Team-Based Cyber Defense Analysis

Michael A. Champion, Prashanth Rajivan, Nancy J. Cooke, and Shree Jariwala

Abstract— **Situation awareness (SA) in the cyber security domain is particularly relevant to teams of security analysts who are responsible for detecting cyber threats by perusing continual floods of data such as intrusion alerts and network logs. The challenges that analysts face are matched by those of researchers attempting to understand, measure, and impact SA in the cyber arena. The ground truth is not available except in simulated cyber situations. In this paper we outline a cognitive task analysis (CTA) focused on teams of analysts and the subsequent preliminary study conducted using a cyber defense simulation environment, CyberCog, built based on the CTA findings. Results from the CTA suggest three areas of fundamental challenge surrounding security analysts: team structure, communication, and information overload. These challenges could be associated to maladies such as cognitive tunneling and increased false alarms. These results are mirrored in the CyberCog pilot simulation study.**

Index Terms—**Cyber Security, Situation Awareness, Team Situation Awareness, Team Cyber Situation Awareness, Cognitive Task Analysis**

I. Introduction

General Douglas MacArthur once said "There is no security on this Earth, there is only opportunity." We can think of no other area in which these words are more resoundingly true than within cyber security. It has become routine that new software is developed at faster and faster paces as new technology emerges. With every iteration, security is often increased to address the concerns of the end users. Although great strides are made towards ensuring the security of new software, time and time again have adversaries found new and innovative methods and created opportunities for undermining these safeguards.

In August of 2011, McAfee, a computer security company, uncovered a large 5-year hacking operation, dubbed 'Shady RAT'. Although the specifics of who was involved in this operation are still open to speculation, this was the action of only one group. This one group managed to infiltrate the systems of 71 organizations including governments, industry, defense contractors, non-profits, and communications companies across 14 countries. The amount of exfiltrated information is estimated to be in the petabytes (1,000+ terabytes) and the current whereabouts of such information and its intended use is unknown. Many other attacks just as complex and just as vast have occurred in the past and are occurring even now [1].

As the threat in cyberspace grows to be more prevalent, organizations and governments have escalated their attempts to mitigate these occurrences. The U.S. Government in particular has formed agencies, such as U.S. Cyber Command, whose sole concern is over the cyber space realm as if it is a war-space just as land, air, sea, and space [2], as well as civilian and military cyber defense teams known as Computer Emergency Readiness Teams (CERTS).

Given the innovation within computer systems, and the evolving nature of cyber infrastructures, we have begun to create a vulnerable battle space. With the amount of information passed each day on the Internet close to 77 petabytes, or 77,000 terabytes [3] it is impossible to completely control, and monitor for, security breaches and threats. As we will describe in a later section, cyber analysts and cyber defense teams often see thousands of security alerts/events each hour. Given the amount of information presented to an analyst, and the expediency and evolution of security threats, the given task of identifying those threats has become inhumane to the analyst.

In this paper, we present our findings from the cognitive task analysis (CTA) on cyber security analyst and results from the preliminary experiments on team based cyber defense conducted using the cyber security simulation environment: CyberCog.

II. Cyber Situation Awareness

The leading definition of Situation Awareness (SA) states that it "is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [4]. When we consider team situation awareness, we then consider the ability of the team to adapt to, maintain awareness of, and respond to the situation at hand [5]. Although, how does this apply with the cyber world in which perception is limited to what a computer can convey through the monitor, where space is seemingly infinite, and comprehension is shared between the computer and analyst?

Manuscript received November 1, 2011. This work was supported by the Army Research Office under MURI Grant W911NF-09-1-0525.

