Form Approved
OMB No. 0704-0188

REPORT DOCUMENTATION PAGE

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS**.

1. REPORT DATE *(DD-MM-YY)*
21-10-16

2. REPORT TYPE
Conference Proceedings

3. DATES COVERED *(From - To)*
10/2015 – 03/2016

4. TITLE AND SUBTITLE

Addressing Human Factors Gaps in Cyber Defense

5a. CONTRACT NUMBER
FA8650-14-D-6501-0009

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Alex Vieane[1], Dr. Gregory Funke[2], Dr. Robert Gutzwiller[3], Dr. Vincent Mancuso[4], Dr. Ben Sawyer[5], and Dr. Christopher Wickens[1]

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
H0HJ (53290813)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

[1]Colorado State University, Fort Collins, CO; [2]Air Force Research Laboratory, Wright-Patterson AFB, OH; [3]Space and Naval Warfare Systems Center Pacific, San Diego, CA; [4]MIT Lincoln Laboratory, Lexington, MA; [5]Massachusetts Institute of Technology AgeLab, New England University Transportation Center, Cambridge, Massachusetts

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Materiel Command
Air Force Research Laboratory
711th Human Performance Wing
Airman Systems Directorate
Warfighter Interface Division
Applied Neuroscience Branch
Wright-Patterson Air Force Base, OH 45433

10. SPONSORING/MONITORING AGENCY ACRONYM(S)
711 HPW/RHCP/RHCPA

11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

88ABW Cleared 03/18/2016; 88ABW-2016-1329.
Human Factors and Ergonomics Society 2016 Annual Meeting (HFES) 19 – 23 September 2016

14.

Cyber security is a high-ranking national priority that is only likely to grow as we become more dependent on cyber systems. From a research perspective, currently available work often focuses solely on technological aspects of cyber, acknowledging the human in passing, if at all. In recent years, the Human Factors community has begun to address human-centered issues in cyber operations, but in comparison to technological communities, we have only begun to scratch the surface. Even with publications on cyber human factors gaining momentum, there still exists a major gap in the field between understanding of the domain and currently available research meant to address relevant issues. The purpose for this panel is to continue to expand the role of human factors in cyber research by introducing the community to current work being done, and to facilitate collaborations to drive future research. We have assembled a panel of scientists across multiple specializations in the human factors community to have an open discussion regarding how to leverage previous human factors research and current work in cyber operations to continue to push the bounds of the field.

15. SUBJECT TERMS

Cyber security, cyber operations, human factors

16. SECURITY CLASSIFICATION OF:

a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	**17. LIMITATION OF ABSTRACT:**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
Unclassified	Unclassified	Unclassified	SAR	5	Gregory Funke
					19b. TELEPHONE NUMBER

ADDRESSING HUMAN FACTORS GAPS IN CYBER DEFENSE

Panel Chair:
Alex Vieane, Colorado State University

Panelists:
Dr. Gregory Funke, Air Force Research Laboratory
Dr. Robert Gutzwiller, Space and Naval Warfare Systems Center Pacific
Dr. Vincent Mancuso, MIT Lincoln Laboratory
Dr. Ben Sawyer, MIT AgeLab
Dr. Christopher Wickens, Colorado State University

Cyber security is a high-ranking national priority that is only likely to grow as we become more dependent on cyber systems. From a research perspective, currently available work often focuses solely on technological aspects of cyber, acknowledging the human in passing, if at all. In recent years, the Human Factors community has begun to address human-centered issues in cyber operations, but in comparison to technological communities, we have only begun to scratch the surface. Even with publications on cyber human factors gaining momentum, there still exists a major gap in the field between understanding of the domain and currently available research meant to address relevant issues. The purpose for this panel is to continue to expand the role of human factors in cyber research by introducing the community to current work being done, and to facilitate collaborations to drive future research. We have assembled a panel of scientists across multiple specializations in the human factors community to have an open discussion regarding how to leverage previous human factors research and current work in cyber operations to continue to push the bounds of the field.

