Cyber resilience metrics needed to meet increased threats

November 25 2013

Cyber threats are rapidly emerging as one of the primary security concerns for the nation and global community as targeted cyber attacks can cause severe consequences to critical infrastructure and sectors of the economy. Recent calls for action, including President Obama's Executive Orders 13636 and Presidential Policy Directive 21, have brought the concept of "resilience" in the face of cyber attacks to the forefront of the nation's consciousness. In a recent special issue of Springer's journal *Environment Systems & Decisions*, Dr. Igor Linkov and colleagues describe a framework for understanding the concept of cyber resilience, and lay out a systematic method by which to generate resilience metrics for cyber systems.

Resilience is the capacity of a system to withstand and recover quickly from both known and unknown threats. The study describes that managing for resilience has been difficult because the concepts of resilience and risk have been conflated and have tended to focus on narrowly defined system components or on specific networks. However, the definition of cyber systems must be expanded to include rich and varied physical, information, cognitive and social networks – or "domains" – that form an integrated whole. Thus, the discussion of resilience should recognize the role of cross-domain communication before, during and after adverse events such as cyber attacks or natural events that may disrupt the functionality of cyber systems.

The study suggests combining the military concept of network-centric operations and the US National Academies' definition of resilience

response stages to quantify and manage the resilience of a cyber system. Together, these factors form a matrix wherein a system's resilience may be quantified using tools of multi-criteria decision.

Regarding cyber resilience, the study describes, "Transition from risk-based approaches focusing on identifying individual vulnerability and fixing them one-at-a-time, to building a whole system for resilience, is required to deal with interconnected global risks and sophisticated adversaries. The resilience matrix approach is just the first step in the process which will lead us to formulating and quantifying resilience as a network property of the system."

More information: Linkov I. et al [add the other authors?] (2013). Resilience Metrics for Cyber Systems, Environment Systems & Decisions, DOI: 10.1007/s10669-013-9485-y

Provided by Springer