Michael A. Champion is with the Arizona State University, TIEM, 7271 E. Sonoran Arroyo Mall, Mesa, Arizona 85212(michael.champion@asu.edu)

Prashanth Rajivan is with the Arizona State University, TIEM, 7271 E. Sonoran Arroyo Mall, Mesa, Arizona 85212(pnrajiva@asu.edu)

Nancy J. Cooke is with the Arizona State University, TIEM, 7271 E. Sonoran Arroyo Mall, Mesa, Arizona 85212 (nancy.cooke@asu.edu, phone: 480.988.7306, fax: 480.988.3162).

Shree Jariwala is with the Arizona State University, TIEM, 7271 E. Sonoran Arroyo Mall, Mesa, Arizona 85212(sjariwala@asu.edu)

McNeese, Cooke, and Champion (2011) [6] state that Cyber Situation Awareness (CSA) is situated both in the analyst and the computer systems sharing the burden of the task at hand. Furthermore, the assertion that more data can equate with improved perception of the situation is shortsighted. Instead, more data could result in cognitive overload. Proponents of the higher data load to increase perception often cite the usage of algorithms in order to maintain a level of awareness [7]. However, automation can decrease situation awareness [8] and automation in the cyber security realm does not necessarily equate to higher awareness [6].

When considering team situation awareness for cyber security we can expand upon the Cyber SA idea to include that CTSA is situated between the team and the computer system that must as a whole, share in the perception, comprehension, and projection of the situation through collaboration and communication.

III. Cyber Cognitive Task Analysis for Team-Based Cyber Analysis

In order to understand and begin to get at the crux of the team cyber security defense issue we began a cognitive task analysis. Our goal for this was not to solve a problem, or develop a solution. The goal was to understand the processes used by analysts in the context of their role as a cyber security defense analyst.

A. Procedure

Our concern originated with the team: How was it structured? How was the task distributed among team members? After the structuring was addressed, the job was then addressed both from a team standpoint and an individual standpoint: What was the threat identification process? What would happen after a threat is identified? We began with interviews of cyber security defense analysts from U.S. CERTs, subject-matter experts, and researchers at the Cyber Situation Awareness Workshop held by the Arizona State University and the Pennsylvania State University. The format of these interviews was an unstructured, free flowing conversation in which analysts and experts were asked key questions, with the interviewer then asking probing questions about the responses. The responses were then collected and began to form the basis of the CTA.

In addition to the workshop, we observed the Air Force Academy's participation in the Cyber Defense Exercise (CDX) put on by the National Security Agency (NSA). The Air Force CDX team consisted of 23 Cadets, all a part of a cyber security student group. Observing the CDX proved to be a useful venue for data collection due to the ongoing security threat being presented by the adversary, in this case, the NSA. Although the task was artificial, the team's reaction is likely equivalent to how a cyber defense team in a real-world situation would respond. Detailed notes of interactions, tactics, team organization, and communications were collected for analysis.

B. Results

In analyzing the data collected through interviews and observations, we identified three major areas of concern. The first was the overall organization of the team. The second is team communication. The third is the amount of information to be processed by the team and individual analysts.

The organization of teams proved to be a large obstacle. During the interviews, analysts and experts often indicated that there is a lack of a robust team structure. It was rare that an analyst would not know to whom to report a cyber security event to directly, the remaining organization of team – including who on the team was responsible for what – was reported as often in question. It held true during CDX observations when Air Force Cadets would often be found monitoring the same system, leaving other systems unmonitored. When asked if individuals knew who they could gather information from regarding certain security alerts or aspects of their job, there was a general consensus that there was no reliable source of information they could consistently turn towards. Often cited, what becomes more troublesome to the task of a cyber security defense analyst is that different offices within even one organization could have different teams and hierarchical structures leading to confusion if the team must cooperate with an outside cyber defense team.

