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

Nicholas J. Multari
Rosalie McQuaid

Organizing committee

Nicholas J. Multari
Rosalie McQuaid
George Sharkov
Volkmar Lotz
Elena Peterson
Jeffrey Picciotto

Publicity chairs

Elena Peterson
Jeffrey Picciotto

Contact us

nick.multari@pnnl.gov
rmcquaid@mitre.org

The CRE 2022 Workshop, focusing on Cyber Resiliency: Strategies, Technologies, and Economics, will continue the exploration of foundational and applied advances in cyber resiliency strategies, policies, and technologies to shift the asymmetric balance in favor of the defender and identify and quantify the effect economic realities have on the decision processes. At the top level, national and organizational strategies and policies are required to understand what is to be achieved and the resources to be made available to protect critical resources and infrastructures. These strategies and policies must be supported by security and resiliency technologies. As a result, in addition to exploring various strategies, the workshop will seek to understand the capabilities, strengths/weaknesses, and benefits of various resiliency technologies whether existing or in research.

The workshop will examine the parameters needed to accurately quantify asymmetric imbalance from both the offensive and defensive perspective; examine technical and non-technical approaches to shifting that balance, including the full range of costs/benefits of each approach; and explore and evaluate a range of options for defining and achieving optimality. It will bring together a diverse group of experts from multiple fields to advance the above concepts.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- National and organizational cyber resiliency strategies and policies related to the development, deployment and use of cyber resiliency technologies.
- Existing IT/OT (and their interfaces) to achieve cyber resilience of CPS environments.
- Research activities in cyber resilience focused on IT and OT solutions, alignment of technical and mission resiliency, and preemptive resilience.
- Benefits and weaknesses of cyber resiliency technologies in CPS environments.
- Metrics, measurements, and economics of cyber resiliency & asymmetry.
- Technical and Economic barriers to the implementation of cyber resiliency technologies.
- Defining practical cyber resiliency and potential use cases and case studies.
- Relationship between resiliency and security in protecting CPS environments.
- Adversary and defender economics: assessing the impact of defender capabilities and actions to the attacker and vice versa.
- Frameworks for ROI analysis (cost, risk, benefit) to guide technology investment (research, development, and utilization).

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/cre.

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