TeamNETS: Scaled World Simulation for Distributed Cyber Teams

Vincent F. Mancuso[1] and Michael McNeese[2]

[1] Oak Ridge Institute for Science and Education
vincent.mancuso.ctr@wpafb.af.mil
[2] The Pennsylvania State University, College of Information Sciences and Technology
mmcneese@ist.psu.edu

Abstract. Cyber operations have become a significant interest to government, military and corporate entities. Unfortunately, the secure nature of cyber operations limits the access that researchers can obtain. Therefore, simulations that can mimic the operating environment are a critical need to push this research forward. The purpose of this paper is to present a human-in-the-loop, scaled world simulation, *teamNETS*, which is capable of simulating multiple types of cyber security tasks. *TeamNETS* simulates the cognitive and collaborative requirements cyber security work and serves as an effective platform to study varying aspects of individual and team cognition, as well as other issues in Human-Computer Interaction.

Keywords: cyber security, simulation, scaled world, team simulation.

1 Introduction

Over the last several years, cyber threats have begun to move to the forefront of the national security discussion. In 2012, a reported 42,887 cyber related incidents (117 incidents per day) resulted in data loss or theft, computer intrusions or privacy breaches[1]. In response to this, the federal government invested $13 Billion on developing effective cyber-operations over the last several years. Currently, much of the work and research has focused on the development of algorithms, and intelligent systems to detect and mitigate cyber threats.

While invaluable to our national goals, to obtain a fully secure cyber space, researchers must not only help improve the technology and algorithms that drive cyber security, but also must find ways to support the human operators. Unfortunately, due to the secure nature of the operating environment, it can be difficult, if not impossible, for human subjects researchers to gain access to the facilities and personnel necessary to develop a holistic and ecological understanding of the cognitive work.

[1] These statistics are taken from the August 21, 2012 of The George Washington University's "Face the Facts USA" program. Found at: http://www.facethefactsusa.org/facts/where-the-battle-lines-are-lines-of-code

C. Stephanidis (Ed.): Posters, Part II, HCII 2013, CCIS 374, pp. 509–513, 2013.

Without access, we must turn our attention to other, established methodologies, such as scaled world simulations, to help drive future human-computer interaction research in the context of cyber operations. Therefore, the purpose of this article, is to present a new team-based simulation, based off the NETS architecture [1], developed to simulate the individual and team cognitive requirements of cyber security work. In the following sections, we will present a new simulation, teamNETS and discuss its implementation and utilization in a human-computer interaction research program.

2 Simulating Cyber Operations

2.1 Ecological Grounding

Much of the previous work in scaled world simulations situates within traditional command and control environments such as battlefield operations and emergency response. While this research has provided us with invaluable knowledge on how individuals, teams, and technology operate in a multitude of contexts, the transfer from the physical to the cyber battlefield may be too drastic of paradigm shift. The cyber battlefield does not abide by the same laws by which the traditional battlefield operates. Traditionally, wars are fought against soldiers on a defined battlefield, during a set period. The cyber battlefield however, transcends army's and soldiers, and consists of civilians who possess the knowledge and resources to execute complex and costly multi-stage cyber-attacks across time and space. These inherent complexities of the cyber-environment create unique demands and stresses on the cognitive work and technologies operating within.

Leveraging these paradigmatic differences and ethnographic research by Tyworth et al. [2], attributes of the cyber environment were carefully extracted and implemented into teamNETS to provide a rich and immersive environment for human-computer interaction research.

2.2 The TeamNETS Simulation

History. TeamNETS builds upon the NeoCITIES Experimental Task Simulator (NETS) platform. The NETS platform is the newest iteration of the NeoCITIES simulation, which has been an effective test bed for team cognition research for close to 10 years [3-5]. Due to the scalability of NETS, and its ability to rapidly develop and deploy realistic cyber-security simulations, it offered a perfect platform for teamNETS.

