Socio-technical cybersecurity educational development for waterway and maritime OT personnel

Summary

Tallinn University of Technology, Estonian Maritime Academy offers two (2) 4-year PhD position in information and communication technology. As a candidate with a combined background in IT and education, you will have the opportunity to work in a collaborative and multidisciplinary research environment across several nations (Estonia, Norway, Netherlands).

Research field:	Information and communication technology
Supervisors:	Ricardo Gregorio Lugo
	Tiia Sõmer
Availability:	This position is available.
Offered by:	Tallinn University of Technology
	Estonian Maritime Academy
Application deadline:	Applications are accepted between October 02, 2023 00:00 and October 23, 2023 23:59 (Europe/Zurich)

Description

Abstract

The EU aims to strengthen cyber resilience, especially in critical infrastructure (CI). The backbone of CI is operational technology (OT or industrial automation). With regulations, the EU focusses on what to do. Organisations like ENISA publish supporting information on how to act.

Many EU initiatives have addressed that the human factor plays a major role when filling the competence gap in public administrations / SME in the implementation cybersecurity in general. For CI in the water sector, the challenge is especially demanding: Public water utilities are often operated in traditional working routines. Public institutions and SMEs are closely intertwined in this sector, resulting in private and public employees being equally integrated in the procedures and would therefore be equally responsible for counteraction in the case of cyberattacks. The competence level required comprises all operational levels, from management to all levels of service provision. In addition, climate change is underlining the relevance of this sector. Facing the upcoming mandate of the NIS(2) directive to ensure sufficient cybersecurity training the urgency calls for integrated and fast action.

Description

The primary objective of this research is to develop and Improve cybersecurity protection readiness of the water sector by developing educational and training approaches that will contribute to the ENISA's portfolio through up-to-date cybersecurity competence trainings in the water sector and increase the competence level of people working with OT (SME / public employees) to:

- understand cyber risk enabling them to act. This is done by applying innovative technologies in combination with OT user centric content
- develop, pilot and roll out an innovative approach to improving cybersecurity competences thereby using proven techniques and anchoring innovative tools along the entire chain of execution in the water sector. ATHENA will strive for an increase of maturity in cybersecurity capacities of both SME and public administrations
- taking up market-ready solutions to tackle the challenge of the human factor and to deploy custom-fit training for both SME and public employees in the water sector across the entire chain of execution
- securing accessibility to the trainings through embedding of core content to open platforms on EU and MS level (e.g. ENISA, Cyberagentur in DE, etc.).

Responsibilities and (foreseen) tasks:

- Conduct research on the development educational technologies for delivering cybersecurity training
- Design evidence-based evaluation approaches for developed cybersecurity learning technologies
- Collaborate with other researchers and industry partners to develop new applications for educating cybersecurity

- Write scientific publications and present research findings at conferences and meetings
- Participate in departmental activities, such as seminars and workshops
- Supervise students (master's, bachelor's)

Applicants should fulfil the following requirements:

- a master's degree in education or information technologies, computer science, human-factors or related fields
- the candidate has a high academic level
- a clear interest in the topic of the position
- programming skills
- excellent command of English
- strong and demonstrable writing and analytical skills
- capacity to work both as an independent researcher and as part of an international team
- capacity and willingness to provide assistance in organizational tasks relevant to the project

The following experience is beneficial:

- Experience with IT and educational development
- Working knowledge of qualitative and quantitative data analysis

We offer:

- A fully paid 4-year PhD position. The chance to do high-level research in a multidisciplinary team (psychologists, IT & OT engineers)
- Opportunities for conference visits, research stays, and networking

About the department

The Centre for Maritime Cybersecurity is a research centre with a primary focus on advancing cybersecurity in the maritime industry. The Centre was founded though the MariCybERA project (Horizon 2020 ERA Chair) to establish the Centre in response to the increasing cyber threat in the maritime sector. The Centre was established in collaboration of two units of the Tallinn University of Technology: The Centre of Digital Forensics and Cyber Security, and the Estonian Maritime Academy. The goal is to provide a platform for the development of cutting-edge cybersecurity solutions for the maritime industry, as well as to raise awareness about the importance of the cybersecurity of the maritime sector, and at the same time attract young people to the field.

Estonian Maritime Academy, a structural unit of Tallinn University of Technology, provides multi-level education and does professional research in marine sciences and fields related to them, making it the only competence centre of its kind in Estonia.

The mission of the Centre for Maritime Cybersecurity at Tallinn University of Technology is to advance internationally and nationally relevant state of the art in research and apply it in bachelor, MSc and doctoral education in the areas of maritime cybersecurity with the goal to solve problems the society is facing and support sustainable development. For further information, please contact Dr. Ricardo G. Lugo (Ricardo.Lugo@taltech.ee)

To get more information or to apply online, visit https://taltech.glowbase.com/positions/694 or scan the the code on the left with your smartphone.