Gaps and Opportunities in Situational Awareness for Cybersecurity

ROBERT GUTZWILLER, Arizona State University, Ira A. Fulton Schools of Engineering (The Polytechnic School), Human Systems Engineering Program, Mesa, AZ

JOSIAH DYKSTRA, Cybersecurity Collaboration Center, National Security Agency, Ft. George G. Meade, MD

BRYAN PAYNE, Netflix, Los Gatos, CA

Demand is present among security practitioners for improving cyber situational awareness (SA), but capability and assessment have not risen to match. SA is an integral component of cybersecurity for everyone from individuals to business to response teams and threat exchanges. In this Field Note, we highlight existing research and our field observations, a recent review of cyber SA research literature, and call upon the research community to help address three research problems in situational awareness for cybersecurity. The gaps suggest the need to (1) understand what cyber SA is from the human operators' perspectives, then (2) measure it so that (3) the community can learn whether SA makes a difference in meaningful ways to cybersecurity, and whether methods, technology, or other solutions would improve SA and thus, improve those outcomes.

CCS Concepts: • **Security and privacy** → **Human and societal aspects of security and privacy**; *Network security*; • **Human-centered computing** → *HCI theory, concepts and models*;

Additional Keywords and Phrases: Cybersecurity, situational awareness, human factors

ACM Reference format:

Robert Gutzwiller, Josiah Dykstra, and Bryan Payne. 2020. Gaps and Opportunities in Situational Awareness for Cybersecurity. *Digit. Threat.: Res. Pract.* 1, 3, Article 18 (August 2020), 6 pages.

<https://doi.org/10.1145/3384471>

1 THE PRACTITIONERS' NEED FOR SA IN CYBERSECURITY

Practitioners in cybersecurity operate in a highly dynamic and tactical environment. The human factor affects these operations. For example, fatigue and cognitive workload resulting from cyber operations have been documented [Paul and Dykstra 2017]. One way for defenders to manage the fatigue and cognitive workload associated with security is through supporting their situation awareness [SA; Endsley 1995a], a concept most are familiar with by name or by experience.

Situation awareness refers to gathering information, perceiving and understanding the state of the world, and predicting states of the world forward in time. These are cognitive processes and activities undertaken by individuals performing dynamic tasks [Durso et al. 2007; Gutzwiller and Clegg 2013]. A demand for such awareness is generally created by having a task-related goal in mind. The driver of a car, for example, has a

Authors' addresses: R. Gutzwiller, Arizona State University, Ira A. Fulton Schools of Engineering (The Polytechnic School), 7271 E Sonoran Arroyo Mall, Santa Catalina Hall 150E, Mesa, AZ 85212, USA; email: rgutzwil@asu.edu; J. Dykstra, Cybersecurity Collaboration Center, National Security Agency, 9800 Savage Road, Ft. George G. Meade, MD, 20755, USA; email: josiah.dykstra@cyber.nsa.gov; B. Payne, Netflix, 121 Albright Way Los Gatos, CA, 95032, USA; email: bryanp@netflix.com.

Publication rights licensed to ACM. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of the United States government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only.

© 2020 Copyright held by the owner/author(s). Publication rights licensed to ACM.

2576-5337/2020/08-ART18 \$15.00

<https://doi.org/10.1145/3384471>

destination they want to reach safely, which necessitates the search for potential hazards or impediments. The first process, *perception*, relates to searching for information—looking out the windows and checking mirrors for important objects. The result of that search (there may be an obstacle or vehicle in between you and your goal) is critical for achieving the goal safely but is not all there is to achieving it. Accident avoidance requires the additional processes of *comprehension* and understanding of a complex, dynamically evolving situation, as well as using such understanding—especially once a driver has built up extensive experience—to *generate predictions* about what could happen in the near future. These three general processes; perception, comprehension, and prediction comprise a common model of human situation awareness [Endsley 1995a].

SA is relevant to individuals performing in dynamic environments, as in the case of good SA informing safe driver actions, but it also applies to teams [Salmon et al. 2009]. As related to cybersecurity, formal security groups such as computer emergency response teams (CERTs) and other communities like information sharing and analysis centers (ISACs) rely significantly on shared information, understanding, and prediction. These processes go well beyond the normal perceptual activities of an individual, and heavily rely on transmission of information via interaction between agents and systems. Therefore, teams perform a more complicated process than simply “looking” or “perceiving” information; their ability to understand and predict is similarly complicated.

