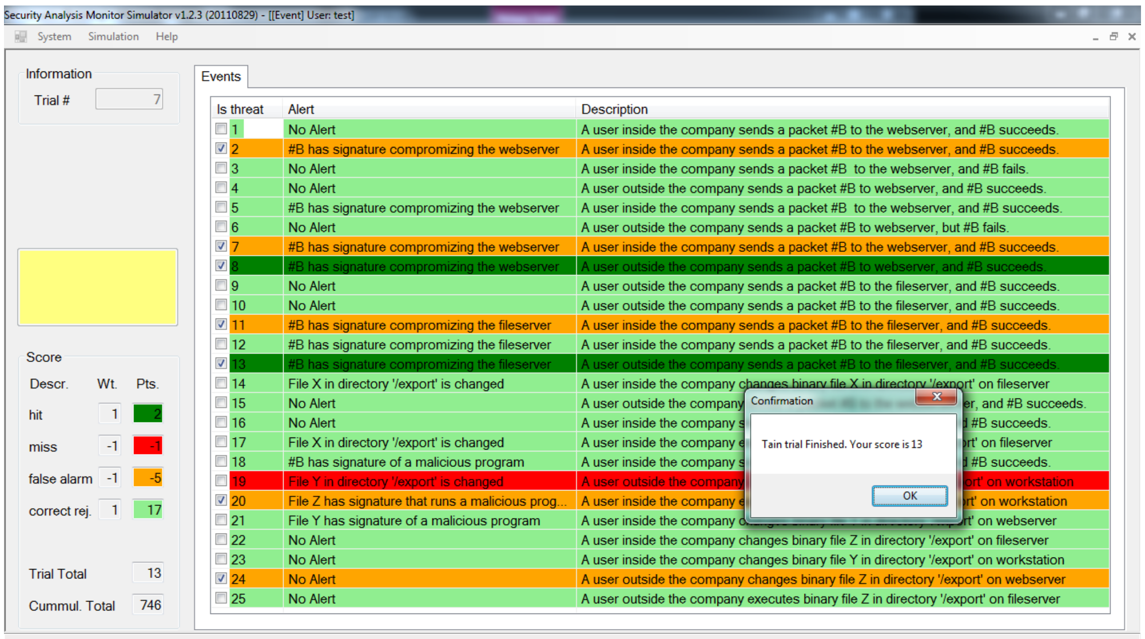
Network (Multiple Defenders and Attackers).
Behavioral Network Theory;
Network science (& topology)
Organizational Learning;
Group Dynamics; Political and Social Science

Experimental paradigms.

Individual Level

Defender

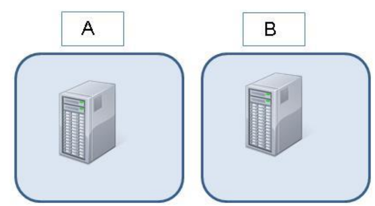
IDS Tool



Is threat	Alert	Description
1	No Alert	A user inside the company sends a packet #B to the webserver, and #B succeeds.
☑ 2	#B has signature compromizing the webserver	A user inside the company sends a packet #B to the webserver, and #B succeeds.
3	No Alert	A user inside the company sends a packet #B to the webserver, and #B fails.
4	No Alert	A user outside the company sends a packet #B to webserver, and #B succeeds.
5	#B has signature compromizing the webserver	A user inside the company sends a packet #B to the webserver, and #B succeeds.
6	No Alert	A user outside the company sends a packet #B to webserver, but #B fails.
☑ 7	#B has signature compromizing the webserver	A user inside the company sends a packet #B to the webserver, and #B succeeds.
☑ 8	#B has signature compromizing the webserver	A user outside the company sends a packet #B to webserver, and #B succeeds.
9	No Alert	A user outside the company sends a packet #B to the fileserver, and #B succeeds.
10	No Alert	A user outside the company sends a packet #B to the fileserver, and #B succeeds.
☑ 11	#B has signature compromizing the fileserver	A user inside the company sends a packet #B to the fileserver, and #B succeeds.
12	#B has signature compromizing the fileserver	A user inside the company sends a packet #B to the fileserver, and #B succeeds.
☑ 13	#B has signature compromizing the fileserver	A user outside the company sends a packet #B to the fileserver, and #B succeeds.
14	File X in directory '/export' is changed	A user inside the company changes binary file X in directory '/export' on fileserver
15	No Alert	A user outside the company ... er, and #B succeeds.
16	No Alert	A user inside the company s... #B succeeds.
17	File X in directory '/export' is changed	A user inside the company ... rt' on fileserver
18	#B has signature of a malicious program	A user inside the company s... #B succeeds.
19	File Y in directory '/export' is changed	A user outside the company ... ort' on workstation
☑ 20	File Z has signature that runs a malicious prog...	A user inside the company ... rt' on workstation
21	File Y has signature of a malicious program	A user inside the company ... rt' on webserver
22	No Alert	A user inside the company changes binary file Z in directory '/export' on fileserver
23	No Alert	A user inside the company changes binary file Y in directory '/export' on workstation
☑ 24	No Alert	A user outside the company changes binary file Z in directory '/export' on webserver
25	No Alert	A user outside the company executes binary file Z in directory '/export' on fileserver

