Resilience Metrics for Cyber Systems

Igor Linkov[1], Daniel A. Eisenberg[2], Kenton Plourde[1], Thomas P. Seager[2], Julia Allen[3], Alex Kott[4]

[1] US Army Engineer Research & Development Center, [2] Arizona State University, [3] Carnegie Mellon Software Engineering Institute, [4] Army Research Laboratory

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

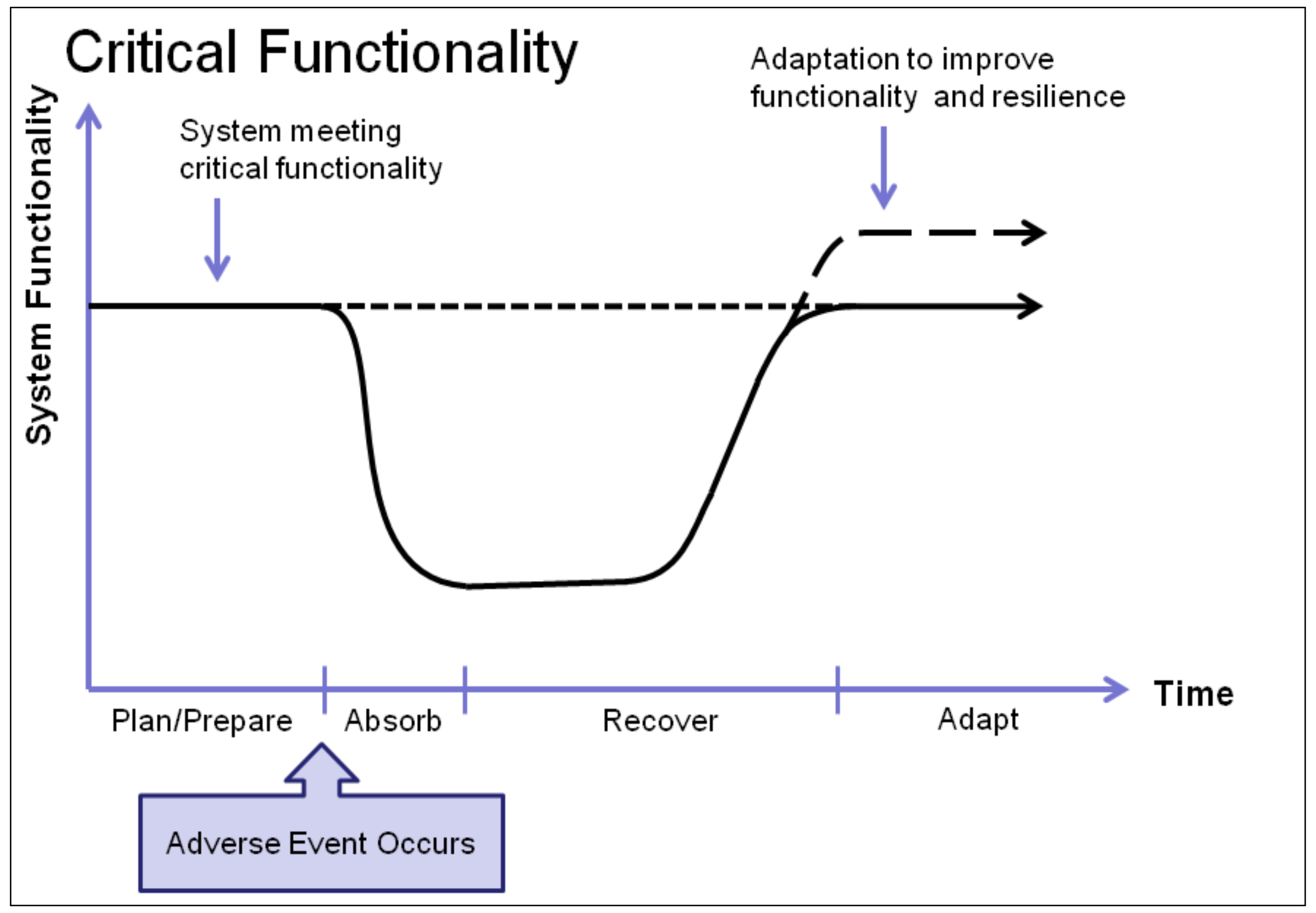
Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

As federal agencies and businesses rely more on cyber infrastructure, they are increasingly vulnerable to cyber attacks that can cause damages disproportionate to the sophistication and cost to launch the attack. In response, regulatory authorities call for focusing attention on enhancing infrastructure resilience. Despite the national and international importance, resilience metrics to inform management decisions are still in the early stages of development. There is a need for a generic approach that could integrate actual data, technical judgment, and literature-based measures to assess resilience across physical, information, cognitive, and social domains.

What is Resilience?

