PERSPECTIVES ON THE ROLE OF COGNITION IN CYBER SECURITY

Session Chair: Michael McNeese, Ph.D.
The Pennsylvania State University

Panelists:

Nancy J. Cooke, Ph.D., Arizona State University
Anita D'Amico, Ph.D., Secure Decisions
Mica R. Endsley, Ph.D., SA Technologies, Inc.
Cleotilde Gonzalez, Ph.D., Carnegie Mellon University
Emilie Roth, Ph.D., Roth Cognitive Engineering
Eduardo Salas, Ph.D., University of Central Florida

The cyber security task is an intensely cognitive task that is embedded in a large multi-layered sociotechnical system of analysts, computers, and networks. Effective performance in this world is hampered by enormous size and complexity of the network data, the adaptive nature of intelligent adversaries, the lack of ground truth to assess performance, the high number of false alarms presented by automated alerting systems, by organizational stove pipes thwarting collaboration, and by technology that is thrown at the problem without an adequate understanding of the human needs. Further, the consequences of effective system performance in the cyber security domain are unparalleled because our world is so dependent on its cyber infrastructure. We have assembled a panel of six experts in cognitive engineering to provide perspectives on the cyber security problem and promising solutions.

 DOI 10.1177/1071181312561063

INTRODUCTION

Contemporary perspectives within the cyber security community unfortunately repeat the history of the recent past in ignoring the impetus of the human factor within complex systems. Although cyber security is necessarily coupled with technological substrates (including automation software, sensors, information networks, social-mobile-cloud computing, and hardware infrastructure), it is embedded within the broader situated context mediated by human and social interaction.

Issues that arise in cyber security areas such as intrusion detection, hacking attacks, and network threats are a) Not subject to the laws of physical space (they incur within the confines of a cyber-space), b) Amplified through extreme order of scale requirements (e.g., millions of attacks can be launched automatically and repeatedly from a large number of different sources within a very short temporal frame), and c) Complicated owing to organizational stove-piping that inhibits collaboration and the cross flow of information. In turn, the first level cyber security response (i.e., a techno-centric approach) has been to generate an array of automated computer system sensors to detect and alert human analysts in charge of managing cyber security. Unfortunately these systems produce a high number of false alarms and have algorithms that make rigid assumptions that compromise performance.

Situated cognition within this kind of unprecedented environment places much dependency on generative learning, deep levels of thinking and perception (situation assessment, sense making, information seeking, decision making, and visualization), and *distributed collaboration* to execute coordination, communication, and joint action. To make matters worse cyber-space can be illusory and easily constructed to afford deception, spoofing, and a false sense of "security". Given these unique demands, this panel of leading experts is brought together to examine various perspectives of cognitive science/cognitive engineering as a basis to understand cyber security from their Weltanschauung. The goal is to present six different themes from experts, lead discussion and obtain audience participation to develop a genuinely interdisciplinary synthesis that leads to a situated cognition purview.

PANELIST ABSTRACTS

Cyber Security and the Role of Collaboration

Nancy J. Cooke, Ph.D.
Arizona State University

Cyber analysts are faced with extraordinary amounts of information to sift through. Situation awareness requires that various pieces of information be connected in space and time. This connection necessitates collaboration among analysts working at different levels and on different parts of the system. The science of teamwork with evidence-based training, assessment, and design for collaboration has much to offer this problem.

Observations (Champion, Rajivan, Cooke, & Jariwala, 2012) have indicated that coordination and collaboration among analysts in cyber systems is minimal at best. If it happens, it is largely through discussion, as tools and visualizations to support collaboration are limited. Coordination across teams is *ad hoc* and burdened by security and information system interoperability challenges. Team roles are neither clearly defined, nor uniform across settings. Team training is absent.

The good news is that there is much low hanging fruit. User-centered tools can be developed to facilitate coordination, team training in simulators and through live exercises can be carried out and team roles can be designed and delineated to systematize information coordination for system effectiveness and resilience.

Cyber Security, Visualizations and Visual Analytics

Anita D'Amico, Ph.D.
Secure Decisions

Network defense analysts comb through large volumes of network data and intrusion detection alerts to discover real attacks amidst false alarms, identify suspicious activities that may have slipped through the security sensors, detect and report vulnerabilities, and identify unauthorized usage and policy violations that may expose a network to greater risk of compromise. These cyber defense analysts, regardless of their specific role, strive to attain and maintain *situational awareness* of the networks they defend and the attackers they defend against; this awareness includes discovering the unexpected. Visualizations and visual analytics that allow analysts to move from global views of network activity to detailed views of individual IP address activity, can assist the analyst in maintaining awareness and discovering the unexpected.

