Intelligent tutoring system for cyber security with a trust management system component

Robert Arrabito, Ming Hou, Sebastian Fischmeister, Tiago Falk, Hannah Willoughby, Madison Cameron, Liam Foley, Sarah Normandin, and Simon Banbury

Abstract—The Royal Canadian Navy (RCN) strategic vision Cyber Strategy 2020-2025 requires that the RCN workforce is trained, educated and aware of cyber risks and their role in cyber security and defence [1]. To support the RCN vision, Defence Research and Development Canada (DRDC) – Toronto Research Centre recently commenced an investigation to research advanced training strategies for maintaining operational resilience against cyber attacks onboard His Majesty's Canada (HMC) platforms based on the identification of a corpus of human-noticeable aspects of cyber attacks. This paper presents training strategies that are based on emerging artificial intelligence (AI) technologies for teaching cyber security to RCN operators to support cyber damage control on future HMC platforms. We promote that AI systems can achieve state-of-the-art results for cyber security training.

We began our investigation by interviewing six Department of National Defence/Canadian Armed Forces subject matter experts (SMEs) with substantial experience in cyber damage control on how to identify potential cyber security risks, and mitigations strategies to detect, respond, and recover from cyber security incidents onboard HMC platforms [2]. Cyber awareness training for all RCN ranks was identified by the SMEs as the biggest mitigator to improve operator awareness of compromised platform systems such as the Integrated Platform Management System or the Combat Management System.

One means of future instruction for the RCN is the design and development of an Intelligent Tutoring System (ITS) [3, 4]. Traditional ITS uses static instructional training in cyber security education, which is not able to meet the evolving landscape of cyber threats across a wide student population. New ITS will need to employ adaptive learning for individuals with different backgrounds to improve the student learning experience [5, 6].

Combating cyber threats also requires trust in Information Technology (IT) as it relates to cyber damage control. As a potential additional component of an ITS, a Trust Management System (TMS) needs to be implemented to help build, maintain, and repair operator trust in IT. The TMS will identify when trust in the system is lost using psychophysiological-based techniques (e.g., eye tracking, electroencephalography, heart rate variability, and galvanic skin response) to detect whether an operator is aware of ongoing human-noticeable aspects of cyber attacks. In addition, various sensor-based intrusion detection methods (e.g., host-based detectors) can submit an alert to notify the TMS of a cyber security breach. If trust is lost, the TMS will instruct the system how to adapt its behaviour in an attempt to repair and restore the operator's trust in it using a model of operator trust that is being developed at DRDC [7, 8]. In case of a loss of trust, the system or operator can restore the system to an approved state. Communication between the TMS and the operator will be through a graphical user interface of the ITS. The operator can use a checklist and ITS to learn more before initiating the restore process.

References

[1] Department of National Defence, "Royal Canadian Navy cyber strategy 2020-2025 / RDIMS#436259," Ottawa: Director of Naval Information Warfare, 2019.

[2] S. Fischmeister, T. Falk, H. Willoughby, M. Cameron, L. Foley, et al., "A scoping study of suitable training systems for operational resilience against cyber-attacks," Defence Research and Development Canada, unpublished.

[3] M. Hou, S. Banbury, and C. Burns, *Intelligent Adaptive Systems – An Interaction-Centered Design Perspective*. Boca Raton, FL: CRC Press, 2014.

[4] M. Hou and C. M. Fidopiastis, "A generic framework of intelligent adaptive learning systems: From learning effectiveness to training transfer," *Theoretical Issues of Ergonomics Science*, vol. 18, pp. 167–183, 2016.

[5] P. Seda, J. Vykopal, J. Čeleda, and I. Ignác, "Designing adaptive cybersecurity hands-on training," *IEEE Frontiers in Education Conference*, pp. 1–8, 2022.

[6] M. Sette, L. Tao, K. Gai, and N. Jiang, "A semantic approach to intelligent and personal tutoring system," *IEEE 3rd International Conference on Cyber Security and Cloud Computing*, 2016.

[7] M. Hou, G. Ho, D. Dunwoody, "IMPACTS: A trust model for human-autonomy teaming, Journal of Human-Intelligent Systems Integration," *Special Issue on Human-Autonomy Teaming in Military Context*, vol. 3, pp. 79–97, 2021.

Robert Arrabito is with the Human Effectiveness Section, Defence Research and Development Canada, Toronto, ON M3K 2C9 Canada (phone: 416-635-2033; fax: 416-391-6388; e-mail: robert.arrabito@drdc-rddc.gc.ca).

Ming Hou is with the Human Effectiveness Section, Defence Research and Development Canada, Toronto, ON M3K 2C9 Canada (e-mail: ming.hou@drdc.drdc.gc.ca).

Sebastian Fischmeister is with the Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON N2L 3G1 Canada (e-mail: sfischme@uwaterloo.ca).

Tiago Falk is with the Centre for Energy, Materials and Telecommunications, Institut national de la recherche scientifique, Montreal, QC, H5A 1K8, Canada (e-mail: tiago.falk@inrs.ca).

Hannah Willoughby is with C3 Human Factors, Québec City, QC G1V 0B9 Canada (e-mail: hannah.willoughby@c3hf.com).

Madison Cameron is with C3 Human Factors, Québec City, QC G1V 0B9 Canada (e-mail: madison.cameron@c3hf.com).

Liam Foley is with C3 Human Factors, Québec City, QC G1V 0B9 Canada (e-mail: liam.foley@c3hf.com).

Sarah Normandin is with C3 Human Factors, Québec City, QC G1V 0B9 Canada (e-mail: sarah.normadin@c3hf.com).

Simon Banbury is with C3 Human Factors, Québec City, QC G1V 0B9 Canada (e-mail: simon.banbury@c3hf.com).

[8] M. Hou, Y. Wang, L. Trajkovic, K. N. Plataniotis, S. Kwong et al., “Frontiers of brain-inspired autonomous systems: How does the defence R&D drive innovations?,” *IEEE Systems, Man, and Cybernetics Magazine*, vol. 8, 8–20.