ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 12, Issue 01, January 2022 SJIF 2021 = 7.492
A peer reviewed journal

SITUATIONAL AWARENESS GAPS AND OPPORTUNITIES FOR CYBER SECURITY

Orinov Nodirbek Toxirjonovich*; Xolmirzayeva Gulchexra Tulanovna**

*Teacher,
Department of Information Technology,
Andijan State University, UZBEKISTAN
Email id: nodirbekurinov1@gmail.com

**Teacher,
Department of Information Technology,
Andijan State University, UZBEKISTAN
Email id: egaist_1609@mail.ru

DOI: 10.5958/2249-7137.2022.00082.9

ABSTRACT

Security practitioners feel the need to improve cyber situational awareness (SA), but capabilities and assessments have not been matched. SA is an essential component of cyber security for everyone, from individuals to companies, response teams and threat exchange. In this field note, we highlight existing research and our field observations, a recent review of cyber security research literature, and call on the research community to help address three research challenges in situational awareness for cyber security. Gaps suggest the need to (1) understand what cyber is – SA from the perspective of human operators, and then (2) measure it so that (3) the community can know if SA has meaningful pathways to cyber security and if methods, technology, or other solutions are used would improve SA and thus improve would these results.

KEYWORDS: *Cyber security, Situational Awareness, Human Error.*

INTRODUCTION

THE NEED OF PRACTITIONERS IN SA FOR CYBER SECURITY

Cyber security practitioners operate in a highly dynamic and tactical environment. These operations are influenced by the human factor. For example, cyber fatigue and cognitive load have been documented [Paul and Dykstra 2017] **[1].** One way to protect HRDs to cope with safety fatigue and cognitive load is to keep them aware of the situation, a concept most are familiar with by name or experience.

Situation awareness refers to gathering information, perceiving and understanding the state of the world, and predicting future states of the world. These are cognitive processes and actions taken by people performing dynamic tasks [Durso et al. 2007 **[2]**; Gutzwiller and Clegg 2013] **[3].** The demand for such awareness usually arises from the presence in the head of a goal related to the task. For example, a car driver has a destination they want to travel safely, which requires looking for potential hazards or obstacles. The first process, *perception*, is about seeking information — looking out the window and checking important objects in mirrors. The result of

this search (maybe an obstacle or a vehicle between you and your goal) is critical to achieving the goal safely, but it is not all that is needed to achieve it. Accident avoidance requires additional processes of *understanding* and understanding a complex, dynamically changing situation, as well as using such understanding, especially when the driver has accumulated extensive experience, to *generate predictions* about what may happen in the near future. These are three general processes; perception, understanding and prediction constitute a general model of human understanding of a situation [Endsley 1995a] **[4].**

SA is relevant for people working in a dynamic environment, as is the case for a good SA that informs the driver of safe actions, but it also applies to commands [Salmon et al. 2009] **[5].** When it comes to cyber security, formal security teams like Computer Emergency Response Teams (CERTs) and other communities like Information Clearinghouse and Analysis Centers (ISACs) rely heavily on shared information, insight and prediction. These processes go far beyond normal human perceptual activity and rely heavily on the transfer of information through interactions between agents and systems. Consequently, teams perform a more complex process than simply "searching" or "perceiving" information; their ability to understand and predict is also difficult.

Between the identification of the elements of the SA, the need to communicate and articulate as a team to support data interpretation and understanding, as well as general working load created by this process, even in the indie - iCal officials and experts performers [Gutzwiller and Clegg 2013 **[3]**; Sohn and Doane 2004] **[6],** we argue that any improved support for operator or group SA processes will have a positive impact. Examining SA within a domain often leads to improvements, which is somewhat obvious; in general, better awareness leads to better decisions [Endsley and Garland 2000] **[7].** In many cases, it is the prediction element - environmental prediction for the near future that is most strongly correlated with good performance [O'Brien and O'Hare 2007 **[8]**; Sulistyawati et al. 2011] **[9]**, although some studies also show disruptions in perception and attention, such as data that are difficult to detect, individual inability to track new data and misperceptions have a major impact [Jones and Endsley 1996] **[10].** In an environment of dynamic change, understanding must also be continually generated and improved before any decision can be made [Endsley 2015 **[11]**; Klein 1997 **[12]**].