Because no single visualization or visual analytic technique will support all the different network defense roles, visualization designers must focus on the *specific* role of the target user, and the stage of situational awareness the visualizations are intended to support: perception, comprehension, or projection. New visual idoms may not be needed; network defenders are clever at adapting visualizations from other domains and applying them to their needs. Whatever visual designs are used, the interaction that is made available to network defenders is a key to their utility. In addition to the "overview, zoom, drill-in'' mantra, analysts need to share items of interest that they discovered through a visual inquiry, annotate visualizations, be able to apply complex filters to the data and have aids to recalling those filters, and communicate their findings using other visualizations that are more comprehensible to non-experts.

Situation Awareness in Cyber Operations

Mica R. Endsley and Erik Connors
SA Technologies, Inc.

Before cyber warriors can act to defend against these attacks, perform recovery actions, or even retaliate, they must first achieve and maintain a level of situation awareness (SA) that allows them to identify, understand, and anticipate evolving threats. Achieving SA for any complex domain is always a unique blend of technology with human cognitive abilities. Establishing effective understanding of the complex and often hidden aspects of the cyberspace domain stresses this technology-human relationship beyond that of typical military and intelligence applications. The extreme volume of data and the speed at which that data flows rapidly exceeds human cognitive limits and capabilities. Additionally, new methods of attack and exploitation are constantly being developed and permuted in order to circumvent existing cyber defense methodologies.

This motivates the development of new technologies that can operate in these extreme conditions to effectively augment human understanding and decision-making. However, to ensure that technology developments are appropriately focused, it is first necessary to fully understand the requirements for cyber defense SA. This begins with developing an understanding of the effects of disruptions and information attacks on cyber systems, the information that is required to understand these cyber events and situations, the decisions that operators are required to make, and how technology solutions will be evaluated in their ability to improve SA and the decision making processes.

This presentation will focus on defining situation awareness needs within the context of the cyberspace environment. In particular the role of both technological solutions and human decision making will be discussed as they inter-relate to create effective systems for countering potential cyber attacks.

What, So What, and Now What: Using Cognitive Engineering Methods to Define Decision-Support Requirements for Cyber Security

Emilie Roth, Ph.D.
Roth Cognitive Engineering

Cyber Network degradation and exploitation can covertly turn an organization's technological strength into operational vulnerabilities. While much of the attention in both military and commercial cyber security communities has been on abrupt, blunt, network attacks, the most insidious threats to an organization are subtle attacks that compromise databases, processing algorithms, and displays. These have the potential to more profoundly undermine the ability of an organization to meet its mission objectives. There is growing appreciation that cyber security requires active participation of not only information technology specialist but also system end-users and decision-makers at all levels of an organization.

There remains a wide gap between the cyber security awareness needs of individuals and the tools made available to them to detect and respond to cyber security breaches. Most cyber security support systems in place today do little more than list instances of intrusion attempts, attack types and attack sources. As Gualtieri and Elm (2002) point out this is analogous to a military decision aid that reports the number and type of munitions fired at friendly forces without providing information on the impact of those fires. In contrast, as one military commander recently put it (in response to an inadequate briefing during a simulated cyber

security breach), what is needed for effective operational response is not only to know 'the what' but also the 'so what' (the implications of a breach in operational terms) and the 'now what' (the options available for continuing to meet organization mission objectives).

Cognitive engineering methods, ranging from cognitive task analysis and cognitive work analysis, to ecological interface displays and collaborative automated aiding technologies can play a valuable role in defining the critical decisions involved in preventing, detecting, and responding to cyber security breaches at all levels of an organization, and creating visualizations and decision-support systems that provide the needed information in forms that are easy to assimilate. Recent successful examples will be used to illustrate this.

From Individual Decisions from Experience to Behavioral Game Theory: Lessons for Cybersecurity

Cleotilde Gonzalez
Carnegie Mellon University

Understanding of how defender and adversarial behaviors influence accurate and timely detection of cyber attacks has become more important as cyber attacks become common and threaten national security. We use models of human behavior, based on the Instance-Based Learning Theory (IBLT) (Gonzalez, Lerch & Lebiere, 2003), to help predict the influence of defender and adversarial behaviors on cyber attack detection. IBL models have been highly successful in representing and predicting individual's behavior of decisions from experience (see Gonzalez & Dutt, 2011 for a summary of applications of IBL models). Currently, we are using these models to represent a security analyst's experience and cognitive characteristics that would result in accurate predictions of threat identification and cyber-attack detection (Dutt & Gonzalez, 2012; Dutt, Ahn, & Gonzalez, 2012). The IBL models derive predictions on the accuracy and timing of threat detection in a computer network (i.e., cyber situation awareness or cyberSA). I will summarize the current state of models at the individual level. Next, I will discuss a central challenge arising from the success of modeling human behavior in making decisions from experience: our ability to scale these models up to explain non-cooperative team behavior in a dynamic cyberspace.

