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.*

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.