Between the identification of relevant SA elements, the need to communicate and cohere as a team in support of data interpretation and understanding, and the overall workload created by this process, even within individuals and expert performers [Gutzwiller and Clegg 2013; Sohn and Doane 2004], we argue that any improved support of the operators or teams SA processes would be impactful. Investigating SA within a domain often results in improvements, somewhat obviously; in general, better awareness leads to better decisions [Endsley and Garland 2000]. In many cases, it is the predictive element—the projection of the environment in the near future—that most strongly correlates with good performance [O’Brien and O’Hare 2007; Sulistyawati et al. 2011], though some research also shows perceptual and attentional failures, such as data that are hard to detect, individual failures to monitor for new data, and misperception, make a serious impact [Jones and Endsley 1996]. In an environment with dynamic changes, understanding must also be continually generated and improved ahead of any decision opportunity [Endsley 2015; Klein 1997].

2 GAPS IN SA FOR CYBERSECURITY

Gutzwiller’s research and our additional professional field observations in government, industry, and academia suggest that the utility of SA analysis and measurement has yet to be realized in cyberspace [Gutzwiller et al. 2015], unlike in aviation, driving, process control and nuclear power plant control, healthcare, and interactions with autonomous systems [Endsley 2019]. With a few exceptions, we know of almost no experimental work on measuring or characterizing the process or product in developing cyber situational awareness from the human’s perspective. Much work in cyber SA is on data fusion models that often do not consider the humans SA directly [Barford et al. 2010]. In a majority of the existing experiments [Giacobe et al. 2013; Malviya et al. 2011; Stevens-Adams et al. 2011; Zhang et al. 2015], cyber SA is not the focus of the work, or there are ecological, methodological, or analytical concerns that preclude strong conclusions [Gutzwiller 2019]. Occasionally, good data is provided [Champion et al. 2012]. And recently, Rajivan and Cooke [2018] showed that operators with unique information often do not share it with the team, which suggests a team SA deficit.

The cyber community faces additional challenges that SA measurement may help address or reveal. Increasingly cyber environments rely on automation. There is established history of automated processes garnering less attention by supervisory human operators monitoring them, degrading SA for the task at hand [Endsley and Kiris 1995]. The loss here is especially important if the automated process could fail or error in some way; and grows worse if the automation is allowed to make decisions [Onnasch et al. 2014].

Cybersecurity is also heavily reliant on interfaces, whether terminal command lines or visual data graphics. These interfaces are crucial human interaction points for perceiving, understanding, and projecting information.

Their proper design requires study of the operators' goals, roles, and information needs [Endsley and Jones 2012], which should lead toward better awareness. Specific methodologies exist to facilitate awareness, and initial application Goal Directed Task Analysis and other cognitive task analysis methods in cybersecurity [Trent et al. 2019] suggest the effectiveness of those methods at better understanding of what human operators need to be aware [Mckenna et al. 2015].

Despite the need, and potential value added to cybersecurity by the goal of studying and improving situation awareness for human operators, there is a major gap. We find almost no research measuring SA in the cybersecurity environment [Gutzwiller 2019]. Interestingly, this is despite a wealth of reports claiming that a new or unique tool or interface, often untested, could improve it ([Gutzwiller 2019]; and see the important review by Staheli et al. [2014] of cyber visualizations in research). The claims in research literature mirror claims by industrial software solutions, which many cyber professionals abhor and abandon. Even popular tools and practices, such as the MITRE ATT&CK Framework, have not been evaluated against usability, awareness, or cybersecurity outcomes, even though it includes SA-related aspects such as account manipulation. Together, this suggests that demand for SA improvement is present, but actual capability to measure SA or apply human factors methods to properly examine this technology has not risen to match. If it could be done, then human factors application, especially for cyber operation awareness, would improve even existing state-of-the-art technology, because humans are still critical. This represents a reasonable but serious challenge. On the one hand, SA as a human-centered concept has not been prominent in cybersecurity, so it will be difficult and require multi-disciplinary collaboration to address. On the other hand, even as strictly technical capabilities have improved security, the human remains a major factor, from user, to CISO, to CERTS and SOCs.

