Understanding Cyber Situational Awareness in a Cyber Security Game involving Recommendations

Palvi Aggarwal[1, 2], Frederic Moisan[2], Cleotilde Gonzalez[2], Varun Dutt[1]

[1]Applied Cognitive Science Lab, Indian Institute of Technology, Mandi, India
[2]Dynamic Decision Making Lab, Carnegie Mellon University, Pittsburgh, USA

ABSTRACT

Intrusion Detection Systems (IDSs) help in creating cyber situational awareness for defenders by providing recommendations. Prior research in simulation and game-theory has revealed that the presence and accuracy of IDS-like recommendations influence the decisions of defenders and adversaries. In the current paper, we present novel analyses of prior research by analyzing the sequential decisions of defenders and adversaries over repeated trials. Specifically, we developed computational cognitive models based upon Instance-Based Learning Theory (IBLT) to capture the dynamics of the sequential decisions made by defenders and adversaries across numerous conditions that differed in the IDS's availability and accuracy. We found that cognitive mechanisms based upon recency, frequency, and variability helped account for adversarial and defender decisions better than the optimal Nash solutions. We discuss the implications of our results for adversarial-and-defender decisions in the cyber-world.

Keyword: Behavioral cyber-security; simulated defenders; simulated adversary; Intrusion detection systems; situation awareness; alerts; cyber-security game; Instance-based Learning Theory.

1 INTRODUCTION

Recently, GitHub's code hosting website was hit with the largest-ever distributed denial of service (DDoS) attack that generated an unmanageable amount of Internet traffic in a very short time (Khandelwal, 2018). Similarly, a group named RASPITE targeted the electric utility sector in America to cause largescale blackouts (Newsweek, 2018). Literature reveals that the hacking groups in these cyber-attacks shared information among each other about the vulnerabilities present in networks, exploitable targets, and backdoors available to enter networks (Hausken, 2017a; 2017b). This information sharing caused cascading failures in networks, where the failure of one element in a network disconnected the whole network (Chen, Du, Cao, & Zhou, 2015; Wu, Tang, & Wu, 2016). Overall, due to the increase in cyber-attacks, there is an urgent need for cyber situational awareness, i.e., the perception, comprehension, and projection of situations involving cyber threats and the protection of cyber infrastructure against these threats (Situation Awareness, 2018; McAfee, 2016; Endsley, 2017).

One way of protecting cyber infrastructure and preventing cyber-attacks is via intrusion detection systems (IDSs), systems that alerts defenders about potential cyber threats (Dutt, Moisan, & Gonzalez, 2016). According to Dutt, Moisan, and Gonzalez, (2016), IDSs may be present in certain network infrastructures or they may be absent. Also, IDSs may have varying levels of accuracies. For example, sometimes IDSs may be very accurate or very inaccurate; whereas, sometimes IDSs may work at the chance level and they may simply be uninformative (Dutt, Moisan, & Gonzalez, 2016).

In this paper, we investigate how the presence and accuracy of IDSs influence the cyber situational awareness of defenders and adversaries, i.e., when these stakeholders make sequential trial-by-trial decisions. The sequential analysis allows us to investigate the dynamics of decision-making over trials. Furthermore, we also evaluate how certain cognitive models with different cognitive mechanisms account for the dynamics of human behavior over trials in the different conditions that vary the presence and accuracy of IDSs.

In what follows, first, we discuss related work in literature to highlight the contribution of this study. Second, we discuss a cyber-security game involving IDS-like recommendations and Nash equilibria in this game. Third, we perform novel sequential analyses of the data collected in the cyber-security game. Fourth, we develop cognitive models and test the ability of these models in accounting for sequential decisions of adversaries and defenders compared to the Nash predictions. Finally, we discuss the implication of our results for decision-making of adversaries and defenders in the real world.

2 RELATED WORK

Hausken and Levitin (2012) have provided a framework for understanding the cyber-attack process, which involves both attackers (or adversaries: Dutt, Ahn, & Gonzalez, 2013; Jajodia, Liu, Swarup, & Wang, 2010) and security-analysts (or defenders: Dutt et al. 2013; Jajodia et al., 2010). According to Hausken et al. (2012) the process of attacking and defending significantly relies on system structure, defense measures, and attack tactics and circumstances (Hausken et al., 2012). System structure defines the target, which could be a single element, multiple elements, interdependent systems, and networks (Hausken et al., 2012). Defense measures could be protection, prevention, separation of elements, and deception (Hausken et al., 2012). Adversaries can choose various attack tactics and circumstances such as random attack, attacking single or multiple units, and consecutive attacks (Hausken et al., 2012).

Under the protection defense measure in the Hausken et al., (2012)'s framework, there are several ways in which defenders could gather cyber situational awareness and to protect networks and data from cyber-attacks. For example, data could be protected by defenders in the network by dividing it into multiple blocks and storing these blocks on distributed servers (Levitin, et al., 2012). To prevent loss of information, these data blocks can further be replicated on multiple servers (Levitin, et al., 2012). Similarly, another way in which defenders could protect networks and data from cyber-attacks is via information sharing about the recent incidents, zero-day exploits, and service dependencies among organizations (Bloem, Alpcan, & Basar, 2006).

Although data blocking on distributed computers and information sharing are ways of protecting networks and data from cyber-attacks, another way to prevent the majority of attacks is via IDSs (Dutt, Moisan, & Gonzalez, 2016). The IDSs and their alerts may help provide defenders with cyber

situational awareness, i.e., IDSs may help defenders to perceive, comprehend, and project an emergent cyber-attack situation in the network (Endsley, 2017).

Mostly, defenders may not be able to directly observe adversaries' actions on the network (Jajodia et al. 2010; Endsley, 2017; Roy et al., 2010). Thus, defenders often need to rely upon alerts from IDSs to organize and structure network activity; and, to help make network information relevant, meaningful, and useful (Gonzalez, Ben-Asher, Oltramari, Lebiere, 2014). However, accuracies of IDSs are questionable; false-alarms (reporting an attack when there is none) and misses (not reporting an attack when there is one) are common (Laszka, Abbas, Sastry, Vorobeychik, & Koutsoukos, 2016), and it is up to the defender to rely or not on recommendations provided by the IDS. Adversaries also know that IDSs are not fault-free (Bhatt, Koshti, Agrawal, Malek, & Trivedi, 2011) and they may also take advantage of the knowledge about inaccuracies present in IDSs.

Dutt, Moisan, and Gonzalez (2016) investigated the role of presence and accuracy of IDS-like alerts in a simulated game where human players played the role of defenders and adversaries. In terms of Hausken and Levitin (2012)'s framework, the system structure considered was an abstract network, the defense measure was protection, and the attack tactics were consecutive attacks (Hausken et al., 2012). These researchers analyzed the aggregated decisions made by both defender and adversary players and compared them against game-theoretic Nash solutions. However, these authors did not investigate how the sequential decisions of defenders and adversaries emerge over trials in the presence of IDS-like recommendations in cyber-security games.

In this paper, we build on the research reported by Dutt, Moisan, and Gonzalez (2016) and the cognitive modeling literature involving Instance-based Learning Theory (IBLT), a theory of decisions from experience (Arora & Dutt, 2013; Aggarwal, Moisan, Gonzalez, & Dutt, 2018; Dutt, Ahn, & Gonzalez, 2013; Kaur & Dutt, 2013). Specifically, we provide a novel analysis of Dutt, Moisan, and Gonzalez (2016)'s data to investigate how the presence and accuracy of IDSs influence the cyber situational awareness, i.e., the sequential over-trial decisions of defenders and adversaries. The sequential analysis allows us to investigate the dynamics of decision-making over trials. Next, we evaluate how Instance-Based Learning (IBL) models with different cognitive assumptions account for the dynamics of human behavior over trials in the different conditions that vary the presence and accuracy of IDS. Also, we investigate the performance of

IBL models compared to optimal Nash predictions in games involving IDS-like recommendations.

3 THE CYBER-SECURITY GAME WITH IDS RECOMMENDATIONS AND NASH EQUILIBRIA

IDSs may help defenders by alerting them about potential cyber threats in the network (Gonzalez et al., 2014; Aggarwal et al., 2018). However, IDSs are not 100% accurate in detecting cyber threats, and they may not be present at all times. Thus, defenders need to use their judgment and experience to decide whether to rely upon alerts from IDSs (Gonzalez et al., 2014). The presence of IDSs and the inaccuracies present in them may also influence the decision-making of defenders and adversaries (Bhatt et al., 2011).

