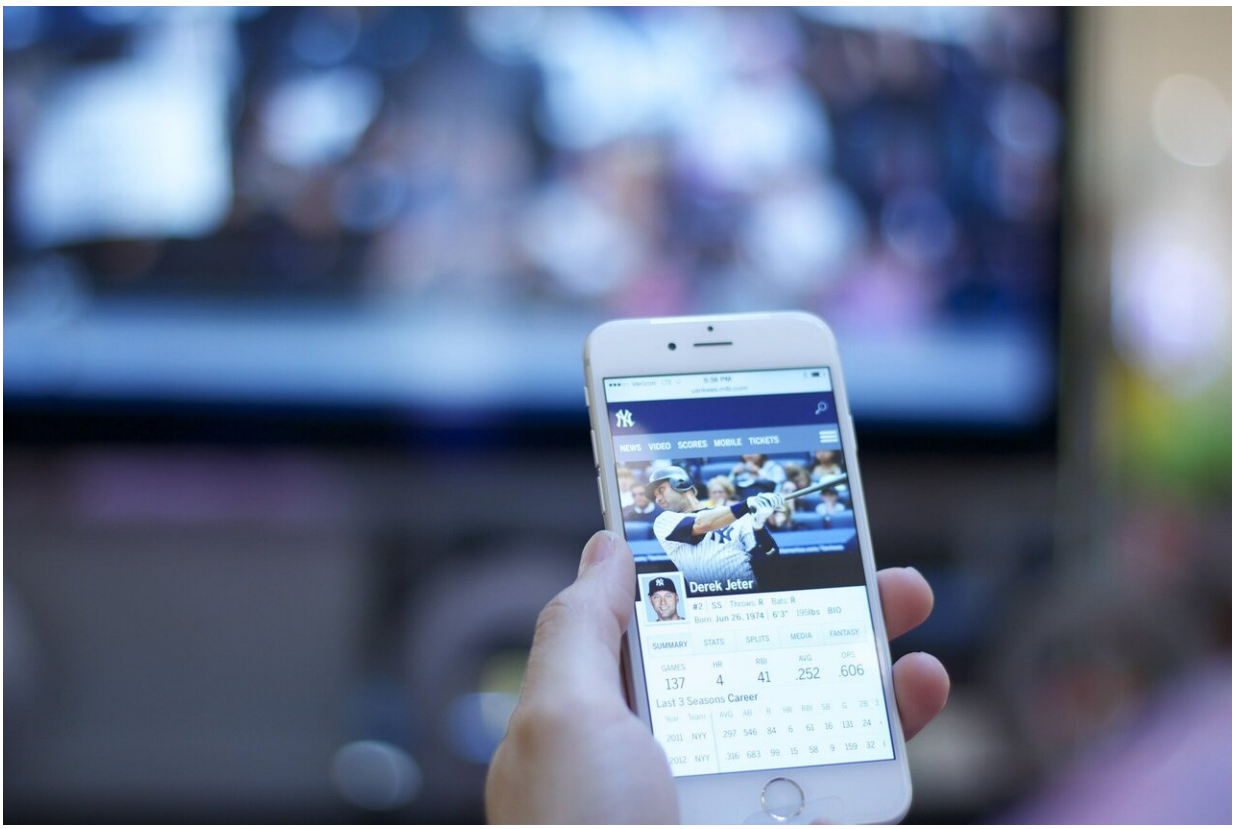
# Macro cyber resilience: Ensuring functionality of interconnected complex systems

April 16 2021, by Casey Knopik




Credit: CC0 Public Domain

For the second straight year, Pacific Northwest National Laboratory (PNNL) researchers are featured in a special edition of the *Journal of*

*Information Warfare*. This issue explores the topic of macro cyber resiliency.

"Last year, PNNL established the concept of autonomic resiliency," said Chris Oehmen, team leader for the Science and Experimentation team in the Cybersecurity group. "That's the idea that systems of the future will be so complex and interconnected that they will have to drive themselves. This year we wanted to build on that idea and talk about how that kind of resiliency thinking will allow us to move from micro cyber to macro cyber."

The journal is a resource for academics and professionals with an interest in information warfare and digital security, offering the latest thinking in operations for the military, government, industry, and educational perspectives.

For the Spring 2021 special edition, Oehmen served as guest editor with colleagues Samuel Clements and Angie Chastain.

**Connecting micro and macro cyber**

The prefixes of 'macro' and 'micro' have been applied to concepts like economics, or even to activities like photography. They are easy ideas to understand in large versus small scales. However, this term is not usually used to define cyber perspectives, an increasingly important area for security applications.

"I can't find anyone using macro cyber in the same way we are at PNNL," said Oehmen. "By using the terms micro and macro we can better define cyber and the areas individuals work in."

Through the nine papers featured in the limited publication, Pensuring the functionality of interconnected complex systemsNNL researchers

define micro as protecting individual devices, and macro as —like those found upholding critical infrastructures, such as the power grid. The approach of autonomic resiliency needs to work in tandem with macro cyber because there is risk with maneuvering in a complex cyber space.

"Cyber is a key part of the puzzle," said Oehmen. Critical infrastructures have existed for decades, having been built long before digital connectedness was even considered. But Oehmen said shifts in operating profiles are also happening in the global conflict space.

"Now operators not only have to worry about natural hazards or structural breakdown, they have to worry about cyber conflict in power grids, or transportation systems, or water treatment systems," said Oehmen."

These two areas play out very differently for an operator. With natural hazards, historical data helps define how frequently disasters happen or how probable it is that multiple disasters could happen at the same time.

"All of that goes out the window with a cyber conflict," said Oehmen. "We're trying to move from this idea of keeping small systems up and running, to resiliency of the system as a whole, or at the macro cyber level."

**Including policy in macro cyber concepts**

The special edition of the journal is organized into three main concepts which highlight areas PNNL excels in: foundations; tools and technologies; and policy and strategy.

"There is a huge body of knowledge at PNNL around these capabilities," said Oehmen. "Foundational representations, devices and approaches, and the policies that govern interconnected systems must work together

to accomplish true systemic resilience, or macro cyber."

Policy in particular is a key topic not often considered during technology development.

"If you want people to use technology or embrace changed behavior, you have to deal with policy at the same time you're building technology or systems," said Oehmen. "How do you think about laws, policy, and regulations in the future when systems won't look anything like they look today? That's what our policy teams are examining."

**More information:** Infrastructure Resiliency from a Macro Cyber Perspective. www.jinfowar.com/journal-issue/volume-20-issue-2

Provided by Pacific Northwest National Laboratory