The above led us to generate several challenges to better examine cybersecurity situation awareness. Most of these challenges should be addressed as collaborations between psychologists, human factors engineers, computer scientists, and cybersecurity experts. We note that this multidisciplinary need is a challenge in itself.

3 OPPORTUNITIES FOR SA IN CYBERSECURITY

The gaps identified here suggest the need to (1) understand what cyber SA is from the human operators' perspectives, then (2) measure it so that (3) we can learn whether SA makes a difference in meaningful ways to cybersecurity, and whether methods, technology, or other solutions would improve SA and thus, improve those outcomes. We call upon the research community to help collaboratively address these research problems.

1. **Define Cyber SA.** Today, a challenge is defining situation awareness for various types of operators, completing various types of security tasks. SOC operators, for example, may monitor firewall logs for alerts while a red team penetration test operator has very different goals such as scanning for vulnerable servers. One method could be to construct a taxonomy of security goals, tie these to the operators involved, and then determine the critical SA-related information the operators need to cognitively process to achieve the goal, beginning with the highest importance or criticality goals (e.g., the approach advocated by Endsley and Jones [2012]). This would result in a set of SA-relevant information, to be used in constructing better interfaces, processes, or reports. Many efforts like this have been undertaken [D'Amico and Whitley 2008; Erbacher et al. 2010; Gutzwiller et al. 2016; Mahoney et al. 2010] but not pursued to completion and validation through experimentation by the organizations.
2. **Measure Cyber SA.** Measurement is one enabling force toward reliable improvements in situation awareness. Measuring the veracity of human information processes (memory, attention) or awareness-based work products is the main way to measure SA. Many environments (as in the driving example) easily lend themselves to measurement, whether subjective or objective—"Did you see the bus in the right lane?" has a ground truth answer. The method of comparing the state of the world (the bus is present or not) objectively with a state of awareness (whether the operator believes a bus is present or not) across users has continued to aid system design [Endsley and Jones 2012]. Broadly, cybersecurity presents a far more

complicated domain for understanding situation awareness needs (measurement of what to perceive), how to make sense of it (measurement of whether operators and teams understand a given situation), and how to predict (measurement of expected near-future states of the environment). Defining what SA information is relevant to each is required (as stated in Challenge 1 above), but how to assess whether that information resides in the agents of the system that need it is a measurement challenge. The many theories of SA that exist each align with different types of measurement approaches that have yet to be tried in cybersecurity. For example, Endsley's theory makes use of the SAGAT method, which uses questions derived from expert knowledge elicitation to probe and measure operator SA during "break" or "pause" moments of job performance [Endsley 1988, 1995a; Endsley 2019]. Operator answers are then compared to ground truth. Other methods use subjective reporting (e.g., Taylor [1990]), though these are problematic for various reasons [Jones 2000]. Others simply imply a good or bad state of awareness based on actions operators take during operations, with no need to directly query them (e.g., Gutzwiller and Clegg [2013]). An example is measuring whether participants avoided a hazard while landing a plane; a reasonable assumption is that if they do not take action to avoid the hazard but the information to do so was available (a visible plane outside the cockpit), then they must not have been aware.

3. **Does Cyber SA Improve Security?** Defining "performance" in cybersecurity is already a challenge. Further evaluation is needed to determine whether the relationship between SA and performance in these cases is strong enough to care about. This is a separate but hybrid issue, as the relationship depends both on how cyber SA is measured and how performance is measured. The current literature is absent of these effects for cyber [Gutzwiller 2019]. In other words: SA is probably important, but what aspects of cyber performance could either high or low SA be affecting? Once SA is defined and understood, it is still unclear how performance should be defined; other domains have used decision making, reaction time, or some combination of communications and informational reporting. More broadly, performance could be viewed as risk reduction, through the lens of an analytical model such as the Factor Analysis of Information Risk (FAIR) model [Freund and Jones 2014]. A similar argument can be made for other known cognitive factors, such as the influence of individual and team mental workload, stress, fatigue, training, and expertise on performance. Interestingly, those variables are likely to exert an impact on both SA and cyber defense performance, complicating the relationship. Improved methods of analysis may be required, such as factor analytics or moderating/mediated regression models to sort out the most important influences.