GAPS IN SA FOR CYBER SECURITY

Gutzwiller's research and our additional professional field observations in government, industry and academia indicate that the usefulness of SA analysis and measurement in cyberspace has yet to be realized [Gutzwiller et al. 2015] **[13]**, in contrast to aviation, driving, process control and nuclear power plants, healthcare and interaction with autonomous systems [Endsley 2019] **[14].** With a few exceptions, we are almost unaware of experimental work to measure or characterize a process or product in the development of cyber situational awareness from a human perspective. Much of the work in cyber - SA is conducted on data fusion models that often do not directly address human SA [Barford et al. 2010] **[15].** In most of the existing experiments [Giacobe et al. 2013 **[16]**; Malvia et al. 2011 **[17]**; Stevens-Adams et al. 2011 **[18]**; Zhang et al. 2015] **[19]**, Cyber SA is not the main topic of the work, or there are environmental, methodological or analytical problems that do not allow making unambiguous conclusions [Gutzwiller 2019] **[20].** Good data are sometimes provided. Recently, Rajivan and Cook [2018]

[21] showed that operators with unique information often do not share it with the team, which indicates a shortage of group SA.

The cyber community faces additional challenges that can help solve or identify the SA dimension. Cyber environments increasingly rely on automation. There is a history of automated processes that have received less attention from human supervising operators monitoring them, degrading the SA for the task at hand [Endsley and Kiris 1995] **[22].** Losses are especially important here if the automated process can fail or fail in some way; and it gets worse if automation allows decision making [Onnasch et al. 2014] **[23].**

Cyber security is also heavily dependent on interfaces, be it terminal command lines or graphical representations of visual data. These interfaces are key human interaction points for perceiving, understanding and projecting information.

Proper design requires an examination of the goals, roles and information needs of the operators [Endsley and Jones 2012] **[24]**, which should lead to better understanding. There are specific methodologies for raising awareness and initial application of goal-oriented task analysis and other cognitive task analysis techniques in cyber security [Trent et al. 2019] **[25]** demonstrates the effectiveness of these techniques to better understand what operators need to know [Mckenna et al. 2015] **[26].**

Despite the need and potential added value of cyber security in order to study and raise awareness of the situation for human operators, there is a major gap. We find almost no studies measuring SA in the cyber security environment. Interestingly, this is in spite of numerous reports alleging that a new and unique tool or interface, often unchecked, can improve it; see Important Review. Kibervizualizatsii in studies made Staheli et al [2014] **[27]**. The claims in the research literature reflect claims from industrial software solutions that many cyber professionals hate and reject. Even popular tools and techniques like the MITER ATT & CK Framework have not been evaluated for usability, awareness, or cybersecurity, even though they include SA-related aspects such as account manipulation. Taken together, this suggests that there is a need to improve SA, but the actual ability to measure SA or apply Human Factors techniques to properly study this technology has not yet reached the level. If it were possible, the use of human factors, especially for awareness of cyber operations, would improve even existing modern technologies, because people are still critically important. This is a sensible but serious challenge. On the one hand, SA as a human-centered concept has not gained much importance in cybersecurity, so solving it will be difficult and will require interdisciplinary cooperation. On the other hand, even though strictly technical capabilities have improved security, the human remains the main factor, from the user to the CISO, CERTS and SOC.

The above led us to create several tasks to better examine cybersecurity awareness. Most of these problems should be addressed through collaboration between psychologists, human factors engineers, computer specialists, and cybersecurity experts. We note that this interdisciplinary need is itself a problem.

OPPORTUNITIES FOR SA IN CYBER SECURITY

The gaps identified here suggest the need to (1) understand what cyber- SA is from the perspective of human operators, and then (2) measure it so that (3) we can know if SA influences meaningful cybersecurity pathways and methods, technologies or other solutions would improve

SA and thus improve these results. We call on the research community to help solve these research problems together.