TeamNETS Interface. Based on previous research of the design of simulation user interfaces [6] and an assessment of freely available cyber security tools, a simple user interface was designed. Careful consideration went into the design of the simulation user interface, as it is the player's only window into the state of the scaled world thus having a major impact on their performance. The final design (Figure 1) of the interface requires players monitor multiple resources, interpret complex data sets, and make multi-tiered decisions within the context of cyber-security.

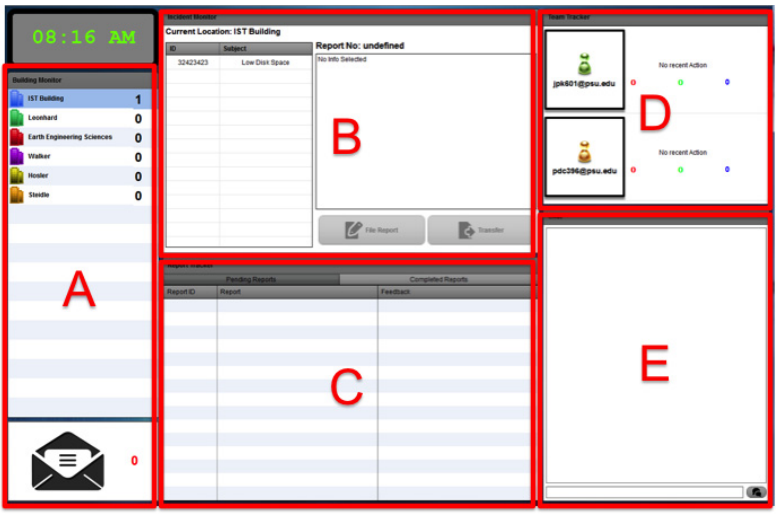

Fig. 1. teamNETS Interface

The main teamNETS interface consists of 5 components, the Location Tracker (A), Incident Report Monitor (B), Action Report Monitor (C), Team Monitor (D) and Chat (E). In addition to these components, there are pop-up windows to allow players to transfer information and file action reports. This interface allows players to monitor different locations on the simulated network, investigate or transfer emerging events, file action reports, and monitor individual and team progress in the simulation.

Playing teamNETS. In *teamNETS* simulations, teams include three participants. Each player is assigned a specific specialty, intrusion detection, malicious software detection, or policy management based off of the four primary functional domains found in Tyworth et al [2][2].

In *teamNETS*, players are responsible for monitoring locations for events, interpreting event descriptions, submitting action reports, and sharing information with their teammates. During a scenario, each player will receive reports of possible threats that are occurring on the network at varying time intervals. When a player recognizes an actual threat, in the location tracker (A in Figure 1), they must use the incident report monitor (B in Figure 1) to read the event description (in the form of a textual description and/or computer log file). Once they have identified the problem, they have two courses of action, try to mitigate the threat by filing an action report, or transfer the event to another player who may be better suited for that particular type of threat.

To mitigate a threat, players file action reports that consist of a categorization of the type of threat that it is and extra meta-data of specifics of the threat. Depending on how accurate the categorization, and meta-data is, their score will be either higher or

[2] Due to the constraints of the simulation, and focuses on reactive cyber operations, we removed threat landscape analysis from the final role structure.

lower. If a player chooses to not attach a piece of meta-data, they will receive no negative points, however if they attach an incorrect piece, it will negatively impact their score.

If a player does not know how to solve an event (i.e. does not know the correct meta-data or categorization), they can rather transfer the incident to another player. This information sharing recreates the report transfers found in the work of Tyworth et al. [2], and is a regular occurrence in cyber operations.

After filing a report, players receive feedback in the action report monitor (C in Figure 1) on the accuracy of their report and whether or not the threat was removed from the network. In addition to the information sharing mechanisims, players can maintain awreness of their teammates actions through the team tracker (D in Figure 1), as well as communicate via the chat panel (E in Figure 1).

