
# Call for Papers

## Important dates

Paper submission deadline:
**June 3, 2024 AoE**
Authors' notification:
**July 3, 2024 AoE**
Camera-ready submission:
**July 14, 2024 AoE**
Early registration deadline:
**July 20, 2024 AoE**
Workshop dates:
**September 2–4, 2024**

## Workshop chairs

Nicholas J. Multari (US)
Rosalie McQuaid (US)

## Organizing committee

George Sharkov (BG)
Volkmar Lotz (FR)
Elena Peterson (US)
Kelly McSweeney (US)

## Technical program committee

Michael Atighetchi (US)
Michael Bailey (US)
Tom Carroll (US)
Yung Ryn Choe (US)
Fabio De Gaspari (IT)
Herve Debar (FR)
Erich Devendorf (US)
Sabrina D.C. Di Vimercati (IT)
Kevin Driscoll (US)
Ilir Gashi (UK)
Doug Jacobson (US)
Dong Seong Kim (AU)
Nuno Neves (PT)
Karthik Pattabriraman (CA)
Craig Rieger (US)
Luigi Romano (IT)
Meghan Sahakian (US)
Reginald Sawilla (CA)
O Sami Saydjari (US)
Neeraj Suri (UK)
Marco Vieira (US)
Chris Walter (US)

## Publicity chairs

Elena Peterson (US)
Kelly McSweeney (US)

## Contact us

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

The IEEE CSR CRE workshop explores the foundational and applied advances in cyber resiliency strategies, policies, and technologies to shift the balance in favor of the defender, ensure critical processes continue to operate in face of a successful cyber-attack, and identify and quantify the effect economic realities have on the decision processes. At the top level, national and organizational strategies and policies are needed to understand what is to be achieved and the resources to be made available to protect critical resources and infrastructures. 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 technologies whether existing or in research. This includes the incorporation of new technologies that are not resilience-focused but still have significant impact on a system's ability to continue to operate in face of attack. Such examples include artificial intelligence and machine learning that can be used by defenders and attackers to impact the asymmetric balance.

The workshop focuses on the parameters needed to accurately quantify asymmetric imbalance from 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; 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.

The workshop is held in conjunction with the IEEE CSR 2024 conference as a **hybrid event**, during September 2–4, 2024. 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 on the development, deployment, and the 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/OT solutions, alignment of technical & mission resiliency and preemptive resilience
- Benefits and weaknesses of cyber resiliency technologies in CPS environments
- Metrics, measurements, and economics of cyber resiliency and 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)

The IEEE CSR CRE workshop will accept high-quality research papers presenting strong theoretical contributions, applied research and innovation results obtained from funded cyber-security and resilience projects, and industrial papers that promote contributions on technology development and contemporary implementations.

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. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for 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