Repeated Decisions from Experience

72% 44% 56%



Should you protect path A or Path B?

A	B
$-40K	
	$-30K
	$-30K
$-40K	
$-40K	
$-0K	
$-40K	
$-40K	$-30K
…	…..

Main behavioral results in: Ben-Asher & Gonzalez, 2014

Experimental paradigms.
Pair Level

Defender Attacker

Game Theory 2x2 Games

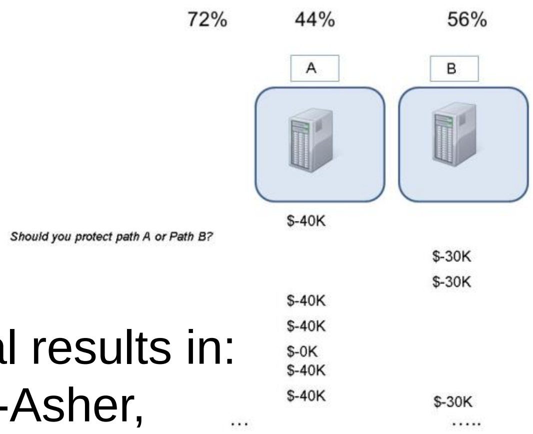
Prisoner's Dilemma

		Player 2 Action	
		D	C
Player 1 Action	D	-1, -1	10, -10
	C	-10, 10	1, 1

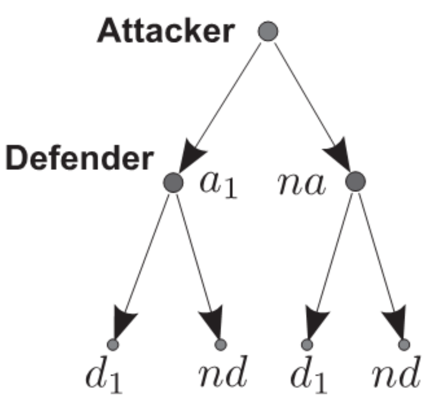
Chicken Dilemma

		Player 2 Action	
		D	C
Player 1 Action	D	-10, -10	10, -1
	C	-1, 10	1, 1

Repeated Decisions from Experience



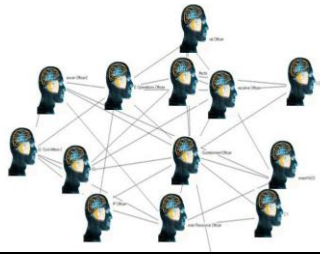
simultaneous and sequential games



		Attacker	
		a	na
Defender	d	\$32, \$0	\$32, \$30
	nd	\$30, \$32	\$30, \$0

Main behavioral results in: Gonzalez, Ben-Asher, Martin & Dutt, 2014

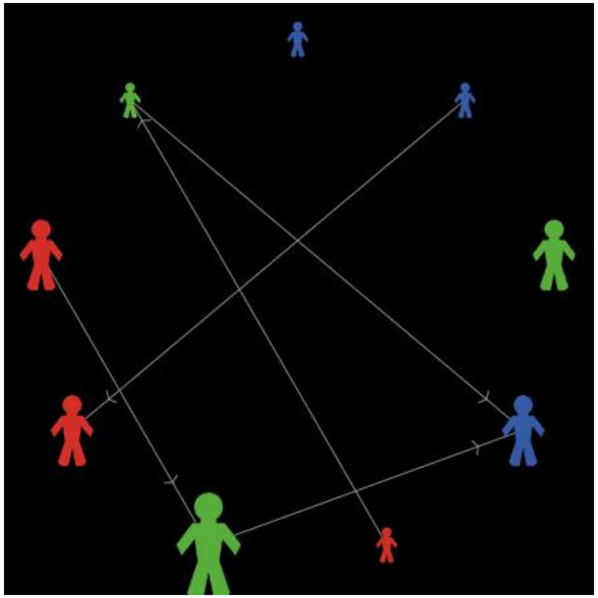
Experimental paradigms. Network Level



Cyber War: multiple attackers/Defenders

- N players – Each player makes decisions whether to: Attack, Defend, do Nothing against each of the other players
- Each player is characterized by two essential attributes:
  - **Power**
  - **Assets**
- Decisions are led by the goal of maximizing own assets.
- Multi-round game.
- Decisions result in an Outcome (Gain or Loss) which changes the Assets available in the following round.