Dutt, Moisan, and Gonzalez (2016) experimentally investigated the impact of the presence and accuracy of IDS alerts on the attack and defend decisions made in a simulated cyber security game. The experiment involved an online system randomly pairing two human players across one of the two roles, adversary or defender, where the adversary performed as a "hacker" player and the defender performed as an "analyst" player. Hacker and analyst pairs were randomly assigned to one of the following two between-subject conditions: IDS-absent (N = 20 pairs) and IDS-present (N = 80).

In the IDS-absent condition, the IDS was not present on any trials. In the IDS-present condition, the IDS was present on all trials. The IDS-present condition was further split into three between-subject conditions that varied the IDS accuracy: 10% accuracy (known as informative, N = 25 pairs); 50% accuracy (known as uninformative, N = 29 pairs); and, 90% accuracy (known as informative, N = 26 pairs).[1] Each condition involved 100 repeated trials, wherein each trial both hackers and analysts made attack-and-defend decisions. In the IDS-present conditions (see Figure 1), first, the hacker chose to attack or not-attack the network. The hacker's decision was followed by an IDS alert to the analyst about whether the network event was a cyber-threat or not (cyber-threats meant an attack on the network). Based on the IDS alerts, the analyst chose to defend or not defend the network. Once the analyst had made her choice, both players were provided with information about the actions taken and payoffs obtained by them and their

[1] If the IDS was X% accurate, then on X out of the 100 trials, the IDS responded correctly: It generated threat alerts for threat events and non-threat alerts for non-threat events. Thus, on 100 – X trials, the IDS responded incorrectly: It generated threat alerts for non-threat events and non-threat alerts for threat events.

opponent, IDS alerts in the last trial (if IDS was present), and the player's own cumulative payoff (opponent's cumulative payoff was not shown) (see Figure 1).

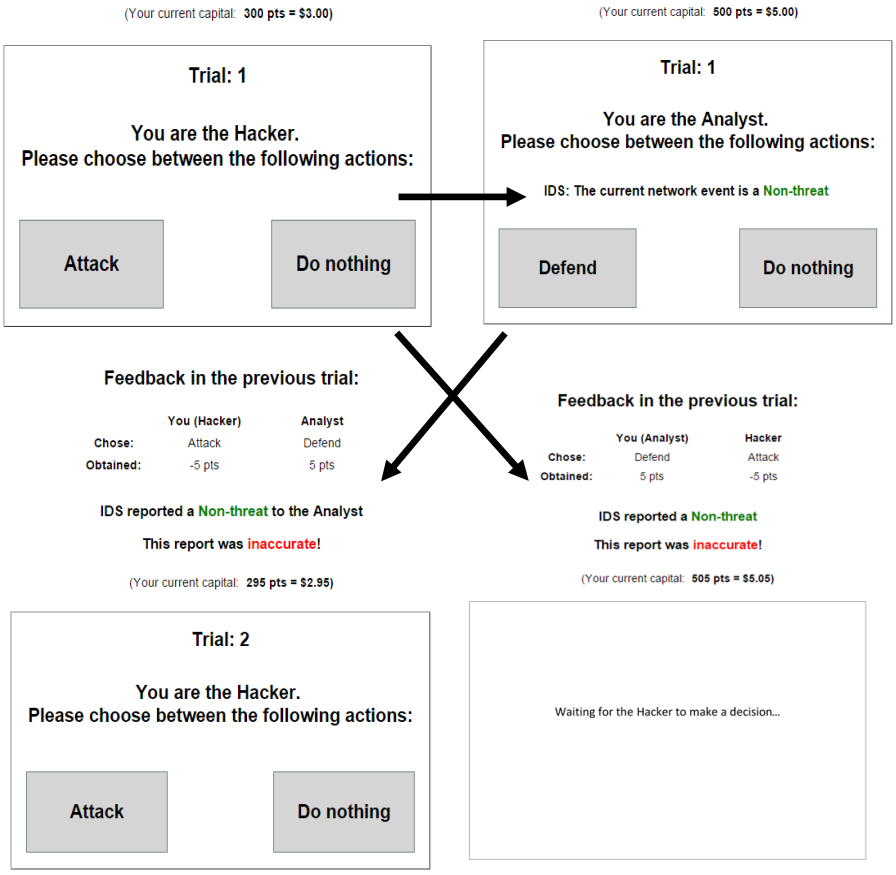


Figure 1. The dynamics of a trial in one of the IDS-present conditions in the cyber-security game. This figure is adapted from Dutt, Moisan, and Gonzalez (2016)

Figure 2 shows the payoff-matrix used in a game between the hacker and the analyst by Dutt, Moisan, and Gonzalez (2016). As seen in Figure 2, when hackers and analysts took not-attack and not-defend actions, respectively, then both players got 0 points. In this case, as no effort was made by hackers to attack the network and there was no evidence of attack for an analyst to defend, both these players did not get any rewards or punishments. However, if the hacker took an attack action while the analyst

took a not-defend action, then the hacker got +10 points (for a successful attack and information gain) and the analyst got -15 points (for information lost due to not defending when there was an attack). In contrast, if the analyst took a defend action and the hacker took a not-attack action, then the hacker got 0 points (no effort to attack the network and thus no rewards or punishments), and the analyst got -5 points (for wasted effort in defending the network when there was actually no attack). Finally, if the analyst took a defend action while the hacker took an attack action, then the hacker got -5 points (for getting caught while attacking the network) and the analyst got +5 points (for successfully defending the network from a cyber-attack).

		Hacker	
		Not Attack	Attack
Analyst	Not Defend	0, 0	-15, +10
	Defend	-5, 0	+5, -5

Figure 2. The payoff-matrix used in the cyber-security game by Dutt, Moisan, and Gonzalez (2016). The first and second payoffs in each cell correspond to Analysts and Hackers, respectively.

In an experiment with the cyber-security game, Dutt, Moisan, and Gonzalez (2016) found that the proportion of attack and defend actions were similar when the IDS was absent and when it was uninformative (50% accurate). However, the proportion of defend actions reduced when the IDS was present and when it was mostly 10% or 90% accurate. The proportion of attack actions were not influenced by the IDS's presence and accuracy.

Nash equilibrium is a fundamental concept in game theory and it is a widely used method of predicting the optimal decisions in strategic interactions involving two or more players (Camerer, 2003). According to Camerer (2003), a pure-strategy Nash equilibrium is an action profile with the property that no single player can obtain a higher payoff by deviating unilaterally from this profile. In the absence of a pure-strategy Nash equilibrium, players may be able to choose random probability distributions over their set of actions. Such randomizations over the set of actions are referred to as mixed strategies. According to Camerer (2003), a mixed strategy Nash-equilibrium is then a mixed-strategy profile with the property that no single player can obtain a higher expected payoff by deviating unilaterally from this profile.

Dutt, Moisan, and Gonzalez (2016) calculated the mixed-strategy Nash equilibriums using the Gambit software (McKelvey, McLennan, & Turocy, 2006) in the cyber-security game. When the IDS was absent, then, according to a mixed-strategy Nash equilibrium, the hacker's probability of attack actions equaled 20%; and, the analyst's probability of defend actions equaled to 67%. When the IDS was present with a 50% accuracy, then the Nash probability of attack actions equaled 20% and the Nash probability of defend actions equaled to 67%. Similarly, when the IDS was present with a 10% accuracy, then the Nash probability of attack actions equaled 03% and the Nash probability of defend actions equaled 09%. When the IDS was present with a 90% accuracy, then the Nash probability of attack actions equaled 03% and the Nash probability of defend actions equaled 09%. The appendix details how these Nash proportions were computed for different IDS accuracies. Although the mixed-strategy Nash equilibria are determined for a single trial of the game, these optimal solutions still hold in the case of a repeated (iterative) game involving several trials. In fact, both players following the above strategies in every trial still correspond to the Nash equilibrium in the large game involving N trials (no one is better-off deviating from it in any single trial of the finite game).