1. **Give the definition of Cyber SA.** The challenge today is to determine situational awareness for different types of operators performing different types of safety tasks. SOC operators, for example, can monitor firewall logs for alerts, while a red group penetration test operator has very different purposes, such as scanning vulnerable servers. One method could be to build a taxonomy of security objectives, associate them with the operators involved, and then define the critical information associated with the SA that operators must cognitively process to achieve the objective, starting with the goals of highest importance or criticality (for example, the approach proposed by Endsley and Jones [2012] **[24]**). This will lead to a set of SA-relevant information that will be used to build better interfaces, processes, or reports. There have been many similar attempts [Erbacher et al. 2010 **[28]**; Gutzwiller et al. 2016 **[29]**; Mahoney et al. 2010] **[30]**, but not brought to completion and validation through experimentation by organizations.
2. **Measure Cyber SA.** Measurement is one of the driving forces to reliably improve situational 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) are easy to measure, both subjective and objective: "Did you see the bus in the right lane?" has a foundational answer. The method of comparing the state of the world (whether the bus is present or not) objectively with the state of awareness (whether the operator believes the bus is present or not) among users has continued to assist in the design of the system. In general, cyber security is a much more complex area to understand the need for situational awareness (measuring what should be perceived), how to understand it (measuring whether operators and teams understand a given situation), and how to predict (measuring the expected near - future state of the environment). Determining what SA information is relevant to each is required (as outlined in Task 1 above), but how to assess whether that information is in the system agents that need it is a measurement problem. Each of the many existing SA theories correspond to different types of measurement approaches that have yet to be tested in the field of cyber security. For example, Endsley theory uses the sagatah method, which uses questions derived from expert knowledge to research and the SA operator's measure during "break" or "pause" moments of work [Endsley 1988] **[31]**. The operator's responses are then compared to true. Other methods use subjective reporting (eg, Taylor [1990] **[32]**), although this is problematic for various reasons [Jones 2000] **[33]**. Others simply imply a good or bad state of awareness based on the actions that operators take during operations without having to directly query them. An example would be determining whether participants escaped a hazard when boarding an aircraft; the reasonable assumption is that if they didn't take action to avoid the danger, but information was available to do so (visible aircraft outside the cockpit), then they should not have known.
3. Increases whether the Cyber SA security? Defining "performance" in cyber security is already a challenge. Further evaluation is needed to determine if the relationship between SA and performance is strong enough in these cases to be taken care of. This is a separate but hybrid issue, as the relationship depends on both how cyber- SA is measured and how performance is measured. In modern literature, these effects for cyberspace are absent. In

other words: SA is probably important, but what aspects of cyber performance might be affected by high or low SA? After defining and understanding SA, it is still unclear how performance should be defined; other areas used decision making, reaction time, or some combination of communication and information reporting. More broadly, performance can 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] **[34].** A similar argument can be made for other known cognitive factors, such as the effects of individual and team mental workload, stress, fatigue, training, and experience on performance. Interestingly, these variables can influence both SA and cyber defense effectiveness, complicating the relationship. Improved analysis techniques such as factor analytics or moderation / mediated regression models may be required to sort out the most important influencers**. [35-37]**

If these problems are solved in whole or in part, they will lead to the emergence of valuable opportunities; that is, organizations and researchers will be able to better define their SA requirements, determine if cyber SA is improved by different methods, and finally, whether the improvement is valuable for security.

REFERENCES

1. Paul CL, Dykstra J. Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. J. Info. Warfare, 2017;16(2):1-11.

2. Durso FT, Rawson K, Girotto S. Comprehension and situation awareness. In Handbook of Applied Cognition. 2007.

3. Gutzwiller RS, Clegg BA. The role of working memory in levels of situation awareness. J. Cogn. Eng. Decis. Making 2013;7(2):141–154.

4. Endsley MR. 1995a. Measurement of situation awareness in dynamic systems. Hum. Fact. 1995a;37(1):65–84.

5. Salmon PM, Stanton NA, Walker GH, Jenkins DP. Distributed Situation Awareness: Theory, Measurement and Application to Teamwork. CRC Press, Boca Raton, FL; 2009.

6. Sohn YW, Doane SM. Memory processes of flight situation awareness: Interactive roles of working memory capacity, long-term working memory, and expertise. Hum. Fact. 2004;46(3):461–475.

7. Endsley MR, Garland DJ. Situation awareness: Analysis and measurement, In: Endsley M and. Garland DJ (Eds.). CRC Press, Boca Raton, FL; 2000.

8. O'Brien KS, O'Hare D. Situational awareness ability and cognitive skills training in a complex real-world task. Ergonomics 2007;50(7):1064–1091.

9. Sulistyawati K, Wickens CD, Chui YP. Prediction in situation awareness: Confidence bias and underlying cognitive abilities. Int. J. Aviation Psychol. 2011;21(2):153–174.

10. Jones DG, Endsley MR. Sources of situation awareness errors in aviation. Aviat. Space Environ. Med. 1996;67(6):507–512.

