

Approaches to Quantify Cyber Risk and Resilience

Igor Linkov, Alexander Ganin, Benjamin D. Trump, Kelsey Poinsatte-Jones

- 1 US Army Corps of Engineers, Engineering Research and Development Center, Virginia Road, Concord, MA 01742. Phone: (617) 233-9869
Email: Igor.Linkov@usace.army.mil; aag2k@virginia.edu;
benjamin.d.trump@usace.army.mil; Kelsey.M.Poinsatte-Jones@usace.army.mil

Cybersecurity is an increasingly popular term used to define the actions taken by individuals, businesses, and governments to protect their digital infrastructure from deliberate external attacks. In such events, nefarious computer hackers seek to exploit one or several computing vulnerabilities in order to steal private and secured information, disrupt existing processes handled by software, or to usurp control of a system from a remote location. Experts are required to keep up with the constant cybersecurity innovations in order to best prepare for potential cyber-attacks. Where government and industry installations may receive hundreds to thousands of hostile cyber-attacks each day, resilience thinking is crucial.

Traditionally, cyber threats are approached from the position of risk analysis. For the context of cybersecurity, risk analysis is focused on the evaluation of threats (e.g., deliberate cyber-attacks) that exploit system vulnerabilities that result in economic or political consequences. Risk is the product of various hazards, vulnerabilities, and consequences, whereby risk analysts seek to gain a measure of the damage that could be incurred by a given threat alongside its relative likelihood of occurrence. These efforts are well described in literature for routine and well characterized threats, yet generally rely upon robust sources of quantitative data to populate an assessment. Unfortunately, cybersecurity threats exploit increasingly complex information systems and technology networks in a manner that is rarely predictable and is difficult to quantify. As such, traditional risk assessment may not be able to address cybersecurity concerns in the near term.

Resilience analysis can serve as a complementary approach to explore threats that *are* inherently complex in nature, and are difficult to predict or characterize. Resilience practitioners adopt a systems-view of threat, where emphasis is placed upon reviewing a system's dynamical properties, such as robustness, recoverability, and adaptability, for a wide range of potential threats. Where resilience would allow users to review system absorption *and* recovery for cyber threats, we use two methods to operationalize resilience in various contexts. This includes (i) resilience matrices, and (ii) network science. For the former, a resilience matrix utilizes a decision analytical approach to integrate disparate sources of qualitative and semi-quantitative information to assess system performance across multiple domains, including physical, information, and social. For the latter, network science quantitatively assess a system's topology and interdependencies, where a failure could trigger cascading failures in other connected components of the system. Such approaches can help identify, in real time, the best available options to mitigate damage from cyber threats, as well as identify those alternatives available to reduce the time, money, and manpower needed to recover from such threats.

Thus, resilience analysis can be used to not only identify and reduce vulnerabilities of individual components but also to return systems back to original functionality and adaptation following an

adverse event. While risk assessment is a useful tool to identify and characterize known, quantifiable system threats, resilience analysis is useful for the preparation, absorption, recovery, and adaptation of infrastructural, social, and informational systems against unknown, uncharacterized, low-probability events. Given the complementary nature of these two approaches and complexity of cyber threats, resilience analysis and risk assessment must be adopted as dual forms to support management of cyber threats.