The second of the three major hurdles involved communication and communication breakdowns. One of the most cited problems within cyber defense teams reported was intra-team communication. Often times there was no communication between analysts which when compounded with the two other areas of concern only exacerbated the issue. Analysts reported finding themselves occasionally working on the same data set as other analysts, and often this was discovered after the work was completed when the communication no longer was useful to the analysis task. Further promoting this issue, team communication and collaboration was rarely fostered, while competitiveness within the team often lead to analysts remaining silent in order to appear more prestigious if they were the ones to report a security breach alone. During the CDX observation, lack of communication was not a propagated factor due to a rigid command structure. Nor was intra-team competition a factor due to the overall nature of the exercise in which the team as a unit was judged. What became a factor during the CDX was effective communication of the current situations. Cadets would often shorthand communications in ways that were not entirely clear to the team as a whole. Other reported communication breakdown causes ranged from security clearance differences, effective job training and original communications, and the lack of feedback on reported cyber security events.

Lastly, the vast amount of information reported by the analysts was staggering. Several reports indicated that the level of possible security events to be researched per analyst ranged from the hundreds to thousands to tens-of-thousands in any given hour. Analysts reported feelings of being overwhelmed and overloaded with information, which led to frustration and cognitive fatigue. During observations of the CDX exercises, there were often hours in which the team would have to analyze hundreds of intrusion alerts per hour –

and there was only one adversary rather than an entire globe of adversaries! During peak attacks period, Cadets in this exercise often became dejected and frustrated with the level of security events they had to analyze. It should be noted that in this artificial environment a team of 23 cadets were used to analyze one system; however, in true implementation one CERT may have dozens if not hundreds of systems to oversee.

Given the three major hurdles we have identified, we are building an understanding of where breakdowns occur within a Team Cyber Defense Task. With a deeper understanding of these hurdles, we can begin to develop appropriate counter measures and begin to instill proper techniques to combat such delinquencies. For our purposes, we began by utilizing this information in the development of our testbed, CyberCog.

IV. CyberCog

The CyberCog testbed is a Synthetic Task Environment based on Cooke and Shope (2004) [9] and is the third variation based on Rajivan, Venkatanarayanan, and Cooke (2011) [10].

A. CyberCog Version 3.0 Software

The CyberCog software was designed to emulate a number of frequently mentioned tools used within cyber security defense tasks reported during our CTA. These tools are security alert monitors, network and system logs, network maps, network vulnerabilities, user databases, and Internet-based data sources. The system is a web page based system populated with data from the CDX data collected from the U.S. Military Academy at West Point's participation in 2009. Each analyst had two monitors in which the CyberCog software was presented. The main screen is a security intrusion alerts page where alerts are populated during the exercises. Each alert on the main page has to be classified to one of the four categories. The four classification categories were: "Reconnaissance", "False Positive", "Failed Attack", and "Attack". For example, "Port Scan" is a security alert. In the exercise, Analyst 1 was provided with complete information regarding the classification of this alert and the other two analysts were given instructions to ask Analyst 1 for more information on how to classify the security event.

A second tabbed screen, much like in popular Internet browsers, showed completed network and system logs. A third screen showed events as they were being classified in their respective groups. A fourth screen was a "User Search" function for searching usernames in the mock system for validation. The fifth tabbed screen was unique to each analysts with Analyst 1 having "System Vulnerabilities" that is what each computer system is susceptible in terms of infiltration; Analyst 2 had a wiki-style information page that contained "stories" related to the task about certain attack methods; Analyst 3 had a network map showing the network in its entirety. Analysts had two screens that were shared and interactive with the rest of the team. "Attack Path" was where teams reported the specific systems affected in the scenario and the order in which they were affected. The shared screen "Shared Events" was a screen on which teams could share events with each other, if needed, in order to correctly classify the events.