11. Endsley MR. Situation awareness: Operationally necessary and scientifically grounded. Cogn. Technol. Work 2015;17(2):163–167

12. Klein G. Developing expertise in decision making. Think. Reason. 1997;3(4):337–352.

13. Gutzwiller RS, Fugate S, Sawyer BD, Hancock PA. The human factors of cyber network defense. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2015. pp.322–326.

14. Endsley MR. A systematic review and meta-analysis of direct objective measures of situation awareness: A comparison of SAGAT and SPAM. Hum. Fact. 2019.

15. Barford P, Dacier M, Dietterich TG, Fredrikson M, Giffin J, Jajodia S, Yen J. Cyber SA: Situational awareness for cyber defense. In Cyber Situational Awareness. Springer, Boston, MA; 2010. pp.3–14.

16. Giacobe NA, McNeese MD, Mancuso VF, Minotra D. Capturing human cognition in cyber-security simulations with NETS. In Proceedings of the IEEE ISI Conference. 2013. pp.284–288.

17. Malviya GA, Fink L, Sego, Endicott-Popovsky B. Situational awareness as a measure of performance in cyber security collaborative work. In Proceedings of the IEEE International Conference on Information Technology: New Generations. 2011. pp.937–942.

18. Stevens-Adams S, Carbajal A, Silva A, Nauer K, Anderson B, Reed T, Forsythe C. Enhanced training for cyber situational awareness. In Foundations of Augmented Cognition. Springer, Berlin; 2011, pp.90–99.

19. Zhang H, Maoyuan S, Yao D, North C. Visualizing traffic causality for analyzing network anomalies. In Proceedings of International Workshop on Security and Privacy Analytics (IWSPA'15). 2015. pp.37–42.

20. Gutzwiller RS. Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment through 2015. (No. TR-3184). NIWC Pacific San Diego United States. 2019.

21. Rajivan P, Cooke NJ. Information-pooling bias in collaborative security incident correlation analysis. Hum. Fact. 2018;60(5):626–639.

22. Endsley MR, O.Kiris E. The out-of-the-loop performance problem and level of control in automation. Hum. Fact. 1995;37(2):381–394.

23. Onnasch L, Wickens CD, Li H, Manzey D. Human performance consequences of stages and levels of automation: An integrated meta-analysis. Hum. Fact. 20145;56(3):476–488.

24. Endsley MR, Jones DG. Designing for situation awareness: An approach to human-centered design (2nd ed.). Taylor & Francis, London. 2012.

25. Trent S, Hoffman RR, Merritt D, Smith S. Modelling the cognitive work of Cyber Protection Teams. Cyber Defense Rev. 2019;4(1):125–135.

26. Mckenna S, Staheli D, Meyer M. Unlocking user-centered design methods for building cyber security visualizations. In Proceedings of the IEEE Symposium on Visualization for Cyber Security (VizSec'15). 2015. pp.1–8.

27. Staheli D, Yu T, Crouser R, Damodaran S, Nam K, O'Gwynn D, Harrison L. Visualization evaluation for cyber security: Trends and future directions. In Proceedings of the 11th Workshop on Visualization for Cyber Security, 2014. pp.49–56.

28. Erbacher RF, Frincke DA, Wong PC, Moody S, Fink G. 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, 2010. p.75300H.

29. Gutzwiller RS, Hunt SM, Lange DS. 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). 2016. pp.14–20.

30. Mahoney S, Roth E, Steinke K, Pfautz J, Wu C, Farry M. A cognitive task analysis for cyber situational awareness. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2010. pp.279–283.

31. Endsley MR. Situation awareness global assessment technique (SAGAT). In Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON'88). 1988. pp.789–795.

32. Taylor RM. Situational Awareness Rating Technique (SART): The Development of a Tool for Aircrew Systems Design. AGARD, Situational Awareness in Aerospace Operations, 1990. 17p.

33. Jones D. Subjective measures of situation awareness. In Situation awareness: Analysis and measurement, M. R. Endsley and D. Garland (Eds.). Lawrence Erlbaum Associates, Mahwah, NJ; 2000. pp.113–128.

34. Freund J, Jones J. Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, Oxford, UK. 2014.

35. Champion M, Jariwala S, Ward P, Cooke NJ. 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. 2014. pp.310–314.

36. D'Amico D, Whitley K.. 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. 2008.

37. Durso FT, Nickerson RS, Dumais S, Lewandowsky S, Perfect T. Handbook of Applied Cognition. John Wiley & Sons, West Sussex, 2007. pp.163–193.