Defense in cyberspace is a high-ranking national security concern, supported by recent congressional testimony noting that the U.S. saw a 782% increase (from 5,503 to 48,562 cases) in the number of reported cyber attacks against federal agencies from 2006 to 2012 (GAO-13-462T). Recent revelations of large scale data breaches in both the private and public sectors (e.g., Kuranda, 2015) further emphasize the need for improved cyber defense. In response to these and other emerging cyber threats, the President's Fiscal Year 2017 budget called for $19 billion in cyber security spending, an approximate 35 percent increase over current spending levels (Calmes, 2016). In addition, for the first time the budget explicitly identifies human factors research in cyber as a priority (Waldrop, 2016).

Given the importance of cyber defense to national security, it is critical that the human factors research community continues to contribute to this difficult problem area. Significantly, three panel discussions devoted to human factors issues in cyber have been featured in recent Annual Meetings of the Human Factors and Ergonomics Society (i.e., Knott et al., 2013; Mancuso et al., 2014; McNeese et al., 2012). These panels brought together researchers with a variety of backgrounds to discuss their unique perspectives on the role of human factors in cyber operations, and have helped initiate discussions concerning contributions human factors researchers and practitioners can make to cyber security. The purpose of the current panel is to continue this trend.

PANELIST ABSTRACTS

Training Challenges in Cyber Security

Dr. Gregory Funke
Air Force Research Laboratory

With our nation's growing reliance on cyber systems, the need for resilient and effective cyber operations has become increasingly apparent (Maybury, 2015). To date, most of the research in cyber security has been focused on technology applications (e.g., network intrusion detection sensors and algorithms, intelligent system designs, etc.), thus ignoring consideration of the critical roles humans play (e.g., applying these technologies, assimilating information, and arriving at threat diagnoses) in cyber operations. To fully capitalize on the promises of advanced cyber security technologies we must also understand the roles, tasks, and responsibilities of human operators in these environments.

At present training for careers in cyber defense are largely unstandardized. Novice cyber defenders are likely to have disparate backgrounds, leading to partial or incomplete understanding of system vulnerabilities. These deficits are currently overcome through on-the-job-training and certificate programs, but this requires commitment of significant additional investments (in the forms of time and resources) transforming novices into expert cyber defenders. Even after defenders develop a degree of expertise, the rapid pace of advancements in malicious software and defensive counter software frequently outpaces their opportunities to remain current.

In military contexts, this problem is exacerbated by job stressors, such as long work shifts, significant manpower shortages, and slow moving government bureaucracy which

Not subject to U.S. copyright restrictions. DOI 10.1177/1541931213601176

DISTRIBUTION STATEMENT A. Approved for public release. Cleared, 88PA, Case #2016-1329.

impairs defenders' choices with regard to software platforms (Chappelle et al., 2013). The net result appears to be that many cyber defenders receive substantial training in the military, but separate as soon as they are able, transitioning to higher paid, and potentially less stressful, work in the private sector, further exacerbating manpower shortages in many units (Apps & Goh, 2013).

The human factors community is in a unique position to make contributions in this area, as many of the relevant issues have been successfully addressed in existing work contexts (e.g., shift work), while others, such as approaches to accelerate training, provide novel areas for researchers to focus their efforts on.

Cyber-Cognitive Situation Awareness

Dr. Robert Gutzwiller
Space and Naval Warfare Systems Center Pacific

Cyberspace is a realm of dynamic information transmittal. Information is literally moving at the speed of light through hundreds of thousands of connections over a vast array of networks and billions of devices. Naturally this precludes an easily conjured understanding of what any given cyber analyst sees and does. For defenders in particular, I take some effort to define that cyberspace defense is multifaceted. Defense improvements can be as simple as network users choosing not to click on phishing emails; given the proclivity for these types of cyber vulnerabilities this is a relevant area to address. But for the current purposes I believe we must dig deeper into another human element in cyber defense, that of the analyst (e.g., D'Amico et al., 2005). Analysts operate closely with the literal network communication and transmission, using software tools to examine down to the level of packets of information and internet protocol addresses. The tools, often command-line driven, monitor the network activity, help parse and search through information, and track potential and current threats to security. These threats change on a daily basis with every new patch and update to programs and operating systems, as well as hardware changes. The number of threats is always increasing, and there are an unknown amount of so-called "zero-day" threats which have no current mitigation. In all respects, defenders are at the mercy of cyber attackers.