- Actions have a cost: Cost of attack, cost of defend, cost of doing nothing is zero

Repeated Decisions from Experience



The Role of Power and Assets

- Power represents capabilities and abilities:
  - Investment in cyber infrastructure (e.g., computational power); Knowledge and sophistication (e.g., zero-day exploit); Vulnerabilities
  - The ability to execute an action successfully.
    - successfully defend against an attack or successfully execute an attacks against other players
  - $p(success)i = \frac{Poweri}{Poweri+Powerj}$
- Assets are the currency for maximization
  - A players' goal is to maximize his/her own assets
  - An action results in obtaining (losing) a percentage *g* of Assets
  - The outcome in round t changes the value of Assets available in the next round t+1
  - Assets are needed to be part of a war: there are costs (C) to attack and to defend (*D*)
  - A player with no assets is suspended for a fixed number of rounds (r)

Actions and Outcomes (Player *i*, Player *j*, change in Assets)

$$OA_{ij} = p(success)_i * \left(g * Assets_j\right) - C$$

$$OD_{ij} = p(success)_j * (g * Assets_i) - D$$

$$ONA_{ij} = p(success)_j * (g * Assets_i)$$

$$OND_{ij} = 0$$

$$ONN_{ij} = 0$$

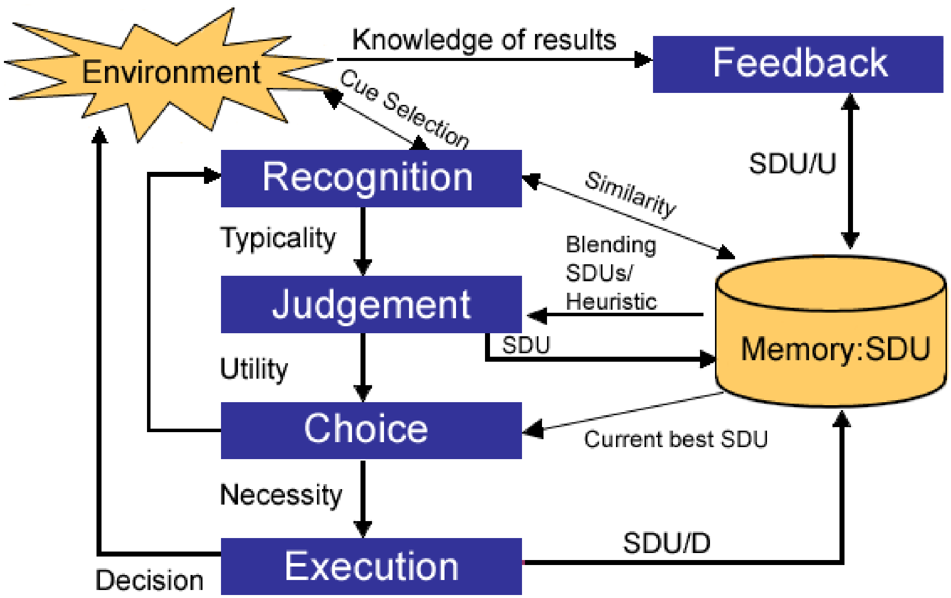
Player j Action

Player i Action

	A	D	N
A	OAij OAji	OAij ODji	OAij ONAji
D	ODij OAji	ODij ODji	ODij ONDji
N	ONAij OAji	ONDij ODji	ONNij ONNji