4 SEQUENTIAL ANALYSES OF DYNAMIC DECISIONS IN CYBER-SECURITY GAME

We performed sequential analyses of data collected by Dutt, Moisan, and Gonzalez (2006) to investigate the influence of IDS' presence and accuracy on the cyber situational awareness, i.e., the over-trial decisions of adversary and defender players. When appropriate, we also compared human decisions to the Nash equilibrium solutions and predictions from an IBL model. In agreement with the prior literature (Maqbool, Makhijani, Pammi, & Dutt, 2017), we used mixed-factorial ANOVAs to analyze the influence of IDS' presence and its accuracy on the over-trial proportion of attack actions and the proportion of defend actions. The proportion of attack and defend actions have been traditionally used in literature to document the adversarial and defender behavior, respectively (Aggarwal, Moisan, Gonzalez, & Dutt, 2018; Dutt, Ahn, & Gonzalez, 2013; Kaur & Dutt, 2013; Maqbool, Makhijani, Pammi, & Dutt, 2017). These proportions were computed by first coding each attack and defend the action as 1.0 and each not-attack and not-defend as 0.0 for each participant in each trial. Next, the proportion of attack or defend actions were computed for a trial by averaging the 1.0s and 0.0s across all participants performing in the trial. In agreement with the literature, we computed the average proportion of attack or defend actions per block, where a block consisted of a contiguous sequence of 10-trials.

The average proportion of attack or defend actions per block were computed by averaging these actions across the 10-trials in the block. Also, we performed t-tests to compare human and Nash proportions. Statistical analyses were performed at an alpha level of .05 and a power threshold of 0.8.

4.1 Learning and Choices over Blocks

First, we investigated the cyber situational awareness via the change in proportions of attack and defend actions over blocks. Figure 3 shows the average proportions of attack and defend actions across 10-blocks in different experimental conditions.[2] Overall, the proportion of attack actions decreased significantly over blocks (F (9, 864) = 22.56, $p < .001$, η_p^2 = 0.19), and this behavior was similar across different levels of IDS presence and accuracy (F (27, 864) = 1.08, p = 0.35, η_p^2 = 0.03). Similarly, the proportion of defend actions decreased significantly over blocks (F (9, 864) = 13.89, $p < .001$, η_p^2 = 0.13); but, in this case, the presence and accuracy of the IDS significantly influenced how this decrease occurred (F (27, 864) = 2.56, $p < .001$, η_p^2 = 0.074). As seen in Figure 3b and 3d, the proportion of defend actions decreased significantly over blocks in the informative IDS (10% accuracy and 90% accuracy) conditions. However, the proportion of defend actions did not change significantly over blocks when the IDS was absent or it was uninformative (50% accuracy) (see Figure 3a and 3c).

To further understand the learning process, we compared the average proportion of attack and defend actions in the last two rounds against the Nash proportions across different conditions. The dotted lines in Figure 3 show the Nash proportions for adversary and defender participants in different conditions. One expects that the proportion of actions would show stable preferences by the last 2-blocks as participants would have already undergone an interaction over 80-trials. As expected, the average proportion of attack actions in the last 2-blocks were not significantly different from their Nash equilibriums (0.20) when the IDS was absent (0.21) (t(19) = 0.08, p = 0.94) and when the IDS was uninformative (50% accurate) (0.25) (t(28) = -1.11, p = 0.28). However, against our expectations, the average proportion of attack actions in the last 2-blocks were significantly higher compared to the Nash equilibrium (0.03) when the IDS was 90% accurate (0.11) (t(25) = 2.86, $p < .01$) and when it was 10% accurate (0.21) (t(24) = 4.10, $p < .001$).

[2] Each block represents the average of the attack and defend decision across 10-trials. Thus, 100-trials were reduced to 10-blocks. Reducing the number of trials to blocks helps us control the inflation of degree of freedom in statistical tests.

Furthermore, as expected, the average proportion of defend actions in the last 2-blocks was consistent with the Nash equilibrium (0.66) when the IDS was absent (0.62) ($t(19) = -0.78$, $p = 0.44$) and when it was 50% accurate (0.62) ($t(28) = -0.91$, $p = 0.37$). However, against our expectations, the average proportion of defend actions in the last 2-blocks were significantly higher compared to the Nash equilibrium proportion (0.09) when the IDS was 90% accurate (0.19) ($t(25) = 2.38$, $p < 0.05$) and when it was 10% accurate (0.37) ($t(24) = 5.62$, $p < 0.001$).

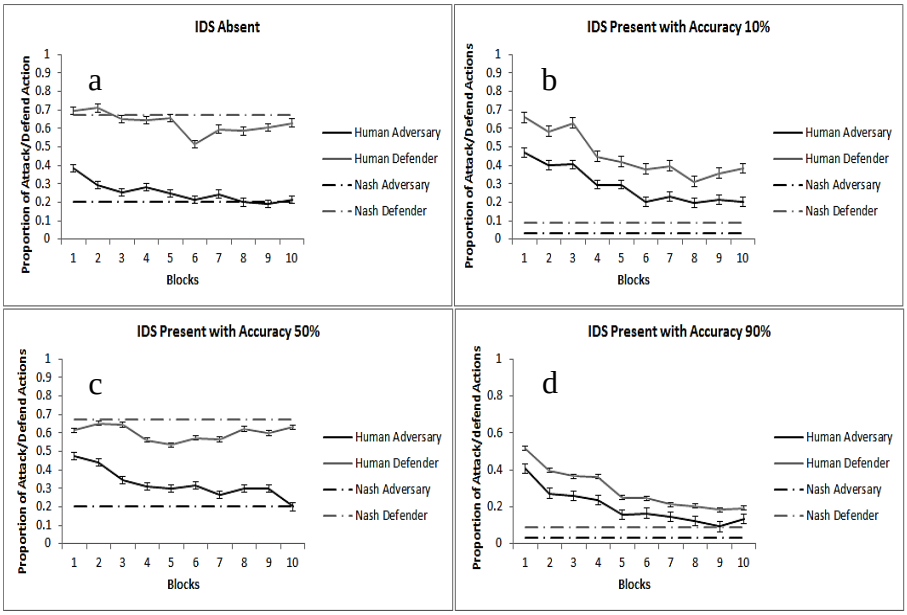


Figure 3. The proportion of attack and defend actions across 10-blocks in different conditions. a) IDS Absent condition; b) IDS present with 10% accuracy; c) IDS present with 50% accuracy; and, d) IDS present with 90% accuracy. The dotted lines show Nash equilibriums in different conditions for hacker and analyst participants. The error bars show the 95% confidence interval around the average estimate.

5. IBL MODEL

Prior research has used IBLT (Gonzalez, Lerch & Lebiere, 2003) to evaluate the cyber situational awareness of adversaries and defenders in cyber-security games (Aggarwal, Moisan, Gonzalez, & Dutt, 2018; Dutt, Ahn, & Gonzalez, 2013; Kaur & Dutt, 2013; Maqbool, Makhijani, Pammi, & Dutt, 2017). IBLT relies on cognitive processes like similarity and activation and imperfect retrievals from memory in complex task situations (e.g., the IDS

task in Figure 1). According to IBLT, human players tend to take those decisions that maximize their experienced utility but within their cognitive constraints and according to the cognitive demands of the task (Gonzalez et al., 2003). For example, in the cyber-security game when the IDS is absent, defenders would try to maximize the experienced utility by taking defend actions over time as it is possible to get a positive reward (+5) by defending the network. As defenders increase defend actions, one expects situationally aware adversaries to reduce their attack actions over time (to minimize the experienced disutility of facing defend actions when attacking the network). Here, we develop a computational cognitive model based upon IBLT to account for the decisions of participants performing as defenders and adversaries in the cyber-security game.

In the IBL model, an instance for a player consists of the following: player's situation (i.e., the context in which a decision is being made), player's choice (i.e., the decision to choose an option), and player's experienced utility (i.e., the outcome of choosing an option in a current situation). For a given situation, a decision is made by retrieving and blending all the instances belonging to each option. In the IBL model, among all the options, the option that has the highest blended value is chosen as a decision. The blending mechanism (Lebiere, 1999) has been borrowed from the Adaptive Control of Thought-Rational (ACT-R) architecture, where ACT-R is a general framework consisting of declarative and procedural memories to model human decisions (Anderson & Lebiere, 1998; 2003). The blended value $V_{k,t}$ of option *k* at trial *t* is adapted from (Gonzalez & Dutt, 2011; Lebiere, 1999; Lejarraga et al., 2012) and computed as:

$$V_{k,t} = \sum_{i=1}^{n} p_{i,k,t} * x_{i,k,t} \quad [1]$$

Where $x_{i,k,t}$ represents the outcome of an instance *i* for option *k* at trial *t* (outcomes could be -5, 0, +5, +10 based upon payoffs in Figure 2) and $p_{i,k,t}$ represents probability of retrieval of an instance *i* for option *k* at any trial *t* (value of *k* is either to attack/defend or to not-attack/not-defend).