RESILIENCE is the capability of a system (e.g., infrastructure, biological) to return to normal function after an adverse event.



Components of Resilience

The Event Management Cycle

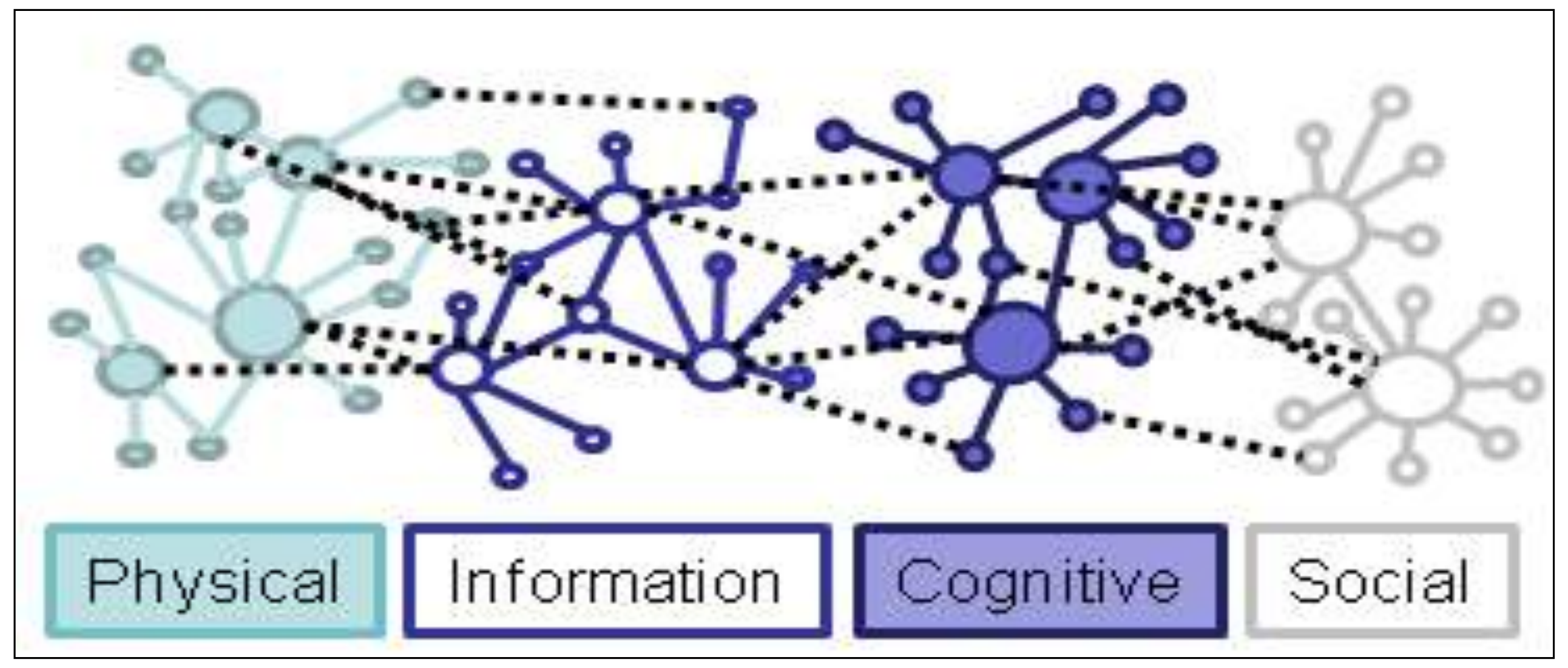
The National Academy of Sciences (NAS) identifies four stages of the event management cycle that a system needs to maintain to be resilient:

- **Plan/Prepare:** Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack)
- **Absorb:** Maintain most critical asset function and service availability while repelling or isolating the disruption.
- **Recover:** Restore all asset function and service availability to their pre-event functionality
- **Adapt:** Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient.

