Important dates

Paper submission deadline:
March 15, 2023
Authors' notification:
April 01, 2023
Camera-ready submission:
April 15, 2023
Early registration deadline:
May 5, 2023

Workshop Co-Chairs

Nicholas J. Multari
Rosalie McQuaid

Organizing Committee

Nicholas J. Multari
Volkmar Lotz
Elena Peterson
Rosalie McQuaid
George Sharkov
Paul Rowe

Technical Committee

Michael Atighetchi
Thomas Carroll
Andrea Ceccarelli
Yung Ryn Choe
Herve Debar
Sabrina De Capitani di Vimercati
Erich Devendorf
Meghan Galiardi
Arlette Hart
Gernot Heiser
Doug Jacobson
Dong Seong Kim
Volkmar Lotz
Henrique Madeira

Call for Papers

IEEE Workshop on Cyber Resilience and Economics (CRE)
Cyber Resiliency: Strategies, Technologies, and Economics

Scope

A combination of cyber technological feasibility and economic viability drives many of the decisions related to cybersecurity and cyber resiliency by both the defenders and attackers. In this context, technological feasibility is defined as any cyber resiliency technology that has the potential to be developed, fielded, and operationally controlled. In the case of economic viability, the resources required to defend, or attack must be available. We define resources in its broadest sense to include but not limited to the people, equipment, training, required funding, and asset value. On the defensive side, these technological and economic factors determine the cyber security and resiliency policies, procedures and technologies implemented to prevent and respond to cyber-attacks. On the offensive side, they not only determine the type of attack but also the effort expended to ensure its success. In short, these and other factors determine the asymmetric balance between the attackers and defenders.

The CRE23 Workshop 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.

This proposed workshop directly complements the conference's objectives by serving to accelerate the recognition, adoption and application of cyber resilience of critical resources and infrastructures within industry, government and academia by addressing the key concerns of how these techniques and technologies can be realized within the practical constraints of cost, risk, and benefit.

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

Luigi Mancini

Al Mok

Takashi Nanya

Nuno Neves

Rui Oliveira

Mohammad Rahman

Indrajit Ray

Craig Rieger

Luigi Romano

O. Sami Saydjari

Nabil Schear

Neeraj Suri

Reginald Sawilla

Contact us

Nicholas J. Multari,

Email: Nick.multari@pnnl.gov

Rosalie McQuaid,

Email: rmcquaid@mitre.org

Topics of Interest

The topics of interest include, but are not limited to:

- 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
- 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)

IEEE

IEEE SMC Systems, Man, and Cybernetics Society

IEEE SMC Technical Committee on Homeland Security

LOGOS RI RESEARCH&INNOVATION