Elements of Cyber-Cognitive Situation Awareness in Organizations

Chanel Macabante, Sherry Wei, and David Schuster
San José State University

Introduction

- Advances in cybersecurity and the complexity of networks require approaches to measurement that consider elements of the sociotechnical system.
- Cyber-cognitive situation awareness (CCSA; Gutzwiller, Hunt, & Lange, 2016) is critical to the success of cyber defense. Cyber defense is abstract, collaborative, fast-paced, and continually evolving.

Cyber-Cognitive Situation Awareness (CCSA)

- As knowledge needed in the performance of a goal (Rosseau et al., 2004), cyber defenders must maintain CCSA in order to correctly identify and act on threat information.
- Gutzwiller, Hunt, and Lange found three major themes for CCSA: "The network, the world, and internal organization" (2016, p. 17).

New Contribution to CCSA

- Proposition 1: CCSA of the network includes knowledge of trustworthiness of information.
- Proposition 2: CCSA of the network includes knowledge of automation capabilities and performance.
- Proposition 3: CCSA of the world includes distinguishing between hits, false alarms, and benign abnormal activity.
- Proposition 4: CCSA of the team should be assessed at three levels: team member, team, and multiteam system.

SJSU SAN JOSÉ STATE UNIVERSITY

THEORY

We propose additions to cyber-cognitive situation awareness to better reflect new developments and the needs of organizations.

vectrlab.net

Measurement of CCSA

1. Is an alert from "x" trustworthy?
2. What information was considered by automated tool "x"?
3. Was the event "x" an alert, hit, false alarm, or benign abnormal activity?
4. Should you now escalate event "x" to team "y"?

Discussion

- Further development of CCSA and its measurement will help organizations better select and train individual cyber defenders.
- CCSA measurement will also allow diagnosis of gaps, helping organizations to assess training protocols to improve overall communication and team decision making.
- Both qualitative and quantitative research is needed to validate our propositions.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. (1553018). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. Poster layout adapted from Morrison (2019).

References

- Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016, 14–20.
- Rousseau, R., Tremblay, S., & Breton, R. (2004). Defining and modeling situation awareness: A critical review. In S. Banbury & S. Tremblay (Eds.), A Cognitive Approach to Situation Awareness: Theory and Application (pp. 3–21). Burlington, VT: Ashgate Publishing Company.

vectr lab @ sjsu