Resilience Analytics for Infrastructure under Compounding Threats: Methodology and Case Studies

Igor Linkov (igor.linkov@usace.army.mil), Emily Wells, Kelsey Stoddard, Munik Shreshta, Andrew Streltzoff, and Benjamin D. Trump
(US Army Engineer Research and Development Center, US Army Corps of Engineers, Vicksburg, MS)

Background/Objectives. Multiple threat events including compounding and/or cascading threats may disrupt critical infrastructure functioning. Infrastructure protection is likely to be failing with increased frequency resulting in severe economic losses. This is amplified by economic drives that have resulted in optimizing infrastructure design and management to be lean and efficient and thus prone to systemic disruptions. Approaches are needed that strengthen on system properties, especially resilience to reinforce the ability of a system to absorb, recover from, and adapt to a vast possibility of threats.

Approach/Activities. It is currently unclear how diverse yet interconnected critical infrastructure systems have approached resilience under compounding and cascading threat spaces. We model critical infrastructure as an interconnect network of physical, cyber and social domains where response to compounding threats is modeled through disruptions in nodes and links within each network as well as connectivity across multiple networks. The model incorporates the technical, social, and governance-related factors necessary for systems-level resilience over four temporal phases: preparation, absorption, recovery, and adaptation. Methodologically, calculations are done in tiers of increasing complexity: from qualitative and semi-quantitative metrics based approaches utilizing decision analytics and basic statistics to complex machine learning/AI approaches connected with network science. We illustrate the application of approach in the cases of natural disasters and zoonoses to highlight climate-related disrupters on the economy.

Results/Lessons Learned. Given the increasing interconnectivity and interdependencies within critical infrastructure systems across modern society, it is imperative that critical infrastructure systems consider technical and social disruption associated with cascading and compounding threats and hazards. We discuss two case studies: transportation system in CA where we study supply chain issues in port and freight networks as well as cyber/energy systems at military installations. The results indicate a need to focus on critical infrastructure absorption of compounding and/or cascading threats, particularly within the physical and information resilience domains. We conclude with an urgent call to use systems-based approaches with resilience at its core to deal with environmental stressors and disruptions of the economy.