The retrieval probability of an instance *i* is the ratio of activation of i^{th} instance corresponding to the activation of all instances (1, 2 … *n*) created within the option *k*:

$$p_{i,k,t} = \frac{e^{A_{i,k,t}/\tau}}{\sum_{i=1}^{n} e^{A_{i,k,t}/\tau}} \quad [2]$$

Where $\tau = \sigma * \sqrt{2}$ that represents random noise and σ is a free noise parameter. Noise captures the inaccuracy of remembering past experiences from memory. The noise parameter has been borrowed from the ACT-R architecture and it does no possess a default value (Anderson & Lebiere, 1998; 2003). However, the parameter has been found to have a mean of 0.25 in various ACT–R studies (Taatgen, Lebiere, & Anderson, 2005). The activation of each instance in memory depends upon the activation mechanism, which is borrowed from the ACT–R architecture (Anderson & Lebiere, 1998; 2003). A simplified version of the activation mechanism that relied on recency and frequency of instances use was enough in capturing human choice behavior in several repeated binary-choice and probability-learning tasks (Lejarraga et al., 2010; Lebiere, Gonzalez, & Warwick, 2010). We have used this simplified mechanism in the IBL model in this paper. The simplified mechanism to calculate activation of an instance *i* is a function of the recency and frequency of past occurrences of outcomes. At each trial *t*, activation of an instance *i* on option *k* is calculated as:

$$A_{i,k,t} = ln\left(\sum_{t_p \in \{1,\ldots,t-1\}} \left(t - t_p\right)^{-d}\right) \quad + \quad \sigma \,.\, ln\left(\frac{1-\gamma_{i,k,t}}{\gamma_{i,k,t}}\right) \qquad [3]$$

Where *d* represents free decay parameter; $\gamma_{i,k,t}$ represents random number drawn from a uniform distribution confined between 0 and 1; and t_p represents all the previous trials where the instance *i* was either created or its activation was reinforced due to the occurrence of outcome in the task. The numbers of terms in summation correspond to the frequency of observations and the difference of two time periods correspond to the recency of observations. The activation of an instance increases with high frequency and recency of an observation. The decay parameter (*d*), borrowed from ACT-R, helps to capture the rate of forgetting. In ACT–R, the *d* parameter has a default value of 0.5 (Anderson & Lebiere, 1998; 2003). The model pays more attention to recent events for larger values of *d* (> 1.0) compared to the smaller value of *d* (< 1.0). That is because, when *d* value is larger, the distant terms $\left(t - t_p\right)^{-d}$become smaller and their contribution to the instance's activation decreases rapidly. However, when the *d* value is smaller, the distant terms $\left(t - t_p\right)^{-d}$ do not become small and their contribution to the instance's activation does not decrease rapidly. The noise parameter σ helps to capture the trial-to-trial variability in individual decisions. A value of σ > 0.5 indicates rapid changes in choices for a decision-making from one trial to the next. Every time a choice is made, and an outcome is observed, an instance associated with the choice and

outcome is either created in memory (if not present) or reinforced in memory (if already present).

In the IBL model for adversaries and defenders, the situation part of instances contains the IDS recommendations (a threat or non-threat alert from IDS in a trial).[3] The inclusion of IDS alert explicitly in the instance structure of the IBL model will likely help the model to account for IDS recommendations. The decision part of instances consisted of the player's decision and the opponent's decision in a trial. The utility part of instances consisted of the player's experienced outcome as a result of taking a decision. For each choice option (attack or not-attack for an adversary; defend or not-defend for a defender), the values of all observed outcomes associated with that option are blended into a single-blended instance. The action corresponding to the blended instance with the highest blended value is executed in a specific trial. During the first trial, there are no past instances in memory for calculation of blended values of two alternatives. Therefore, the model selects an action based upon two pre-populated instances per player in memory, one for each of the player's action. These pre-populated instance values are calibrated along with d and σ parameters using a genetic algorithm program (Konak, Coit, & Smith, 2006). The outcome in pre-populated instances is analogous to participants' initial expectations from each action (Lebiere, 2010).

5.1 Expectations from the IBL Model

According to IBLT, one expects recency and frequency of outcomes and variability in decisions to influence the cyber situational awareness and the decision-making of both adversaries and defenders. Thus, one expects that higher values of d and σ to better explain human results compared to smaller values of d and σ (which are closer to ACT-R default values). Thus, we expect that the IBL model with calibrated parameters would possess higher d and σ values compared to the IBL model with ACT-R parameters. Furthermore, both adversaries and defenders receive IDS's alerts in the cyber-security game and both these players, due to situational awareness, would make their decision choices based on these generated alerts. Thus, we expect higher recency reliance (i.e., higher d parameter values) to provide a more accurate account of the decisions of both defenders and adversaries compared to the ACT-R parameter values. Furthermore, as human defenders and adversaries rely upon cognitive limitations of memory and recall (e.g.,

[3] The IDS recommendation slot was kept empty when this model was run in the IDS-absent condition.

reliance on recency, frequency, and variability in decisions) as per IBLT, we expect the IBL model to provide a superior account of human decisions compared to the optimal Nash solutions.

5.2 Model Execution

The IBL model was created in Matlab® and it contained two simulated players, the adversary and the defender. Each simulated player had four free parameters: decay *d*, noise σ, and pre-populated instances for different actions (two pre-populated instances with values for attack and not-attack actions for the adversary; and, two pre-populated instances with values for defend and not-defend actions for the defender). Just like human players, a pair of simulated players acted as adversaries and defenders and repeatedly interacted with each other for 100-trials across different between-subject conditions in the cyber-security game. The IBL model used blending and activation mechanisms independently for both adversary and defender players.

Overall, two IBL models were calibrated across the four conditions: IBL model with ACT-R default parameters and the IBL model with calibrated parameters. In the IBL model with ACT-R default parameters, we fixed *d* and σ values for both players to ACT-R defaults ($d = 0.50$, $\sigma = 0.25$) and calibrated the pre-populated instance values for both players. In the IBL model with calibrated parameters, we calibrated all parameters (i.e., *d*, σ, and pre-populated instances) for both simulated players. The ACT-R default parameters (*d* and σ) indicate lesser reliance on recency and smaller variability in decisions. Thus, using the ACT-R default parameters and calibrating all parameters will allow us to check the extent of recency reliance among both adversary and defender players. To get the best set of model parameters per agent, we minimized the sum of Mean-Squared Deviations (MSDs) computed over the proportion of attack and defend actions separately. The MSD for an action (attack or defend) is calculated as:

$$MSD = \frac{1}{100}\sum_{t=1}^{100}(Model\ Actions_t - Human\ Actions_t)^2 \quad [4]$$

Where, $Model\ Actions_t$ and $Human\ Actions_t$ refer to the average proportion of attack or defend actions from the model and human data, respectively, in trial *t* (there were 100 trials in the experiment). The average proportion of attack or defend actions for a trial were computed by averaging these actions across all participants for the trial. Smaller values of MSD close to zero are desirable and show improved performance from models. Genetic algorithm (Konak, Coit, & Smith, 2006) was used to

optimize the parameter values for both adversary and defender participants in the game. We ran the model multiple times with different number of simulated participants to evaluate the run-to-run stability of MSDs obtained. We found that the MSD values were stable and replicable with 100 simulated hacker and 100 simulated defender participants. Thus, we generated our model results using 100 simulated hacker and 100 simulated defender participants.

The trends in the average proportion of attack or defend actions over blocks from human data and models were compared using the R-square (R^2) measure (Bakeman, 2005). The R^2 varies between 0 and 1, where R^2 values closer to 1 indicate the model to accurately capture the over-time trend in human data.