What I am attempting to convey is how necessary it is for cyber defenders to perceive and understand disparate elements of network information in order to determine whether a malicious entity or program is present or attempting an attack. Currently this information is noisy, it is rarely correlated and it is almost never linked with the users' goal of maintaining mission-critical systems or projecting the ability to execute future courses of action. Cyber defense is easily related to a theory of situation awareness (Endsley, 1995), and thus stands a good chance of benefiting from similar study. It should be noted that cyber situation awareness as a concept is actually nothing new: Tim Bass coined the phrase over 15 years ago (Bass, 2000). He was keen at the onset to point out the technological elements to cyber awareness - ways that the system could be made to identify, share and fuse information, to enhance a computer's representation of the environment. But it was simultaneously emphasized that this situation awareness was a critical necessity for humans to possess. It was not enough in this definition to fuse information and represent it within the system, and then assume human awareness.

Unfortunately the audience for Bass's article appears to have fixated on the technocentric bent of cyber situation awareness and its various difficulties. The human, as so often is the case, has in turn been neglected in cyber defense, only recently returning to focus (e.g., Champion et al., 2012; Mancuso et al., 2012; Giacobe, 2013; Gutzwiller et al., 2015). I promote *cyber-cognitive situation awareness* as the proper terminology to identify that in this domain, we are interested in the human perception, understanding, and prediction of the cyber defensive space. Naturally, this is a human-systems integration perspective, and one that fits seamlessly with that of cognitive engineering efforts that are just beginning in the cyber domain. It is critical that the community developing interfaces and visualizations for cyberspace recognize that awareness is not achieved by simply displaying all of the possible information from the system; instead we need situated information, to incorporate the needs of the operators, and a system which can account for the dynamics of both.

Cognitive Coordination of Multi-Sensor Cyber Data

Dr. Vincent Mancuso
MIT Lincoln Laboratory

In Joint Publication 3-13, building and maintaining Cyberspace Situational Awareness (Cyber SA) is identified as a key function for cyber operations. From a computer science and engineering perspective, Cyber SA is an issue solved through maturing, improving, and expanding cyber sensor technologies. The goal of such technologies is to provide data from across a cyber landscape to create a more complete picture of the current situation and potential emerging threats. While these technologies provide a greater breadth of data to an analyst, the challenge of triangulating and fusing the data across sensors becomes unmanageable as the amount of available data increases. Unlike traditional operating environments, in cyber there is a fundamental disconnect between the analyst and their environment, and cyber sensor data is devoid of ecological and contextual anchors (McNeese, Mancuso, McNeese, Endsley, & Forster, 2013). Without anchors, the relationships across cyber sensors and data are only visible through an interpretation of data within the cognitive mind of an individual.

Currently, this task, also known as multi-sensor information fusion, is done manually, often through multiple pieces of software with little or no interoperability. In order to gain a more holistic understanding of the event, operators must extract data from a tool onto a distributed cognitive artifact, such as a word document or notebook paper, and manually "pivot" to another piece of software and search for related data. This pivot is done using correlational linkages, often in the form of text-based data that is made up of time-stamps, IP addresses, host names, port numbers, and codes.

Because of this, the relationships and interdependencies across sensors exist only in the mind of an individual analyst, taxing their working memory and making the maintenance of their Cyber SA challenging. This is even further magnified when scaling to the team, or organizational level, as many of the cyber analysts have diverging mental models of the environment, divided across multiple types of cyber operations (Tyworth, Giacobe, Mancuso, McNeese, & Hall, 2013). Given the importance of Cyber SA, and the importance of the human, there is a critical need for Human Factors research to compliment the emerging sensors and data from other research domains.