Dynamic Decision Theory
Instance-Based Learning Theory (IBLT)
(Gonzalez, Lerch, & Lebiere, 2003)

- Proposes a generic DDM cognitive process: Recognition, Judgment, Choice, Execution, Feedback
- Formalizes representations:
  - Instance: tripled: Situation, Decision, Utility (SDU)
  - Relies on mathematical mechanisms proposed by ACT-R
- Represents processes computationally: to provide concrete predictions of human behavior in various task types



IBL model of choice: Individual

1. Each experience combination is created as an instance in memory (e.g. A-10; N-8; A-1; N-5; A-5) when the outcome is experienced
2. Each instance has a memory “activation” value based on frequency, recency, similarity, etc.
3. The probability of retrieving an instance from memory depends on activation
4. For each option, memory instances are “blended” to determine next choice by combining value and probability
5. Choose the option with the maximum blended value

A	N
	
10	
10	
	8
1	
	5
5	
…	…..

A formalization of an IBL model

(Gonzalez & Dutt, 2011; Lejarraga et al., 2012)

Defender

1. **Each Instance** has an Activation: simplification of ACT-R's mechanism (Anderson & Lebiere, 1998):

$$A_{i,t} = ln\left(\sum_{t_i \in \{1,\ldots,t-1\}} (t - t_i)^{-d}\right) + \sigma \, . \, ln\left(\frac{1-\gamma_{i,t}}{\gamma_{i,t}}\right)$$

Frequency **Recency**

Free parameters: *d* : high d-> More recency *Noise:* σ : high s -> high variability

2. **Each Instance** has a probability of retrieval is a function of memory Activation (A) of that outcome relative to the activation of all the observed outcomes for that option given by:

$$P_{i,t} = \frac{e^{A_{i,t}/\tau}}{\sum_j e^{A_{j,t}/\tau}} \qquad \tau = \sigma \cdot \sqrt{2}$$

3. **Each Option** has a Blended Value that combines the probability of retrieval and outcome of the instances:

$$V_j = \sum_{i=1}^{n} p_i x_i$$

4. **Choose** the option with the highest experienced expected value ("blended" value)

Instance-Based Learning Model
Pair Level

Gonzalez, Ben-Asher, Martin & Dutt, 2014

IBL-PD

Game Theory 2x2 Games
Prisoner's Dilemma

Player 2 Action

Player 1 Action		D	C
	D	-1, -1	10, -10
	C	-10, 10	1, 1

- Experiential & Descriptive
  - An instance includes both players' actions and outcomes [C, D, -10, 10], [C, C, 1, 1], [D, C, 10, -10], and [D, D, -1, -1]
- Adding the "other" outcome to the blending equation: $$V_j = \sum_{i=1}^{n} p_{ij}\left(x_{ij} + w o_{ij}\right)$$
- And how do humans weigh the "other" information into their own decisions? (w=f(t))?
  - Dynamic adaptation of expectations $w_t = 1 - Surprise_t$
  - Surprise is a function of the gap between the expected outcome and the outcomes actually received:

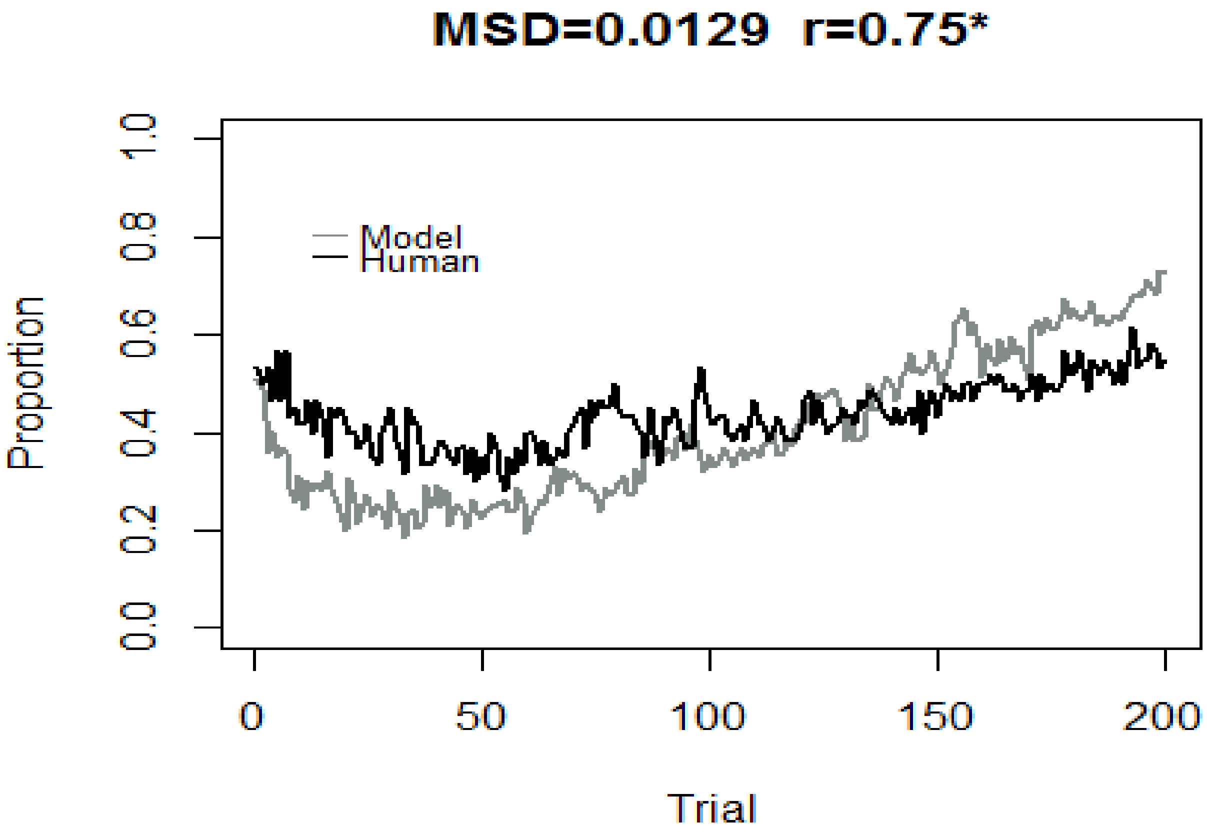
$$Gap_t = Abs[Vj - (Xj + O)]$$

$$Mean\,(Gap_t) = Mean(Gap_{t-1})\left(1 - \frac{1}{200}\right) + Gap(t)\left(\frac{1}{200}\right)$$

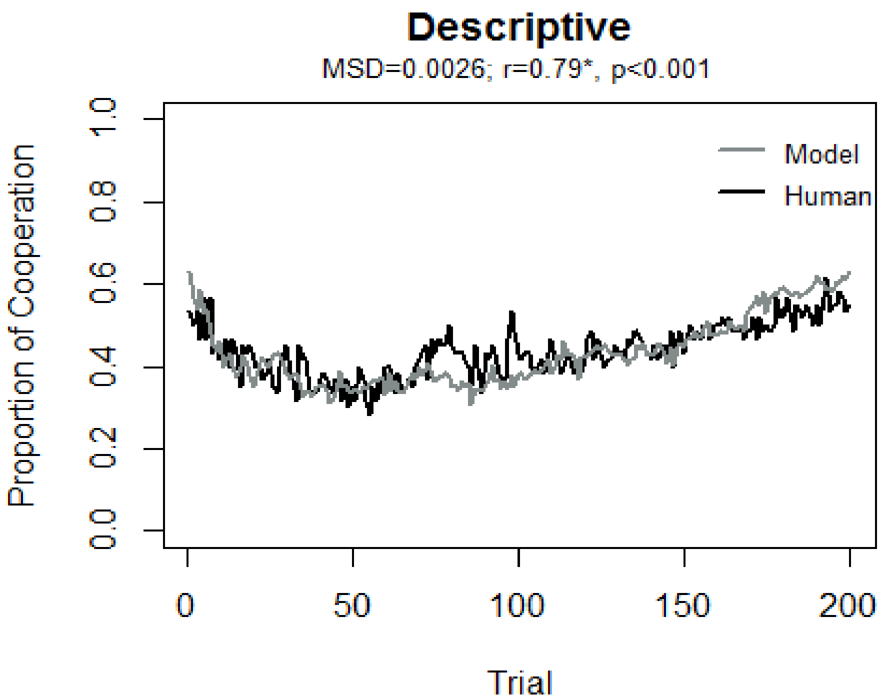
$$Surprise_t = \frac{Gap_t}{[Mean(Gap_t) + Gap_t]}$$