If these challenges are met in whole or part, then they will lead to valuable capability; that is, organizations and researchers will be better able to define their SA requirements, determine whether cyber SA is improved by various methods, and finally whether that improvement is valuable to defense.

ACKNOWLEDGMENTS

We thank the reviewers for their valuable comments and suggestions that improved the manuscript. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official views or policies, either expressed or implied, of the U.S. Government or Department of Defense.

REFERENCES

- P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, and J. Yen. 2010. Cyber SA: Situational awareness for cyber defense. In *Cyber Situational Awareness*. Springer, Boston, MA, 3–14.
- M. Champion, S. Jariwala, P. Ward, and N. J. Cooke. 2014. Using cognitive task analysis to investigate the contribution of informal education to developing cyber security expertise. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 310–314. <http://doi.org/10.1177/1541931214581064>
- A. D. D'Amico and K. Whitley. 2008. The real work of computer network defense analysts: The analysis roles and processes that transform network data into security situation awareness. In *Proceedings of the Workshop on Visualization for Computer Security*, J. Goodall, G. Conti, and K. Ma (Eds.). Springer, Berlin.

- F. T. Durso, K. Rawson, and S. Giroto. 2007. Comprehension and situation awareness. In *Handbook of Applied Cognition*, F. Durso, R. Nickerson, S. Dumais, S. Lewandowsky, and T. Perfect (Eds.). John Wiley & Sons, West Sussex, 163–193.
- M. R. Endsley. 1988. Situation awareness global assessment technique (SAGAT). In *Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON'88)*. 789–795.
- M. R. Endsley. 1995a. Measurement of situation awareness in dynamic systems. *Hum. Fact.* 37, 1 (1995), 65–84.
- M. R. Endsley. 2015. Situation awareness: Operationally necessary and scientifically grounded. *Cogn. Technol. Work* 17, 2 (2015), 163–167. <https://doi.org/10.1007/s10111-015-0323-5>
- M. R. Endsley. 2019. A systematic review and meta-analysis of direct objective measures of situation awareness: A comparison of SAGAT and SPAM. *Hum. Fact.* <https://doi.org/10.1177/0018720819875376>
- M. R. Endsley, and D. J. Garland. 2000. *Situation awareness: Analysis and measurement*, M. Endsley and D. J. Garland (Eds.). CRC Press, Boca Raton, FL.
- M. R. Endsley and D. G. Jones. 2012. *Designing for situation awareness: An approach to human-centered design* (2nd ed.). Taylor & Francis, London.
- M. R. Endsley and E. O.Kiris, 1995. The out-of-the-loop performance problem and level of control in automation. *Hum. Fact.* 37, 2 (1995), 381–394.
- R. F. Erbacher, D. A. Frincke, P. C. Wong, S. Moody, and G. Fink. 2010. Cognitive task analysis of network analysts and managers for network situational awareness. In *Visualization and Data Analysis*, Vol. 7530. International Society for Optics and Photonics, p. 75300H.
- J. Freund and J. Jones. 2014. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, Oxford, UK.
- N. A. Giacobe, M. D. McNeese, V. F. Mancuso, and D. Minotra. 2013. Capturing human cognition in cyber-security simulations with NETS. In *Proceedings of the IEEE ISI Conference*. 284–288.
- R. S. Gutzwiller. 2019. Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment Through 2015. (No. TR-3184). NIWC Pacific San Diego United States.
- R. S. Gutzwiller and B. A. Clegg. 2013. The role of working memory in levels of situation awareness. *J. Cogn. Eng. Decis. Making* 7, 2 (2013), 141–154. <https://doi.org/10.1177/1555343412451749>.
- R. S. Gutzwiller, S. Fugate, B. D. Sawyer, and P. A. Hancock. 2015. The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 322–326. <https://doi.org/10.1177/1541931215591067>
- R. S. Gutzwiller, S. M. Hunt, and D. S. Lange. 2016. A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. In *Proceedings of the IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA'16)*. 14–20. <https://doi.org/10.1109/COGSIMA.2016.7497780>
- D. Jones. 2000. Subjective measures of situation awareness. In *Situation awareness: Analysis and measurement*, M. R. Endsley and D. Garland (Eds.). Lawrence Erlbaum Associates, Mahwah, NJ, 113–128.
- D. G. Jones, and M. R. Endsley. 1996. Sources of situation awareness errors in aviation. *Aviat. Space Environ. Med.* 67, 6 (1996), 507–512. <https://doi.org/10.1039/c4qo00187g>
- G. Klein. 1997. Developing expertise in decision making. *Think. Reason.* 3, 4 (1997), 337–352. <https://doi.org/10.1080/135467897394329>
- S. Mahoney, E. Roth, K. Steinke, J. Pfautz, C. Wu, and M. Farry. 2010. A cognitive task analysis for cyber situational awareness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 279–283.
- A. Malviya, G. A. Fink, L. Sego, and B. Endicott-Popovsky. 2011. Situational awareness as a measure of performance in cyber security collaborative work. In *Proceedings of the IEEE International Conference on Information Technology: New Generations*. 937–942. <https://doi.org/10.1109/ITNG.2011.161>
- S. McKenna, D. Staheli, and M. Meyer. 2015. Unlocking user-centered design methods for building cyber security visualizations. In *Proceedings of the IEEE Symposium on Visualization for Cyber Security (VizSec'15)*. 1–8. <https://doi.org/10.1109/VIZSEC.2015.7312771>
- K. S. O'Brien, and D. O'Hare. 2007. Situational awareness ability and cognitive skills training in a complex real-world task. *Ergonomics* 50, 7 (2007), 1064–1091. <https://doi.org/10.1080/00140130701276640>
- L. Onnasch, C. D. Wickens, H. Li, and D. Manzey. 2014. Human performance consequences of stages and levels of automation: An integrated meta-analysis. *Hum. Fact.* 56, 3 (2014), 476–488. <https://doi.org/10.1177/0018720813501549>
- C. L. Paul, and J. Dykstra. 2017. Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. *J. Info. Warfare* 16, 2 (2017), 1–11.
- P. Rajivan and N. J. Cooke. 2018. Information-pooling bias in collaborative security incident correlation analysis. *Hum. Fact.* 60, 5 (2018), 626–639. <https://doi.org/10.1177/0018720818769249>
- P. M. Salmon, N. A. Stanton, G. H. Walker, and D. P. Jenkins. 2009. *Distributed Situation Awareness: Theory, Measurement and Application to Teamwork*. CRC Press, Boca Raton, FL.
- Y. W. Sohn, and S. M. Doane. 2004. Memory processes of flight situation awareness: Interactive roles of working memory capacity, long-term working memory, and expertise. *Hum. Fact.* 46, 3 (2004), 461–475.
- D. Staheli, T. Yu, R. Crouser, S. Damodaran, K. Nam, D. O'Gwynn, and L. Harrison. 2014. Visualization evaluation for cyber security: Trends and future directions. In *Proceedings of the 11th Workshop on Visualization for Cyber Security*, 49–56.