Cyber Security: A Team Sport

Eduardo Salas
University of Central Florida

Because cyber security is a complex branch of systems and networks with potentially devastating consequences if there are breeches in security, it often necessitates a team to manage all of the complicated parts seamlessly. At the heart of successful teams lies teamwork. Some of the most fundamental components of teams include: cooperation, communication, coordination, and cognition. The first component, cooperation, refers to the team feelings, attitudes, and beliefs that drive behavioral action. Empirical research has demonstrated a link between attitudes and desired team outcomes (e.g., Colquitt, Scott, & LePine, 2007).

The second facet of teamwork is communication, which is "the exchange of information between a sender and a receiver" (Salas, Wilson, Murphy, King, & Salisbury, 2008, p. 335). A recent meta-analysis provided more definitive evidence to the criticality of information sharing (i.e., communication) for effective team performance (Mesmer-Magnus & DeChurch, 2009).

The third element of teamwork, coordination, is the utilization of team behavioral processes being leveraged to transform resources to outcomes (Sims & Salas, 2007). Indeed, studies have provided support for teams that exhibit better performance when displaying effective and efficient coordinating behaviors (Schaafstal, Johnston, & Oser, 2001; Weingart, 1992).

The fourth component, team cognition, refers to the shared knowledge regarding the roles, responsibilities, and capabilities of each team member (Salas et al., 2007). Both field and laboratory research has empirically shown that shared knowledge and understanding affect team behaviors and subsequently, performance (see Mathieu et al., 2008 for a review). Unquestionably, the attitudes (i.e., cooperation), behaviors (i.e., communication and coordination), and cognitions are necessary for all teams, but they are particularly relevant in complex and high-risk situations. This talk will address how these components of teamwork are related to the field of cyber security.

ACKNOWLEDGEMENT

The work of Cooke, Gonzalez, and McNeese was supported by ARO W911NF-09-1-0525 (MURI).

REFERENCES

Champion, M., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-Based Cyber Defense Analysis. *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support.* March 6-8. New Orleans, LA.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology, 92*(4), 909-927.

Dutt, V., & Gonzalez, C. (2012). Cyber Situation Awareness: Modeling the Security Analyst in a cyber-attack scenario through Instance-based Learning. In C. Onwubiko & T. Owens (Eds.), *Situational Awareness in Computer Network Defense: Principles, Methods and Applications*, IGI Global, doi: 10.4018/978-1-46660-104-8. In Press.

Dutt, V., Ahn, Y., & Gonzalez, C. (2012). Cyber Situation Awareness: Modeling Detection of Cyber Attacks with Instance-Based Learning Theory. Under Review.

Gonzalez, C. & Dutt, V. (2011). Instance-Based Learning: Integrating Decisions from Experience in Sampling and Repeated Choice Paradigms. *Psychological Review, 118*(4), 523-551, doi: 10.1037/a0024558.

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

Gualtieri, J. W. and Elm, W. C. (2002). Power tool for countering cyberwar: Visualizations for information assurance and computer network defense. *Proceedings of the Human Factors*

and Ergonomics Society Annual Meeting September 2002 46: 463-467.

Mathieu, J. E., Maynard, M. T., Rapp, T., & Gilson, L. L. (2008). Team effectiveness 1997-2007: A review of recent advancements and a glimpse into the future. *Journal of Management, 34*(3), 410-476.

Mesmer-Magnus, J. R., & DeChurch, L. A. (2009). Information sharing and team performance: a meta-analysis. *Journal of Applied Psychology*, *94*(2), 535-546.

Salas, E., Rosen, M.A., Burke, C.S., Nicholson, D., & Howse, W.R. (2007). Markers for enhancing team cognition in complex environments: The power of team performance diagnosis. *Aviation, Space, and Environmental Medicine, 78*(1), B77- B89.

Salas, E., Wilson, K. A., Murphy, C. E., King, H., & Salisbury, M. (2008). Communicating, coordinating, and cooperating when lives depend on it: Tips for teamwork. *Joint Commission Journal on Quality and Patient Safety, 34*(6), 333-341.

Schaafstal, A. M., Johnston, J. H., & Oser, R. L. (2001). Training teams for emergency management. *Computers in Human Behavior, 17*, 615-626.

Sims, D. E., & Salas, E. (2007). When teams fail in organizations: What creates teamwork breakdowns? In J. Langan-Fox, C. L. Cooper, & R. J. Klimoski (Eds.), *Research companion to the dysfunctional workplace: Management challenges and symptoms* (pp.302-317). Cheltenham, United Kingdom: Edward Elgar Publishing Limited.