Measuring Cognition in teamNETS. As a platform, *teamNETS* lends itself to conducting basic, to high-fidelity human-computer interaction research. At it's core, *teamNETS* is driven by the Human Performance Scoring Model [7], to assess the performance of individuals and teams within the cyber environment. The Human Performance Scoring Model is a multi-dimensional metric that accounts for accuracy and reaction time. This metric has been shown to be a useful measurement of various aspects of team cognition [3].

In addition to raw performance, *teamNETS* has built in data collection mechanisims to capture more abstract components of team cognition and collaboration. Metrics such as communication patterns and information sharing allow researchers to hone in on the behavioral aspects of the collaboration during each simulation. Finally, *teamNETS* has built in support for subjective measures of situation awarnesness (i.e. SAGAT [8]), workload (i.e. NASA TLX), and team mental models.

3 Conclusion and Future Work

In this paper, we have presented an overview of a new experimental platform for studying various aspects of team cognition in distributed cyber teams. Based off of a previously established simulation platform (NETS) we used ethnographic research of cyber security analysts to build a realistic task that can be used to study aspects of individual and team cognition, as well as other Human Computer-Interaction Issues, in a controlled laboratory setting.

Currently, *teamNETS* has been deployed in a study to assess how different types of team knowledge structures impact team performance and collaborations (Mancuso HFES), and assess the utility of shared virtual feedback in improving transactive memory systems for distributed teams [10]. Moving forward, we hope to expand the breadth of *teamNETS* to account for other functional domains within the cyber opperations space. In addition, we hope to continue to move forward with developing new, and introducing established metrics of cognitive and collaborative behavior within the simulation.

Acknowledgements. Work on this paper was partially supported by U.S. Army Research Office (ARO) MURI Grant "Computer Aided Human Centric Cyber Situation Awareness" W911-NF-09-1-0525. The Opinions expressed in this paper are those of the authors only and do not necessary represent the official position of the Army Research Office, the US Army, the Department of Defense or the Pennsylvania State University.

References

1. Mancuso, V.F., Minotra, D., Giacobe, N., McNeese, M., Tyworth, M.: idsNETS: An experimental platform to study situation awareness for intrusion detection analysts. In: 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 73–79. IEEE (2012)
2. Tyworth, M., Giacobe, N.A., Mancuso, V.: Cyber situation awareness as distributed socio-cognitive work. In: Proc. of SPIE, vol. 8408, pp. 84080F–1 (2012)
3. Hamilton, K., Mancuso, V., Minotra, D., Hoult, R., Mohammed, S., Parr, A., Dubey, G., McMillan, E., McNeese, M.: Using the NeoCITIES 3.1 simulation to study and measure team cognition. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 54(4), 433–437 (2010)
4. Hellar, D.B., McNeese, M.: NeoCITIES: A simulated command and control task environment for experimental research. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 54(13), 1027–1031 (2010)
5. McNeese, M.D., Bains, P., Brewer, I., Brown, C., Connors, E.S., Jefferson, T., Jones, R.E.T., Terrell, I.: The NeoCITIES simulation: Understanding the design and experimental methodology used to develop a team emergency management simulation. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 49(3), 591–594 (2005)
6. Mancuso, V., Hamilton, K., McMillan, E., Tesler, R., Mohammed, S., McNeese, M.: "What's on "Their" Mind Evaluating Collaborative Systems Using Team Mental Models. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 55(1), 1284–1288 (2011)
7. Wellens, A.R., Ergener, D.: The CITIES Game. Simulation & Gaming 19(3), 304 (1988)
8. Endsley, M.R.: Situation awareness global assessment technique (SAGAT). In: Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, NAECON 1988, pp. 789–795. IEEE (1988)
9. Mancuso, V.F., McNeese, M.D.: Effects of Integrated and Differentiated Team Knowledge Structures on Distributed Team Cognition. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 56(1), 388–392 (2012)
10. Mancuso, V.F.: An Interdisciplinary Evaluation of Transactive Memory in Distributed Cyber Teams. PhD diss., Pennsylvania State University (2012)