A potential solution to this problem may be found in interactive visual analytic techniques, such as coordinated views. These techniques help users perceive complex and dynamic relationships in the underlying data, facilitating comprehension and pattern recognition. Coordinated views have been used in multiple domains (cf. Roberts, 2007), however current work in cyber is fairly limited and does not account for the human (e.g. Noel, Jacobs, Kalapa, & Jajodia, 2005). In pursuit of this problem, we present the Integrated Open Source Architecture (IOSA), as a platform to facilitate the coordination of cyber analysis across numerous sensor platforms and analysis tools. The goal of IOSA is to automate the manual "pivoting" process that cyber analysts are forced to do in current operations. IOSA is built as a wrapper for numerous cyber tools, but rather than having to manually extract and fuse data across platforms, an operator can quickly jump between platforms. This coordination not only will support the analysis process by shortening the cognitive overhead of cyber data fusion, but will also help reduce the difficulty and time associated with other articulation tasks such as briefing and report generation. In this talk, we will discuss these human factors issues, and provide examples of solutions that better enable the development and maintenance of Cyber SA.

Acknowledgements. This material is based upon work supported under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Air Force.

Vigilance in Cyber Security

Dr. Ben Sawyer
MIT AgeLab

Cyber-defenders have been shown vulnerable to the vigilance decrement (Sawyer et al., in press), a well-studied weakness in human cognition. Characterized by repetitive, seemingly simple tasks that escalate over time into hard, stressful work and compromised operator performance (Warm, Parasuraman, & Matthews, 2008), vigilance has been previously investigated in contexts including air traffic control and medical monitoring. In the cyber context, where display information density is several orders of magnitude above that seen in the aforementioned domains, the need to keep operator workload from exceeding the information processing capacities of security operators is especially crucial. Indeed, the potential use of vigilance-promoting conditions as an attack vector has been suggested (Sawyer et al., in press), and recent research into prevalence effects in email-delivered cyberattacks shows such efforts may be efficacious (Sawyer, 2015). A prevalence denial attack (PDA) would flood a network with "grey signals," purpose-built to be flagged by algorithmic defense systems for human inspection, yet easily identified as non-threats by said operators (see Sawyer et al., in press). This denial & deception (D&D) tactic would artificially depress the signal probability of candidate events presented to cyber-defenders, resulting in compromised cyber-defender accuracy and allowing genuine attacks a greater chance to avoid human detection. PDA D&D cyber tactics clearly expose the importance of the human factor in cyber-warfare, as well as the danger of network defense strategy overly focused on algorithmic protections. Such foreshadows a new class of cyber-cognitive exploits that will effectively "hack the human" rather than the machine.

Attention Switching in Cyber Security

Dr. Christopher Wickens
Colorado State University

Cyber-security analysts at whatever level they serve, must engage in extensive **attention switching**. The cyber security task is far more complex than one of simple single task vigilance. In cyber-security, such switching may be between different threads within a heterogeneous message stream; it may involve switching between different hypotheses regarding the sender's intent within a single thread; it may involve physical pivoting between different screens, or it may involve switching attention to deal with an interruption and perform a very different task.

At the same time that attention switching at many levels (cognitive, physical, task) is necessary, ample research also indicates that it is costly (see Wickens, Gutzwiller, & Santamaria, 2015 for a review). Too much, or too rapid switching can destroy task continuity (even as too few and too slow switching can create unwanted cognitive tunneling). The purpose of this presentation will be to: a) identify and analyze in more detail, different forms of switching, and their costs and benefits within a particular cyber security context; b) apply a recent model of task switching – the STOM model (strategic task overload management, Wickens, Gutzwiller, & Santamaria, 2015) – to switching and multi-tasking scenarios in the cyber-security analyst's workplace; and c) employ this model to derive certain mitigation strategies, in training, procedures, displays, and workplace layout, that may assist the analysts in their task.

REFERENCES

Apps, P., & Goh, B. (2013). *Cyber defenders are in short supply as hacking wars escalate*. NBC News. Retrieved from http://www.nbcnews.com/technology/cyber-defenders-are-short-supply-hacking-wars-escalate-8c11390053

Bass, T. (2000). Intrusion detection systems and multisensor data fusion. *Communications of the ACM, 43*, 99-105.

