Evaluating Macrocognitive Awareness Training

Krish D. Pradhan, Chelsea M. Norton, Christal Chavarin, Tommy T. Tran, Hanan Mubarez, David Schuster
San José State University

Introduction

- Cybersecurity is critical, challenging, and in-demand cognitive work, but we are only starting to understand it.
- As technology continues to advance, so do the threats posed to it, highlighting the need to ensure that cybersecurity professionals are fully equipped with the proper skillset to meet these needs.
- We have previously argued that macrocognition can help us understand how cybersecurity professionals apply cognitive resources to their work (Schuster, in press).
- However, we are not yet at a point where we can develop interventions to improve macrocognition (Khan, Helzer, & Schuster, 2021).

Background

- Macrocognition is the collection of cognitive processes and functions that characterize how people think in natural settings (Klein et al., 2003).
- An awareness training for macrocognition was developed for cybersecurity professions. We hope to evaluate its effectiveness through observing changes in the attitudes, knowledge, and skills of cybersecurity professionals.

Macrocognition Function	Definitions Applied to Cybersecurity Context
Problem Detection	Defenders must be able to identify events that do not conform to a specific pattern. The ability to spot potential problems at an early stage is critical.
Adaptation	Defenders must have the ability to adapt to changes in an environment and deal with uncertainty in contexts of rapid change in threats and threat defense.
Sensemaking and Situation Assessment	Defenders need to make sense of their current situation and also how they predict future events will play out to prevent future attacks.

SJSU SAN JOSÉ STATE UNIVERSITY

Methods

We developed an **awareness training** to teach **cybersecurity professionals** about **cognition.**

vectrlab.net

Proposed Method

1. An IRB approved awareness training for macrocognition was developed for cybersecurity professions.
2. Participants will be given pretest measures and a demographics survey through Qualtrics, followed by a 30-minute training workshop.
3. Additionally, a follow-up questionnaire will be administered in an attempt to capture how our training has impacted cybersecurity professionals job performance.

Predictions

- Our study will provide initial evidence that the training can inform participants about the concept of macrocognition.
- The study will motivate defenders to apply their new knowledge towards their workplace to boost performance in cybersecurity.

References

Khan, H. A., Helzer, M. R., & Schuster, D. (2021, April 20 to 27). Training for macrocognitive skills awareness in cybersecurity professionals [Poster presentation]. Spartan Psychological Association Research Conference, San Jose, CA.

Schuster, D. (in press). Exploring cognitive processes to develop cybersecurity defender proficiency. Cybersecurity Skills Journal: 2020 Special Issue on the NICE Framework.

Klein, G., Ross, K. G., Moon, B. M., Klein, D. E., Hoffman, R. R., & Hollnagel, E. (2003). Macrocognition. IEEE Intelligent Systems, 18(3), 81–85. https://doi.org/10.1109/MIS.2003.1200735

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).

vectr lab