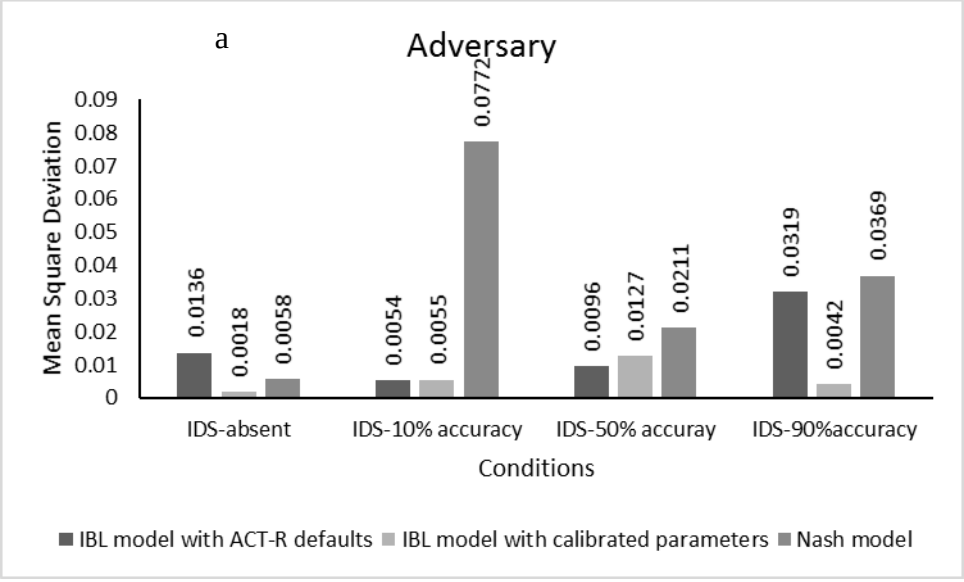
In agreement with the literature (Gonzalez & Dutt, 2011), the d and σ parameters were varied between 0.0 and 10.0; and, the pre-populated instance values were varied between 0.0 and 15.0. The upper bound for the pre-populated instance values was much higher compared to outcomes in the cyber-security game. This high value will allow the model to explore different decision choices for both players. Overall, the parameter ranges ensured that the optimization would capture the optimal values with high confidence. The genetic algorithm had a crossover rate of 80% and a mutation rate of 1%. The algorithm stopped when any of the following constraints were met: stall generations = 200, function tolerance = $1x10^{-8}$, and when the average relative change in the fitness function value over 200 stall generations was less than function tolerance ($1x10^{-8}$).

6 MODEL RESULTS

6.1 Calibration Results

We calibrated the parameters of IBL models with ACT-R default parameters and calibrated parameters across all four between-subject conditions. The objective of this exercise was to generate a single set of parameters for adversaries and defenders across all experimental conditions. We also computed the optimal Nash solutions across all experimental conditions. Figure 4 shows the MSDs obtained from different models in the calibration dataset for adversaries (Figure 4a) and defenders (Figure 4b). As seen in Figure 4a, for adversaries, the IBL model with calibrated parameters possessed the smallest MSDs in IDS-absent condition and IDS-90% accuracy condition. Also, the MSD from this model was about the same as that from the IBL model with ACT-R default parameters in IDS-10%

accuracy condition. The Nash solution performed poorer compared to both IBL models, except for the IDS-absent condition. In the IDS-absent condition, the Nash solution's MSD was slightly better compared to the MSD for the IBL model with ACT-R default parameters. Furthermore, as seen in Figure 4b, for defenders, the IBL model with calibrated parameters possessed the smallest MSDs in IDS-90% accuracy and IDS-10% accuracy conditions. The MSD from this model was inferior to the IBL model with ACT-R default parameters in IDS-absent and IDS-50% accuracy conditions. The Nash solutions performed better compared to both IBL models in IDS-absent and IDS-90% accuracy conditions. The Nash solution's performance was inferior to both IBL models in the IDS-10% condition. In IDS-50% accuracy condition, the Nash solution's performance was about the same as that of the IBL model with calibrated parameters.



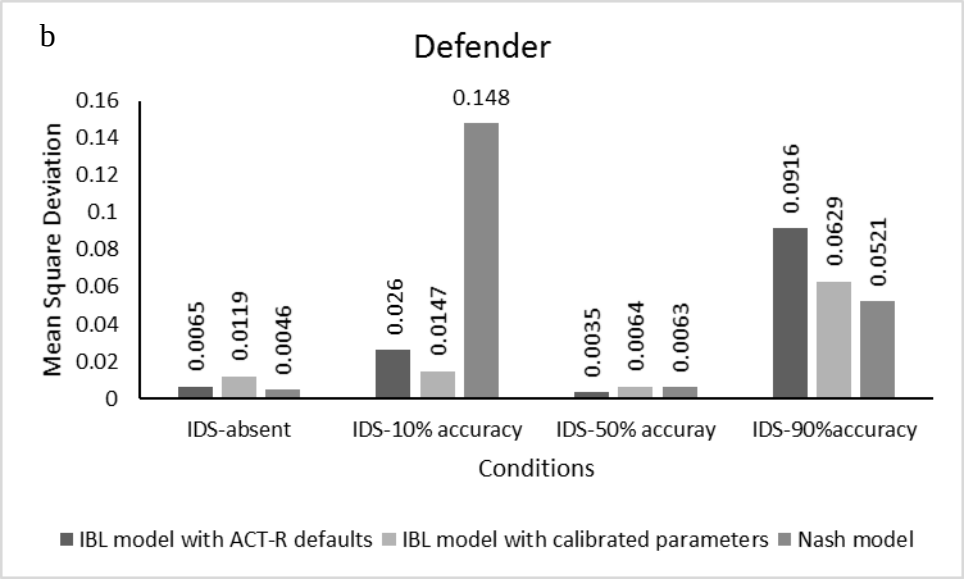


Figure 4: The mean squared deviations (MSDs) between IBL and Nash models and human data in different conditions. (a) The MSDs for IBL models and Nash model adversaries across different conditions. (b) The MSDs for IBL models and Nash model defenders across different conditions.

Figure 5 shows the over-block results for adversaries and defenders from the IBL model with ACT-R default parameters and Nash solutions compared to human data. As seen in Figure 5, the IBL model with ACT-R default parameters accounted for the trend in human data for defenders in only IDS-50% accuracy (Figure 5c; $R^2 = 0.204$) and IDS-90% accuracy (Figure 5d; $R^2 = 0.592$) conditions. Furthermore, this model accounted for the trend in human data for adversaries in only the IDS-10% accuracy condition (Figure 5b; $R^2 = 0.904$). Across all conditions, the Nash solutions did not capture the trend in the human proportion of attack and defend actions (the R^2 were close to 0).

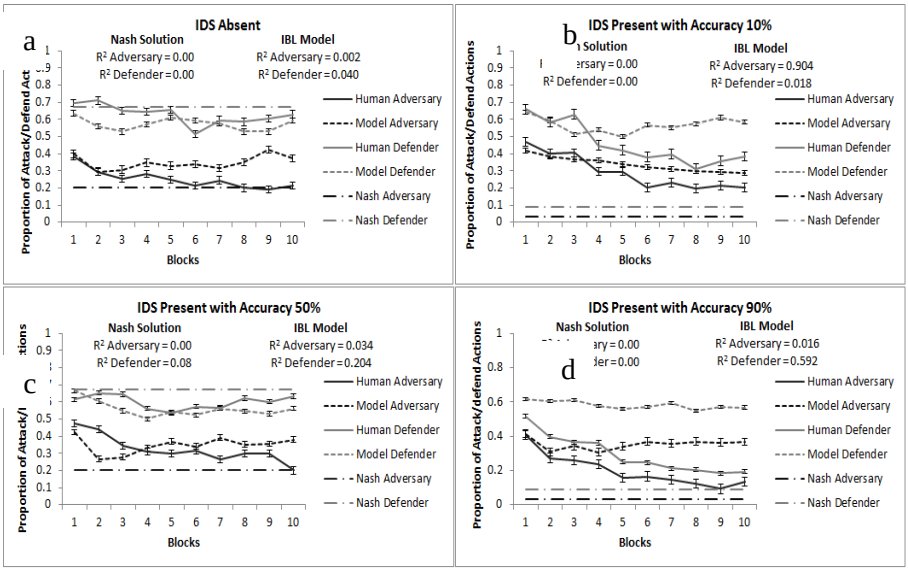


Figure 5: The proportion of attack and defend actions from human data and the IBL model with ACT-R default parameters in different conditions. (a) IDS-absent condition; (b) IDS-present with 10% accuracy; (c) IDS-present with 50% accuracy; and, d) IDS-present with 90% accuracy. The error bars show 95% confidence interval around the average estimate. The R^2 has been shown separately for the IBL model and Nash solutions across different conditions.