Calmes, J. (2016, February 09). Obama's last budget, and last budget battle with congress. *The New York Times*. Retrived from http://www.nytimes.com/2016/02/10/us/politics/obama-budget-cybersecurity-congress.html?_r=0

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012, March). *Team-based cyber defense analysis*. Paper presented at the 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), New Orleans, LA.

Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., & Hayes, W. (2013). *Sources of occupational stress and prevalence of burnout and clinical distress among U.S. Air Force Cyber Warfare Operators* (Technical Report No. AFRL-SA-WP-TR-2013-0006). Wright-Patterson Air Force Base: Air Force Research Laboratory, Human Effectiveness Directorate.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*, 229-233.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 37*, 32-64.

Giacobe, N. (2013). A picture is worth a thousand alerts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*, 172-176.

Gutzwiller, R.S., Fugate, S., Sawyer, B.D., & Hancock, P.A. (2015). The human factors of cyber network defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 59*, 322-326.

Knott, B. A., Mancuso, V. F., Bennett, K., Finomore, V., McNeese, M., McKneely, J. A., & Beecher, M. (2013). Human factors in cyber warfare: Alternative perspectives. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*, 399-403.

Kuranda, S. (2015, July 27). The 10 biggest data breaches of 2015 (so far). *CRN*. Retrieved from http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10

Mancuso, V.F., Christensen, J.C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014). Human factors in cyber warfare II: Emerging perspectives. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*, 415-418.

Mancuso, V.F., Minotra, D., Giacobe, N., McNeese, M, & Tyworth, M. (2012, March) *idsNETS: An experimental platform to study situation awareness for intrusion detection analysts*. Paper presented at the 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), New Orleans, LA.

Maybury, M. (2015). Toward the assured cyberspace advantage: Air Force cyber vision 2025. *IEEE Security & Privacy, 13*, 49-56.

McNeese, M., Mancuso, V., McNeese, N., Endsley, T., & Forster, P. (2013). *Using the living laboratory framework as a basis for understanding next-generation analyst work*. Paper presented at the SPIE Defense, Security, and Sensing, Baltimore, Maryland.

Noel, S., Jacobs, M., Kalapa, P., & Jajodia, S. (2005). *Multiple coordinated views for network attack graphs*. Paper presented at the IEEE Workshop on Visualization for Computer Security, Minneapolis, MN.

Roberts, J.C. (2007). *State of the art: Coordinated & multiple views in exploratory visualization*. Paper presented at the Fifth International Conference on Coordinated and Multiple Views in Exploratory Visualization, Zurich, Switzerland.

Sawyer, B.D. (2015). *Effects of signal probability on multitasking-based distraction in driving, cyberattack & battlefield simulation* (Unpublished doctoral dissertation). University of Central Florida, Orlando, FL.

Sawyer, B.D., Finomore, V.S., Funke, G.J., Matthews, G., Mancuso, V., Funke, M., Warm, J.S., & Hancock, P.A. (in press). Cyber-vigilance: The human factor. *American Intelligence Journal.*

Tyworth, M., Giacobe, N. A., Mancuso, V., McNeese, M., & Hall, D. L. (2013). A human-in-the-loop approach to understanding situation awareness in cyber defence analysis. *EAI Endorsed Transactions on Security and Safety, 13*, 1-6.

U.S. Department of Defense. (2012). *Joint publication 3-13: Information operations*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Waldrop, M.M. (2016). The human side of cybercrime. *Nature, 533*, 164-167.

Warm, J.S., Parasuraman, R., & Matthews, G. (2008). Vigilance requires hard mental work and is stressful. *Human Factors: the Journal of the Human Factors and Ergonomics Society, 50*, 433-441.

Wickens, C.D., Gutzwiller, R.S., & Santamaria, A. (2015). Discrete task switching in overload: A meta-analyses and a model. *International Journal of Human-Computer Studies, 79*, 79-84.