B. Procedure

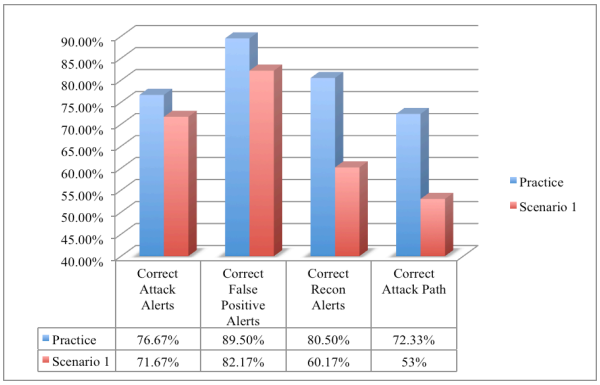
Eight teams were comprised of three participants recruited out of a proprietary subject pool for this pilot test. Participants gave informed consent, and then were provided task specific group training. During training, participants received individualized training on their specific role and knowledge base. The information provided in the individualized training was different for each team member to ensure team collaboration. The remainder of the training task walked the teams through the entire process of identifying security alerts, classifying security alerts, and then reporting the attack path.

After training, teams were given a practice scenario with 10 security alerts each. During this practice, teams were encouraged to ask questions and work through the scenario as quickly and accurately as possible. Thirty minutes were given in order to complete the practice scenario. At the end of the scenario, after teams reported the perceived attack path, teams were asked to submit a team report. This report asked that teams report the specific security breach(es) and in which order they arose. The teams were to formulate this report by working together. The third analyst was responsible for gathering the information and submitting this report. Following the report, a NASA Task Load Index (TLX) Questionnaire [11] was also administered.

The full scenario was administered after the practice scenario. The full scenario proceeded in the same fashion as the practice, except participants received 48 security alerts each and had 60 minutes to complete the scenario.

C. Results

Team Scores. At the end of each scenario, teams were given scores based on completion of classified alerts in percentages. The percentages from the practice scenario were used as a team-specific baseline and a one-way ANOVA was conducted on team scores based on practice and full scenarios. Over all, teams did not significantly differ between the practice and full scenario. Incorrectly classified reconnaissance events were significant ($F(1,15) = 4.584$, $p = 0.05$), with the practice scenario having a mean completion rate of 80.50% of reconnaissance events correctly classified, while the full scenario dropped to only 60.17% correctly classified, as seen in Figure 1.



	Correct Attack Alerts	Correct False Positive Alerts	Correct Recon Alerts	Correct Attack Path
Practice	76.67%	89.50%	80.50%	72.33%
Scenario 1	71.67%	82.17%	60.17%	53%

Figure 1. This graph shows the percentages of correctly classified alerts from the practice and full scenarios.

NASA TLX. Teams were asked to complete the NASA-TLX questionnaire. Teams did not significantly differ between

scenarios. For the full scenario teams reported, on a 10-point scale mental demand was somewhat high (Mean = 6.722, SD = 1.84), temporal demands were somewhat high (Mean = 5.889, SD = 2.56), effort was somewhat high (Mean = 6.222, SD = 2.46), and performance was seen as somewhat low (Mean = 3.944, SD = 1.70).

Cyber Team Situation Awareness. Each team was asked to complete a team report at the conclusion of the scenarios, which included questions that asked about perceived SA. Teams reported that, on average, in both practice and full scenarios, they were "Somewhat Aware" of what was occurring within the network. This was further supported with another team-reported measure stating that on average teams felt that they were 70% confident of their categorization of security alerts. Only 62% of teams felt that they successfully defended their network. Team SA was then calculated from the correctly identified attack paths. Given this, teams overestimated their performance in the full scenario with only 47.7% of the systems correctly identified in order to successfully defend their network. Of these correctly identified systems, only 6.2% of these systems were correctly ordered in the proper attack order. When compared to the practice scenario, teams were on average 75.84% confident in their categorization, while 62.5% felt they successfully defended their network, but only 63% of the teams correctly identified the compromised systems.