Next, we evaluated the ability of the IBL model with calibrated parameters in explaining the trend in human data across different conditions. Figure 6 shows the over-block results for adversaries and defenders from the IBL model with calibrated parameters and Nash solutions compared to human data across different conditions. As seen in Figure 6, the IBL model with calibrated parameters accounted for the trend in human data for defenders and adversaries across most of the conditions (the R^2 values were greater than 0.50 in most cases). The results for the Nash solutions remain the same as discussed in Figure 5.

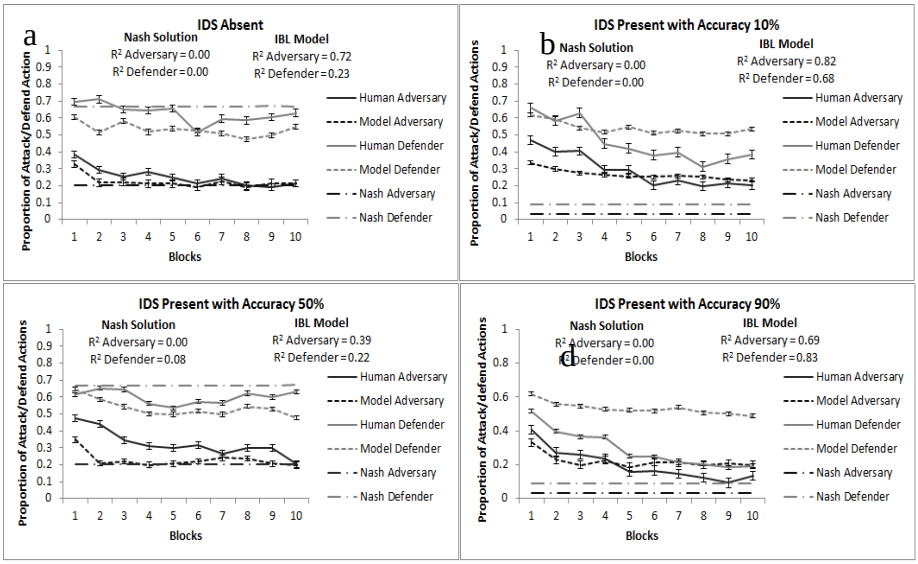


Figure 6: The proportion of attack and defend actions from human data and the IBL model with calibrated parameters in different conditions. (a) IDS-absent condition; (b) IDS-present with 10% accuracy; (c) IDS-present with 50% accuracy; and, (d) IDS-present with 90% accuracy. The error bars show 95% confidence interval around the average estimate. The R^2 has been shown separately for the IBL model and Nash solutions across different conditions.

Table 1 presents the summary of the calibrated parameters in IBL models (both with ACR-R default and calibrated parameters). As seen in Table 1, the IBL model with ACT-R parameters acted as a model with little reliance on recency (smaller *d* value) and the IBL model with calibrated parameters acted as a model with significant reliance on recency (larger *d* value). The model with calibrated parameters possessed slighter higher variability in decisions (σ parameter was greater than 0.5 in the calibrated model). Furthermore, based upon calibrated pre-populated values in both IBL models, the adversaries valued not-attack actions more compared to attack actions and the defenders valued defend actions more compared to not-defend actions.

Table 1: Parameter values in the IBL models in different IDS conditions

	Adversary	**Defender**
IBL model with ACT-R	d^1=0.50, σ =0.25, H_A^3=13.89, H_{NA}^4=14.38	d=0.50, σ =0.25, A_D^5=13.73, A_{ND}^6=10.28

parameters		
IBL model with calibrated parameters	d^1*=7.28,* σ *=0.96,* H_A^3*=12.15,* H_{NA}^4*=14.14*	*d=3.17,* σ *=0.77,* A_D^5*=9.70,* A_{ND}^6*=5.67*

Note. [1] The decay parameter. [2] The noise parameter. [3] Pre-populated instance value for attack actions. [4] Pre-populated instance value for not-attack actions. [5] Pre-populated instance value for defend actions. [6] Pre-populated instance value for not-defend actions.

Overall, as per our expectations, more reliance on recent information and variability in decisions in the calibrated model helped this model to account for decisions of adversaries and defenders in human data. In addition, both IBL models, on account of limitations of memory and recall, better accounted for decisions of adversaries and defenders compared to the Nash solutions.

7 DISCUSSION AND CONCLUSIONS

Cyber-attacks are increasing and IDSs could be an effective way of creating situational awareness among defenders, which helps defenders protect network and data against cyber-attacks. Prior research had documented how the presence and accuracy of IDS alerts influences the attack and defend actions of adversaries and defenders in simulated cyber-security games (Dutt, Moisan, & Gonzalez, 2016). These games involved an abstract network with protection measures against consecutive attacks (Hausken et al., 2013). However, little was known about how the presence and accuracy of IDSs would influence the cyber situational awareness, i.e., the sequential over-trial decisions of defenders and adversaries. Also, little was known on how cognitive models based upon Instance-based Learning Theory (IBLT; Arora & Dutt, 2013; Aggarwal, Moisan, Gonzalez, & Dutt, 2018; Dutt, Ahn, & Gonzalez, 2013; Kaur & Dutt, 2013; Maqbool, Makhijani, Pammi, & Dutt, 2017) would account for the over-time decisions in conditions involving varying presence and accuracy of IDS-like recommendations. In this paper, we addressed these gaps in literature by exploring sequential behavior (i.e., the proportion of attack and defend actions over time); how IBL models with different parameter assumptions capture this evolution; and, how recency, frequency, and variability in IBL models explain the human decisions compared to optimal Nash solutions.

Results of sequential analysis revealed that the proportion of defend actions remained more or less constant over trials when IDSs were absent or when

they were 50% accurate. However, in these conditions, adversaries reduced their attack actions over trials. When IDSs were 10% or 90% accurate, participants performing as defenders and adversaries both reduced their proportion of defend and attack actions., respectively. Furthermore, the proportion of actions were found to converge towards the optimal Nash solutions when IDSs were either absent or they were uninformative (50% accurate). However, the proportion of actions deviated from the optimal Nash solutions when IDSs were informative (10% accurate or 90% accurate).

One likely reason for these experimental results could be the excessive reliance on recency and frequency mechanisms by both adversaries and defenders over trials (Dutt, Ahn & Gonzalez, 2013; Maqbool, Makhijani, Pammi, & Dutt, 2017). Due to the excessive reliance on recency and frequency mechanisms, both players became situationally aware and reacted to immediately experienced utility (rewards and punishments) when the IDS was 10% and 90% accurate. Thus, defenders started with a higher proportion of defend actions and kept a constant defend proportion to maximize their experienced utility over trials. In contrast, adversaries reduced their attack proportions to minimize their experienced disutility. This situation also occurred when the IDS was absent or 50% accurate, where defenders, relying upon recency and frequency mechanisms, did not find the IDS to be informative to their decisions. Thus, situationally aware defenders maintained a higher proportion of defend actions to maximize their experienced utility and situationally aware adversaries reduced their proportion of attack actions to minimize their experienced disutility. Any deviation from Nash solutions does diminish players' actual utility. However, due to the recency and frequency reliance, players may only be able to maximize their experienced utility or minimize their experienced disutility. Thus, players may not be able to maximize their actual utility or minimize their actual disutility.

Next, we evaluated three models, i.e. the IBL model with ACT-R defaults, the IBL model with calibrated parameters, and Nash solutions, in their ability to account for sequential human decisions. Here, we used both error measures (mean squared deviations) and trend measures (R-square) with a large number of simulated model participants to perform our model comparisons. We found that both the IBL models, relying upon frequency, recency, and variability mechanisms, could better account for human data compared to the optimal Nash solutions. Furthermore, we found that the IBL model with calibrated parameters performed better compared to the IBL model with ACT-R defaults. Based upon the parameter values obtained, the

main reasons for our findings were the reliance on recency and frequency of outcome information and variability in decisions by both adversaries and defenders. The IBL model with calibrated parameters, which relied significantly on recency, frequency, and variability processes in its working, provided a more accurate account of human decisions compared to the IBL model with ACT-R default parameters.

We found that the IBL model with ACT-R default parameters performed with slightly smaller mean-squared errors compared to IBL model with calibrated parameters for the adversaries when IDS was 50% accurate and for the defenders when then IDS was absent or when it was 50% accurate. However, across all these conditions, the trend was better accounted by the IBL model with calibrated parameters compared to the IBL model with ACT-R parameters. Thus, overall, based upon the small error differences and large trend differences, we conclude that recency, frequency, and variability processes (as shown by the IBL model with calibrated parameters) were important in conditions where the IDS was uninformative.