The Four Operational Domains

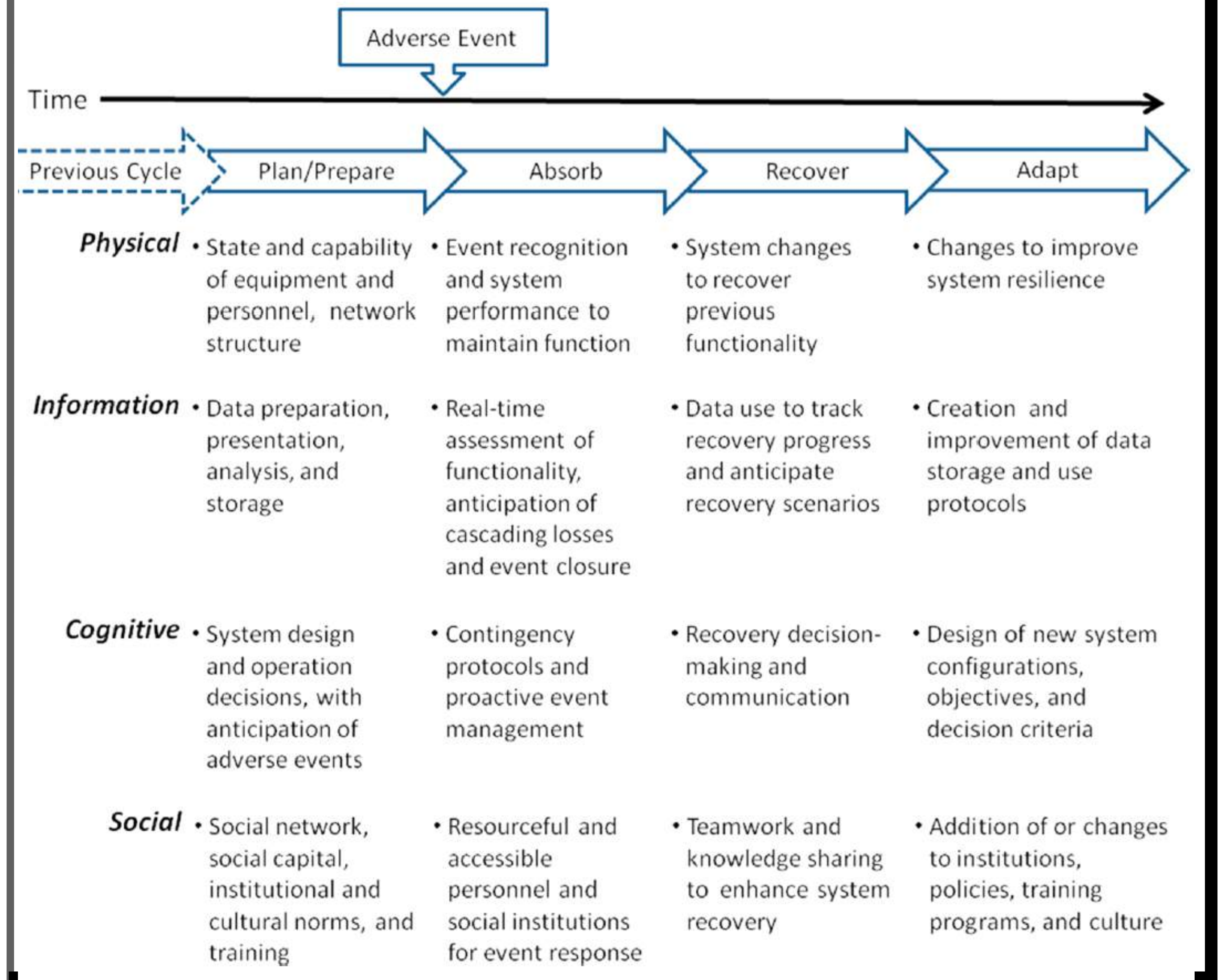
The Network Centric Warfare doctrine identifies four domains that create shared situational awareness and inform decentralized decision-making:

- **Physical:** Physical resources and the capabilities and the design of those resources
- **Information:** Information and information development about the physical domain
- **Cognitive:** Use of the information and physical domains to make decisions
- **Social:** Organization structure and communication for making cognitive decisions



Results: Resilience Matrix

The individual cells of the matrix contain metrics that measure the ability of a system to manage adverse events and present specific metrics for assessing the resilience of a cyber system. When interpreting the matrix, each cell addresses the question: **"How is the system's ability to [plan/prepare for, absorb, recover from, adapt to] a cyber disruption implemented in the [physical, information, cognitive, social] domain?"**



	Plan/Prepare	Absorb	Recover	Adapt
Physical	• State and capability of equipment and personnel, network structure	• Event recognition and system performance to maintain function	• System changes to recover previous functionality	• Changes to improve system resilience
Information	• Data preparation, presentation, analysis, and storage	• Real-time assessment of functionality, anticipation of cascading losses and event closure	• Data use to track recovery progress and anticipate recovery scenarios	• Creation and improvement of data storage and use protocols
Cognitive	• System design and operation decisions, with anticipation of adverse events	• Contingency protocols and proactive event management	• Recovery decision-making and communication	• Design of new system configurations, objectives, and decision criteria
Social	• Social network, social capital, institutional and cultural norms, and training	• Resourceful and accessible personnel and social institutions for event response	• Teamwork and knowledge sharing to enhance system recovery	• Addition of or changes to institutions, policies, training programs, and culture

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A (2013). Resilience Metrics for Cyber Systems. *Environment, Systems and Decisions* 33:471-

Permission was granted by the USACE Chief of Engineers to publish this material. The views and opinions expressed in this paper are those of the individual authors and not those of the US Army, or other sponsor organizations