Cyber Ranges to XR (CRXR): Shaping the Future of Cybersecurity Training

Overview

Both network simulation and extended reality fields use the word ‘Virtual’ but with a different meaning, from Virtualization of computer architectures and networks to immersion into a 3D digital world.

Both these approaches are used for training to cybersecurity, but for different purposes.

This workshop aims at discussing how the network simulation and XR domains could intricate to enhance training in cybersecurity. Human factor approach as a promising link between them will be considered. For example, terms from cognitive sciences as immersion, presence and situational awareness in the context of strategic and technical cybersecurity virtual training could be discussed.

Today, cybersecurity training and education, encompassing all aspects from incident to crisis management in response to cyber threats, has shifted from a predominantly military focus to a critical need across public and private organizations of all sectors, sizes, and structures. Over the past decade, various training modalities—including virtual reality, simulation-based training, and augmented reality—have been tailored to build competencies in cyber defence and crisis management. The exploration of these approaches has become fertile ground for interdisciplinary research, yet the rapid expansion of studies in this emerging field, often following distinct paths, presents challenges in consolidating the current knowledge base.

These training modalities are rooted in immersive learning, which draws on experiential learning principles. Key factors in this context such as presence (the sense of "being there"), objective fidelity (physical and functional), and subjective fidelity (sensory and emotional)—play essential roles in supporting knowledge acquisition and retention. Additionally, situational awareness and cognitive effort contribute significantly to the effectiveness of experiential learning in cybersecurity training. Nevertheless, a crucial question remains: how do these factors differ in influencing competency development, knowledge acquisition, and retention when applied across various training modalities? or How the VR & cybersecurity concepts could intricate, as these domains use virtual environments for training, but those environments are totally different ?

For this reason, this workshop target to explore, discuss, and understand the integration of human factors in designing diverse immersive cybersecurity training programs. Specifically, it seeks to study convergence and divergence across different training modalities, ranging from hybrid approaches—such as cyber ranges and augmented reality—to fully virtual environments, such as those enabled by virtual reality.

Website: https://alexkabil.github.io/CVT_IEEEVR25/

Workshop topics

- Cybersecurity
- XR
- Human Factors
- Crisis management
- Network simulation
- Virtual Training

Submission Guidelines

Submit a 2 pages paper that will be reviewed in order to allow you to present:

- Use cases regarding training in cybersecurity from a network simulation perspective
- Uses cases about Virtual Environment for Training that could be applied to cybersecurity domain
- Position paper about the increasing importance of human factors for cybersecurity training

Please send your paper proposal by email to alexandre.kabil@cnrs.fr following the IEEE Computer Society VGTC conference format available at https://tc.computer.org/vgtc/publications/conference/

Workshop planning

1. Workshop introduction
2. Keynote
3. Presentations of accepted submissions
4. Round table about the workshop's topics

Important dates

- November 18, 2024: Call for papers opening
- January 16, 2025: Call for papers ending
- February 16, 2025: Authors notification of acceptance
- March 8-9, 2025: Workshops (held on the first two days of the conference)

Workshop Organizers

Alexandre KABIL *alexandre.kabil@cnrs.fr*

- XR research engineer, project manager of the French infrastructure CONTINUUM – network of XR, HCI and Data analysis research platforms - and member of the Ex)Situ research team hosted by the LISN (UMR9015) laboratory

Marc PARENTHOEN

- Associate professor (PhD) at Université de Poitiers, XLIM UMR CNRS 7252, head of the RéSISTeCC project about small entities resilience to cyber risks, head of the MRSI master's degree (risk management & cybersecurity)

Jose Manuel Castillo PIMENTEL

- Postdoc at CeRCA UMR CNRS 7285. PhD at LAPCOS (2022). His research is about cognitive ergonomics applied to cyber crisis immersive training.

Marc Oliver PAHL

- Marc-Oliver Pahl is a full professor for cybersecurity at IMT Atlantique, a French Grand École. There he leads the largest industrial chair for cybersecurity in France, the chair Cybersecurity for Critical National Infrastructures (https://cyberCNI.fr).

  Marc-Oliver is president of the German chapter of the Association for Computing Machinery (ACM) (germany.acm.org) and member of the executive committee of the German Informatics Society (gi.de). He is also a steering committee member of the German-French Academy for the Industry of the Future (future-industry.org).

  Marc-Oliver's research targets a holistic approach to cybersecurity with an emphasis on collaborative approaches, including practical applications of federated learning and blockchain, novel side-channel based anomaly detection as well as VR -based cybersecurity interfaces.

  He is an experienced teacher and an eLearning pioneer who has received diverse teaching awards. He continuously organises events for larger audiences, such as the TALK.CYBERcni.fr Speaker Series and the future-iot.org PhD School Series.

Nicolas LOUVETON

- Associate professor (HdR) in cognitive ergonomics at Université de Poitiers, CeRCA UMR CNRS 7295, head of the Web editorial and UX strategy master’s degree (cognitive ergonomics).