- S. Stevens-Adams, A. Carbajal, A. Silva, K. Nauer, B. Anderson, T. Reed, and C. Forsythe. 2011. Enhanced training for cyber situational awareness. In *Foundations of Augmented Cognition*. Springer, Berlin, 90–99.
- K. Sulistyawati, C. D. Wickens, and Y. P. Chui. 2011. Prediction in situation awareness: Confidence bias and underlying cognitive abilities. *Int. J. Aviation Psychol.* 21, 2 (2011), 153–174. <https://doi.org/10.1080/10508414.2011.556492>
- R. M. Taylor. 1990. Situational Awareness Rating Technique (SART): The development of a tool for aircrew systems design. *AGARD Situation. Aware. Aerospace Operat.* 17 (1990), 23–53.
- S. Trent, R. R. Hoffman, D. Merritt, and S. Smith. 2019. Modelling the cognitive work of Cyber Protection Teams. *Cyber Defense Rev.* 4, 1 (2019), 125–135.
- H. Zhang, S. Maoyuan, D. Yao, and C. North. 2015. Visualizing traffic causality for analyzing network anomalies. In *Proceedings of International Workshop on Security and Privacy Analytics (IWSPA'15)*. 37–42. <https://doi.org/10.1145/2713579.2713583>.

Received August 2019; revised January 2020; accepted February 2020