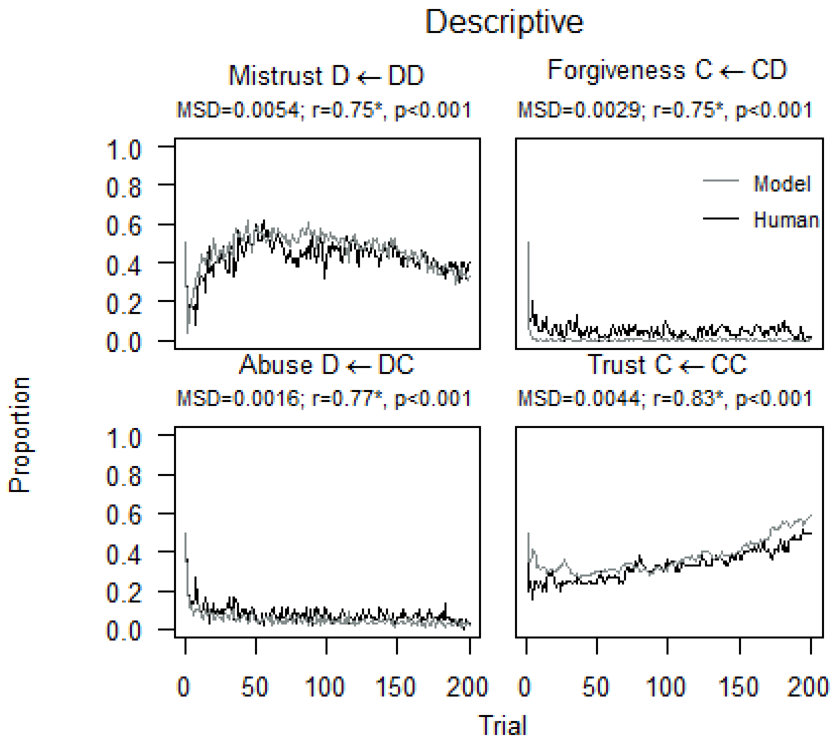
Predictions against human data

Main behavioral results in: Gonzalez, Ben-Asher, Martin & Dutt, 2014

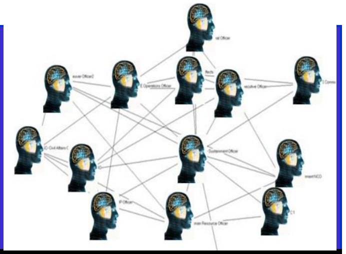


Fitting the model's parameters to data



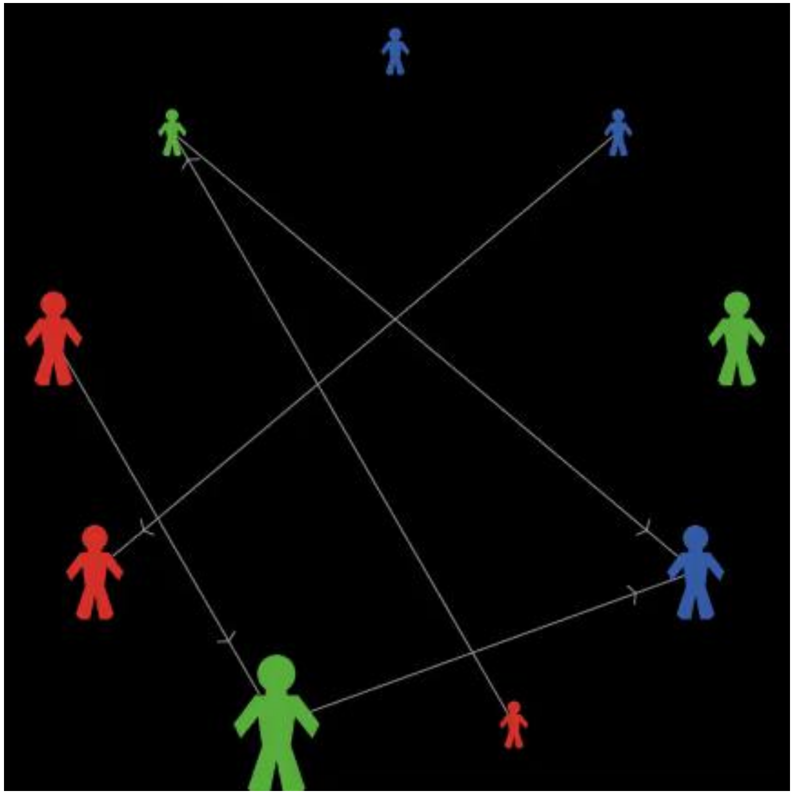


Instance-Based Learning Network Level



Cyber War: multiple attackers/Defenders

- Each active agent evaluates the other active agents, one at a time
- Each active agent is evaluated by calculating the possible outcome from attacking it
- Then the agent evaluates how likely it is to actually obtain that outcome