V. Discussion

The task of cyber security defense, on both the individual and team level, is complex, cognitively demanding and often overwhelming. The results from the CTA show that a cyber security defense analyst team can often be characterized as a group of individuals working independently with little to no communication or collaborative effort with team members. We identified three possible contributing factors to the breakdown of team performance in the cyber security defense task: team structure, team communication, and information overload. It is possible that information overload may drive abnormalities in both team structure and team communication.

The cyber security defense task must therefore be restructured at the process level, utilizing new technologies and strategies to be more team-based by sharing the workload and information efficiently, while interacting effectively to remedy the security threats.

Based on the results of the CTA model, we conducted an experiment to reproduce some of the problematic aspects of the cyber defense task. The results from the experiment, in accordance with the CTA findings, primarily show that situation awareness in the cyber security defense analysis task is moderate-to-low, and only declines with higher information load.

Using practice scenario measures as a baseline for each team, we illustrated a drop in effectiveness, security event detection, and situation awareness. While the practice scenario utilized only 10 security events per team member, the full scenario utilized 48 security events per team member. With the addition of these events, performance declined by 16% in correctly listed compromised systems. With the addition of only 38 events, we were able to decrease team performance at a rate of a 0.42% drop in effectiveness per alert added. If this scale held true, the drop to 0% completion would only require a total of 114 security events!

Contributing factors to this steep decline were increased false alarms, a lack of communication, and wrongful categorization of security events, leading teams to "miss" intended targets. Within the CyberCog experiment, information was distributed in a manner that allowed effectively communicating teams to reach near 100% completion. Although not completely attributable to only a lack of communication, only 47.7% of teams that were able to successful identify the attack path.

The CyberCog findings are emblematic of the findings in the CTA and only begin to scratch the surface of this vastly complex area.

Acknowledgment

We would like to thank the cyber security defense analysts, researchers, and cyber security professionals who donated their time to sit with us and discuss these issues. We'd also like to thank the Cadets at the Air Force Academy for their diligent efforts at helping further our nation's cyber security defense readiness. Lastly, we would like to thank Cliff Wang, and our MURI partners at Penn State, and Ohio State whose insights and information have helped us further our understanding.

References

[1] Alperovitch, Dmitri. (2011). *Revealed: Operation Shady Rat.* [White Paper]. Retrieved from: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[2] Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace.* Retrieved from: http://www.defense.gov/news/d20110714cyber.pdf

[3] Cisco. (2011). *Cisco Visual Networking Index: Forecast and Methodology: 2010 – 2015.* [White Paper]. Retrieved from: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf

[4] Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37,* 32-64.

[5] Gorman, J.C., Cooke, N.J., & Winner, J.L. (2006). Measuring team situation awareness in decentralized command and control systems. *Ergonomics, 49,* 1312-1325.

[6] McNeese, M., Cooke, N.J., Champion, M.A. (2011) Situating Cyber Situation Awareness. *Proceedings of the 10th International Conference on Naturalistic Decision Making.*

[7] Barford, P., Dacier, M., Dietterich, T.G., Fredrickson, M.,Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., Yen, J. (2010). Cyber SA: Situational Awareness for Cyber Defense. In S. Jajodia, P. Liu, P., Swarup, V., Wang, C. (Eds.), *Cyber Situational Awareness* (pp. 3-15). New York, NY: Springer**.**

[8] Wickens, C. D. (2008). Situation awareness: Review of Mica Endsley's 1995 articles on situation awareness theory and measurement, *Human Factors*, *50*, 397-403.

[9] Cooke, N.J., & Shope, S.M. (2004). Designing a synthetic task environment. *Scaled Worlds: Development, Validation, and Application,* pp. 263-278.

[10] Rajivan, P., Venkatanarayanan, S., and Cooke, N.J. (2011). CyberCog: A Synthetic Task Environment for Studies of Cyber Situation Awareness. *Proceedings of the 10th International Conference on Naturalistic Decision Making.*

[11] Hart, S. G., & Staveland L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. *Human Mental Workload,* vol. 1, pp. 139–183.