**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**