- Each agent selects to attack the agent that would yield the highest utility of attacking
- Makes a decision whether to attack or not, according to the highest blended value of the two types of actions "attack" or "no attack"

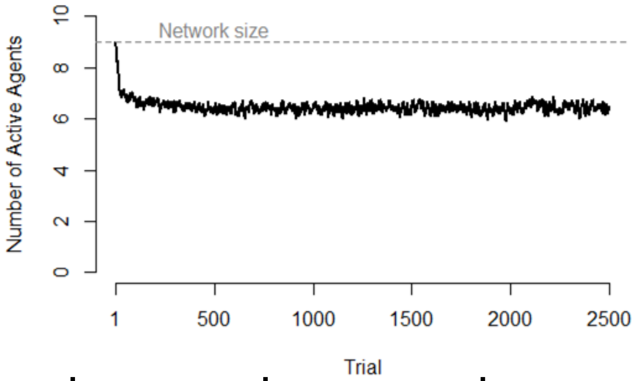


Simulations and Results

- A network with 9 different types agents
  - Power (High, Medium, Low)
  - Asset Value (High, Medium, Low)
- Each network was simulated for 2500 trials.
- 60 simulations with the same network setting.
- Successful attack yields 20% of the opponent's assets
- Downtime - An agent without assets is suspended for 10 trials
- IBL Agents with d=5 and σ = 0.25