Although we ran lab experiments involving canonical (abstract) games, our research does have some implications for the real world. The abstract cyber security games provide various decision-making scenarios where rewards and punishments are involved. Such abstract games could act as a training tool for creating situational awareness among the defenders about the risks and consequences involved in complex cyber-security tasks. Second, adversarial models based upon recency, frequency, and variability processes could be used to train defenders to respond to cyber-attack situations better. Third, newly developed IDS algorithms could be tested with cognitive models of attacker and defenders to evaluate the algorithms' effectiveness in countering cyber-attacks and in aiding defenders enhance their situational awareness and decision-making. Next, one could use cognitive models to project adversaries' and defenders' actions in other novel scenarios where the IDS may not be available all the time or when its accuracy may dynamically vary over time.

8 LIMITATIONS AND FUTURE WORK

We used pre-populated instances as free parameters in this paper. The value of these pre-populated instances was helpful in suggesting that adversaries valued not-attack actions and defenders valued defend actions to maximize their rewards. As part of future work, we could include learning from these parameters in other ways in the model to reduce the reliance on these pre-populated instances. One way could be to reinforce attack and defend

instances more compared to not-attack and not-defend instances, respectively, in the first few trials.

Furthermore, in this paper, we considered the proportion of attack actions and proportion of defend actions as dependent variables. These dependent variables were motivated by literature (Dutt, Ahn & Gonzalez, 2013; Maqbool, Makhijani, Pammi, & Dutt, 2017). However, there may be other dependent variables, e.g., the proportion of successful defenses or successful attacks and the proportion of agreement with the recommender. In the future, we would like to explore some of these dependent variables from both human data and models to understand the situational awareness and decision-making of adversaries and defenders. In addition, in this paper, we punished defenders when they took defend actions in situations where there were no attacks. However, there may be cases when defenders take defend actions as precautionary measures, which may be rewarding as they help avert future attacks. Thus, as part of the future research, we would also like to investigate scenarios where defenders are rewarded for precautionary defend actions, which avert future attacks.

In this paper, motivated by Hausken and Levitin (2012)'s framework, we considered an abstract network scenario, where a single adversary repeatedly exploited a single element against a single defender. However, in the future, we would like to study more complex network topologies involving multiple elements, adversaries, and defenders. Furthermore, beyond IBL models, we plan to consider other cognitive algorithms (e.g., reinforcement learning, Bayesian models, and neural networks models) to model human decision-making in simple and complex scenarios. Some of these investigations form the immediate next steps for us in our ongoing research program on behavioral cyber-security.

9 REFERENCES

Anderson, J. R., & Lebiere, C. (1998). *The atomic components of thought. The atomic components of thought.* Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers.

Anderson, J. R., & Lebiere, C. (2003). The Newell Test for a theory of cognition. *The Behavioral and Brain Sciences*, *26*(5), 587-601; discussion 601-48. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/15179936

Arora, A., & Dutt, V. (2013, July). *Cyber security: evaluating the effects of attack strategy and base rate through instance-based learning.* Paper presented at the 12th International Conference on Cognitive Modeling. Ottawa, Canada.

Aggarwal, P., Moisan, F., Gonzalez, C., & Dutt, V. (2018). Learning about Hacker's and Analyst's Decisions via Cognitive Modeling in Cyber-Security Games involving Alerts. Manuscript under review.

Bakeman, R. (2005). Recommended effect size statistics for repeated measures designs. *Behavior Research Methods*, *37*(3), 379-384.

Bhatt, C., Koshti, A., Agrawal, H., Malek, Z., & Trivedi, B. (2011). Architecture for intrusion detection system with fault tolerance using mobile agent. *International Journal of Network Security & Its Applications*, *3*(5), 167.

Bloem, M., Alpcan, T., & Basar, T. (2006, December). *Intrusion response as a resource allocation problem.* In 45th *IEEE Conference on Decision and Control*, San Diego, USA.

Camerer, C. F. (2003). *Behavioral game theory: Experiments in strategic interaction. Behavioral game theory: Experiments in strategic interaction.* New York, NY, US: Russell Sage Foundation.

Chen, Z., Du, W. B., Cao, X. B., & Zhou, X. L. (2015). Cascading failure of interdependent networks with different coupling preference under targeted attack. *Chaos, Solitons & Fractals*, *80*, 7-12.

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness: modeling detection of cyberattacks with instance-based learning theory. *Human Factors*, *55*(3), 605-618.

Dutt, V., Moisan, F., & Gonzalez, C. (2016). Role of Intrusion-Detection Systems in Cyber-Attack Detection. Advances in Human Factors in Cybersecurity. Springer, Cham. DOI:10.1007/978-3-319-41932-9_9

Endsley, M. R. (2017). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Gonzalez, C., & Dutt, V. (2011). Instance-based learning: Integrating sampling and repeated decisions from experience. *Psychological Review*, *118*(4), 523.

Gonzalez, C., Lerch, J. F., & Lebiere, C. (2003). Instance-based learning in dynamic decision making. *Cognitive Science*, *27*(4), 591-635.

Gonzalez, C., Ben-Asher, N., Oltramari, A., & Lebiere, C. (2014). Cognition and technology. *Advances in Information Security*, *62*, 93–117. https://doi.org/10.1007/978-3-319-11391-3_6

Hausken, K., & Levitin, G. (2012). Review of systems defense and attack models. *International Journal of Performability Engineering*, *8*(4), 355-366.

Hausken, K. (2017). Security investment, hacking, and information sharing between firms and between hackers. *Games*, *8*(2), 23.

Hausken, K. (2017). Information sharing among cyber hackers in successive attacks. *International Game Theory Review*, *19*(02), 1750010.

Jajodia, S., Liu, P., Swarup, V., & Wang, C. (Eds.). (2010). *Cyber Situational Awareness* (Vol. 46). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-0140-8

Kaur, A., & Dutt, V. (2013). Cyber situation awareness: modeling the effects of similarity and scenarios on cyber-attack detection. In *12th International Conference on Cognitive Modeling. Ottawa, Canada*.

Khandelwal, S. (2018). GitHub Again Hit by DDoS Cyberattack. Retrieved from https://thehackernews.com/2015/08/github-hit-by-ddos-attack.html

Konak, A., Coit, D. W., & Smith, A. E. (2006). Multi-objective optimization using genetic algorithms: A tutorial. *Reliability Engineering & System Safety*, *91*(9), 992-1007.

Laszka, A., Abbas, W., Sastry, S. S., Vorobeychik, Y., & Koutsoukos, X. (2016). Optimal thresholds for intrusion detection systems. *Proceedings of the Symposium and Bootcamp on the Science of Security - HotSos '16*, 72–81. https://doi.org/10.1145/2898375.2898399

Levitin, G., Hausken, K., Taboada, H. A., & Coit, D. W. (2012). Data survivability vs. security in information systems. *Reliability Engineering & System Safety*, *100*, 19-27.

Lebiere, C. (1999). Blending: An ACT-R mechanism for aggregate retrievals. In *Proceedings of the Sixth Annual ACT-R Workshop, George Mason University, Fairfax, VA, USA*.

Lejarraga, T., Dutt, V., & Gonzalez, C. (2012). Instance-based learning: A general model of repeated binary choice. *Journal of Behavioral Decision Making*, *25*(2), 143-153.

Lebiere, C., Gonzalez, C., & Warwick, W. (2010). Cognitive Architectures, Model Comparison and AGI. *Journal of Artificial General Intelligence*, *2*(2), 1-19.

Maqbool, Z., Makhijani, N., Pammi, V. C., & Dutt, V. (2017). Effects of motivation: rewarding hackers for undetected attacks cause analysts to perform poorly. *Human factors*, *59*(3), 420-431.

