IEEE CSR 2022
Cyber Security and Resilience
Virtual Conference | July 27–29, 2022
https://www.ieee-csr.org

2022 IEEE CSR Workshop on Cyber Ranges and Security Training (CRST)

Call for Papers

Important dates

Workshop papers' deadline:
~~April 22~~ May 20, 2022
Workshop authors' notification:
~~May 13~~ June 10, 2022
Camera-ready submission:
~~May 27~~ June 24, 2022
Early registration deadline:
June 24, 2022
Workshop's date:
July 27–29, 2022

Workshop chairs

Theodora Tsikrika
Angelos Amditis
George Kokkinis
Dimitrios Kavallieros

Organizing committee

Xavier Bellekens
Eleftherios Ouzounoglou
Egidija Versinskiene
Sotiris Ioannidis
Stefanos Vrohidis
Eleni Darra

Publicity chairs

Damir Haskovic

Contact us

dim.kavallieros@iti.gr

Cyber-attacks are increasing in both sophistication and scale, revealing the extent at which critical infrastructures and other information and communication systems are exposed. More highly skilled cyber security professionals are needed with a deep understanding of cyber-security to deal with the fast growing number of cyber-threats. Cyber-security education and training are becoming more and more relevant as it is the only way in which such incidents can be prevented and handled adequately. A cyber-range (CR) is the environment in which cyber-security experts and professionals can practice technical and soft skills and be trained —in an isolated virtual environment emulating large-scale complex networks— on how to respond to cyber-attack scenarios within various domains. The more realistic the simulated scenarios, the more prepared the trainees will be to face real-world attacks. The cyber-space offered by the CR infrastructure recreates the experience of responding to a cyber-attack, by replicating a security operations center environment, an organization's network and the attack itself. CRs are considered to be the key towards strengthening the robustness and security of critical infrastructures. This area requires further advancements: the generated scenarios are tightly coupled with the domain being modelled, scalable to an organization's infrastructure or software needs and likewise easily extendable to acquire knowledge regarding newly discovered vulnerabilities, threats and attackers' tactics, techniques, and procedures.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Cyber range integration and federation
- Emulation and simulation techniques (Exercises, Architecture, etc.)
- Hybrid system integration
- Emerging technologies in cyber ranges
- Econometric models in cyber security training
- Risk assessment frameworks for training
- Trainee evaluation and situational awareness
- Learning methods in cyber security training certifications
- Serious gaming and visualization
- Cyber-exercises and strategic decision making

This workshop focuses on both research and practical aspects of cyber ranges and aims at addressing the main challenges involved in their development and use in professional cyber security training, as well as in exploring the use of emerging technologies. Aligned with the interdisciplinary nature of cyber security, authors from academia, industry, and government are welcome to contribute.

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. The workshop's proceedings will be published by IEEE and will be included in IEEE Xplore. Detailed information about the paper submission and guidelines to authors can be found at the workshop's website https://www.ieee-csr.org/crst.

Supported by

FORESIGHT
CyberMAR
SPARTA
CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion
ECHO
SECANT

IEEE
IEEE SMC Systems, Man, and Cybernetics Society
SMC Homeland Security Technical Committee
LOGOS RI RESEARCH&INNOVATION