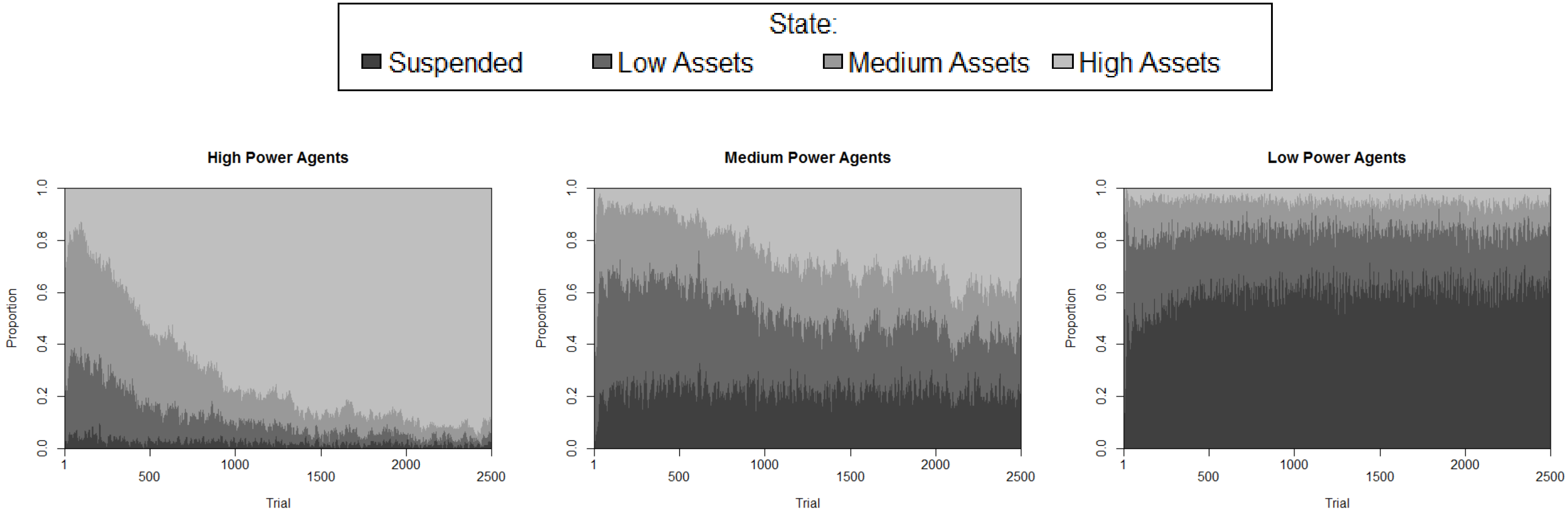
Active Agents in the Network

- Within 500 trials the number of active agents becomes stable (mean=6.42, SD=0.16)
- Power influenced the overall proportion time agents were suspended:
  - High power agents **2%** of the trials
  - Medium power agent **19%** of the trials
  - Low power agents **50%** of the trials



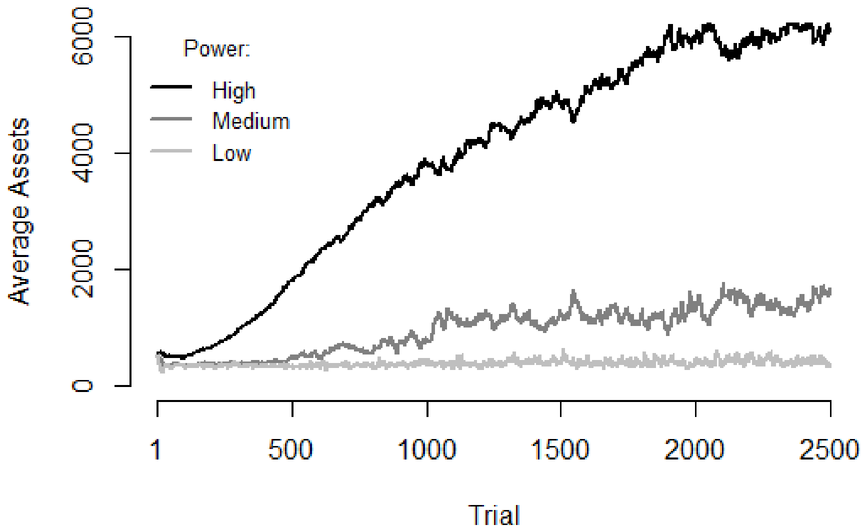
- High power allowed agents to maintain an active state, however even high power did not guaranty that an agent will be active 100% of the time

Role of Power over dynamics of Assets



Power influenced the dynamics of agents' state and the network heterogeneity

Power and Assets Accumulation



- High power allowed accumulation of assets starting from early stages of the interaction
- The difference between Medium and Low power agents was evident only after 500 trials
- The relationship between accumulated assets and power is not linear

Conclusions

- Significant progress in the development of theoretical models of decision making in cyber-security situations. Theoretical models evolved from
  - Individual (Instance-Based Learning Theory)
  - Pair-level (Behavioral Game Theory and IBL-Game Theory)
  - Network Level (Network Theory and IBL-Network)
- Development of experimental paradigms that served to collect human data and conclude with behavioral phenomena:
  - IDS tool, Binary choice repeated decisions, Game theory games, CyberWar game
- Development of computational cognitive models based on theoretical developments including
  - IBL model
  - IBL-PD
  - Cyber War simulations