McKelvey, R. D., McLennan, A. M., & Turocy, T. L. (2006). Gambit: Software Tools for Game Theory. Retrieved from http://jmvidal.cse.sc.edu/lib/mckelvey06a.html

McAfee. (2016). In the Dark: Crucial Industries Confront Cyber-attacks. Retrieved from http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

Newsweek. (2018). Hackers are now targeting U.S. power grid companies—will there be blackouts? Retrieved from https://www.newsweek.com/what-raspite-us-electric-grids-under-threat-new-hacking-group-1054053

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A survey of game theory as applied to network security. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 1–10). IEEE. https://doi.org/10.1109/HICSS.2010.35

Situation Awareness. (2018). Retrieved from https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Taatgen, N., Lebiere, C., & Anderson, J. (2005). Modeling paradigms in ACT-R. In R. Sun (Ed.), *Cognition and Multi-Agent Interaction: From Cognitive Modeling to Social Simulation* (pp. 29–52). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511610721.003

Wu, B., Tang, A., & Wu, J. (2016). Modeling cascading failures in interdependent infrastructures under terrorist attacks. *Reliability Engineering and System Safety*, *147*, 1–8. https://doi.org/10.1016/j.ress.2015.10.019

KEY TERMS

Cyber-security: Refers to the practice of securing the cyber infrastructure from cyber-attacks.

Simulated defenders: A model decision maker responsible for securing the network.

Simulated adversary: A model decision maker responsible for launching a cyber-attack.

Intrusion Detection Systems (IDS): A recommendation system that monitors the network traffic and identify cyber threats in the network.

Alerts: A recommendation generated by IDS against cyber threats in the network.

Cyber-security game: A two-player non-cooperative game between defender and adversary where adversary choose among attack and not-attack actions, whereas, defender choose among defend and not-defend actions.

Instance-based Learning Theory: A theory of making decisions through experience in dynamic tasks. According to the theory, individuals create instance of various events in the memory and retrieve these instances while taking actions.

BIOGRAPHICAL NOTES

Palvi Aggarwal is a post-doctoral fellow at the Dynamic Decision Making Lab, Carnegie Mellon University, Pittsburgh. She received her Ph.D. in Computer Science from Indian Institute of Technology Mandi, India. She received her master's degree in Information security from Thapar University Patiala, India. Her current research areas include cyber security, cognitive modeling, machine learning, and deep learning.

Frederic Moisan received his Ph.D. in logic and experimental economics at the University of Toulouse, jointly working with the Institut de Recherche en Informatique de Toulouse (IRIT) and Toulouse School of Economics (TSE). Currently, he is a postdoctoral research associate at the Faculty of Economics, University of Cambridge. Before that, he was a postdoctoral fellow at Carnegie Mellon University.

Cleotilde Gonzalez received her Ph.D. in management information systems from Texas Tech University in 1996. She is a research professor and director of the Dynamic Decision Making Laboratory, Department of Social and Decision Sciences, Carnegie Mellon University. She is affiliated faculty at HCII, CCBI, and CNBC. She is on the editorial board of a number of

journals including Human Factors and Journal of Cognitive Engineering and Decision Making.

Varun Dutt received his Ph.D. degree from Carnegie Mellon University in 2011. He is an assistant professor and principal investigator at the Applied Cognitive Science Laboratory, School of Computing and Electrical Engineering, Indian Institute of Technology Mandi. He is also the review editor in Frontiers in Cognitive Science and Frontiers in Decision Neuroscience journals. His current research interests include cyber security, cognitive science, judgment and decision making, and artificial intelligence.

REFERENCE

Reference to this paper should be made as follows: Aggarwal p., Moisan F., Gonzalez C., & Dutt V. (2018). Understanding Cyber Situational Awareness in a Cyber Security Game involving Recommendations. *International Journal on Cyber Situational Awareness*, Vol. 3, No. 1, pp. 11-38.

APPENDIX

Nash Calculations

Dutt, Moisan and Gonzalez (2016) generated Nash equilibria by the Gambit software (McKelvey, McLennan, and Turocy, 2010). It is clear from the game in Figure 2 that there exists no Nash equilibrium in pure strategies (in each of the four possible outcomes, one player is better off deviating). Thus, the only equilibrium solution in this game is in mixed strategies (i.e., selecting each action with some probability). The Nash equilibrium in mixed-strategies is the following: the hacker attacks with 0.2 ($\frac{1}{5}$) probability, while the analyst defends with 0.66 ($\frac{2}{3}$) probability.

Dutt, Moisan and Gonzalez (2016) extended the definition of the above security game by introducing an IDS that can alert the analyst regarding the decision made by the hacker (thus, the analyst does not see the actions of the hacker directly; rather, she gets messages from the IDS based upon hacker's decisions). The hacker first makes a choice, followed by the IDS that reports the existence/absence of an attack to the analyst. In the security game, we define *pa* as the probability of the IDS to accurately predict the hacker's

choice (a wrong prediction therefore occurs with probability *1-pa*). The report from the IDS is determined through probability *pa* (e.g., if the hacker attacks by choosing a, IDS reports an attack with probability *pa* and non-attack with probability *1-pa*). After receiving the IDS recommendation, the analyst makes a choice.

Figure A1 lists the Nash equilibria in the cyber-security game described above for *pa* = 10% (i.e., when IDS is 10% accurate). The extensive form of the cyber-security game in Figure A1 along with the Nash equilibria were generated by the Gambit software (McKelvey, McLennan, and Turocy, 2010). As shown in Figure A1, first the hacker makes a choice to attack or not-attack the network, the IDS alerts the analyst by an "attack" or "not-attack" message, and finally the analyst makes a choice.

Let P(a) be the probability (proportion) of attack actions; P(na) be the probability of not-attack actions; P(d) be the probability of defend actions; and P(nd) be the probability of not-defend actions. As shown in Figure A1, when the IDS is 10% accurate, the probability of attack is (0.027 ~ 03%).

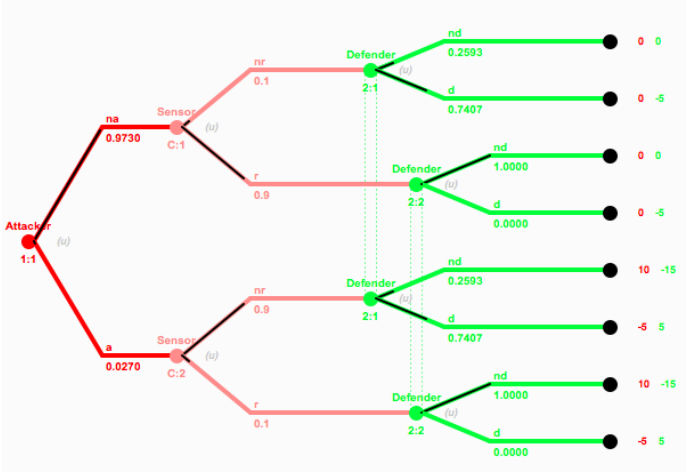


Figure A1. Cyber-security game tree generated with Gambit detailing Nash Equilibria when the IDS is 10% accurate.

Overall, the values obtained from Gambit in Figure A1 are:

P(a) = 0.03; P(na) = 0.97; P("a"|a) = 0.10; P("a"|na) = 0.90; P(d|"a") = 0; and, P(nd|"a") = 1.

Where, P("a"|a) is the probability of IDS to say "attack" given that the hacker attacks; P("a"|na) is the probability of IDS to say "attack" given that

the hacker does not attack; P(d|“a”) is the probability of the analyst to defend the network given that the IDS say “attack”; and, P(d|“a”) is the probability of the analyst to not defend the network given that the IDS say “attack.”

Now, we apply the Bayes’ rule to P(“a”), i.e., the probability of the IDS to say “attack” as per the following:

$$P(\text{“a”}) = P(\text{“a”}|a) * P(a) + P(\text{“a”}|na) * P(na) \qquad (1)$$

Using the values of P(“a”|a), P(a), P(“a”|na), and P(na) from Figure A1 in (1), we get:

$$P(\text{“a”}) = 0.87 \text{ and } P(\text{“na”}) = 0.13 \qquad (2)$$

Now, we apply the Bayes’ rule to P(d), i.e., the probability of the analyst to defend as per the following:

$$P(d) = P(d|\text{“a”}) * P(\text{“a”}) + P(d|\text{“na”}) * P(\text{“na”}) \qquad (3)$$

Using the values of P(“a”) and P(“na”) from (2) in (3), we get:

$$P(d) = 0.09 \text{ and } P(nd) = 0.91 \qquad (4)$$

Thus, the Nash proportion of attack and defend actions equaled to 3% and 9%, respectively, when the IDS was 10% accurate.

Using the same derivation, the Nash proportion of attack and defend actions equaled to 20% and 67%, respectively, when the IDS was 50% accurate. Also, the Nash proportion of attack and defend actions equaled to 3% and 9%, respectively, when the IDS was 90% accurate.