Call for Papers

5TH Annual International CRE Workshop: Cyber Resiliency: Technologies, Economics and Strategy

This proposed workshop will be co-located with the 2020 IEEE International Conference on Software Quality, Reliability, and Security (https://qrs20.techconf.org/), in Macau, China, December 11-14, 2020.

A combination of cyber technological feasibility and economic viability drives many of the decisions related to cybersecurity 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 CRE20 Workshop on Cyber Resiliency: Technologies, Economics and Strategy will explore 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. These strategies and policies must be support 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 will serve to accelerate the recognition, adoption and application of cyber resilience 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.

We are currently seeking manuscripts for a full-day workshop that will be a forum to discuss recent research in areas associated with cyber resilience strategy, technologies and economics. Manuscripts should be submitted in the IEEE standard conference format of 8 pages maximum in the specific topics of interest to include, but not limited to:

- National and organizational cyber resiliency strategies and policies related to the development, deployment and use of cyber resiliency technologies
- Existing technologies to achieve cyber resilience
- Research activities in cyber resilience
- Benefits and weaknesses of cyber resiliency technologies
- Foundations of asymmetric cyber advantage
- Integrated analyses of cyber resiliency & asymmetry within cyber environments
- Metrics, measurements, and economics of cyber resiliency & asymmetry
- Barriers to the implementation of cyber resiliency technologies
- Defining practical cyber resiliency
- Technical & architectural approaches to gaining asymmetric advantage
- Relationship between resiliency and security
- Adversary economics: assessing the impact of defender capabilities and actions to the attacker
- Frameworks for ROI analysis (cost, risk, benefit) to guide technology investment (research, development, and utilization)
- Cyber-resiliency related tools that are guided by economic factors for defender and/or adversary
- Use cases or case studies for defender and/or adversary that include economic factors

In light of the interactions and interdependencies of today's cyber infrastructures, the scope of this workshop is to explore the above topics across the full spectrum of cyber systems to include traditional IT, cloud platforms, cyber-physical systems, Internet of Things, operational technologies, and critical infrastructure.

Chairs:
Nick Multari (PNNL) nick.multari@pnnl.gov
Jeffrey Picciotto (MITRE) jp@mitre.org

Steering Committee:
Christopher Oehmen (PNNL) chris.oehmen@pnnl.gov
Rosalie McQuaid (MITRE) rmcquaid@mitre.org

Key Dates:
Manuscripts Due: June 15, 2020
(see https://qrs20.techconf.org/workshops/cre)
Author Notification: July 10, 2020