Contribution ID: **551** Type: **Paper**

Evaluating Security Implications of the "Splinternet"

Monday 10 February 2020 17:00 (15 minutes)

The internet, which for years has been viewed as a global online commons with standardized protocols but few regulations, is, according to some experts, starting to mirror the contentious political and commercial contours of the physical world.

A number of problems, including data breaches, privacy debates, cyber enabled attacks on critical infrastructure, government surveillance operations, theft of intellectual property, and manipulation of electoral processes, have contributed to a growing skepticism in many states that an open internet will naturally serve the best interests of users, communities, countries, and the global economy. In addition, the rapidly emerging and increasingly lucrative power of data has global superpowers eager to protect their informational sovereignty as an urgent matter of national security.

Recognizing some of the problems associated with an open internet, a number of States have begun making efforts to isolate their domestic internet for politic, economic, or social reasons. This trend towards a more fractured internet, or "splinternet,"has courts and governments embarking on what some call a "legal arms race" to impose a maze of national or regional rules, often conflicting, in the digital realm.

There is a need to evaluate the possible security implications if the internet does indeed fracture into a number of smaller, nationally-administered internets organized along geopolitical boundaries. While the status quo is not without its own vulnerabilities, a new structure may present new or different threats to the physical protection systems and cyber security measures that currently protect nuclear facilities and material worldwide.

Considering a potential future "splinternet,"this paper will specifically assess how a fractured internet may affect the various nuclear security systems operating around the world. Specific questions could include:
• Will fractured monitoring of malware threats increase the severity of malware outbreaks?
• Could less comprehensive evaluation of vulnerabilities further erode trust in safety/security systems?
• Will it be more difficult to provide robust configuration management across unique application domains?
• What are the safety and security implications for industrial control systems (PLCs and similar) if they become less standardized?
• If the Internet fractures along national borders, will it lead to new protocols and architectures for large networks?
• Will it enable or hinder attribution of bad actors in the digital realm?

State

United States

Gender

Author: GERHRIG, Lindsey (Pacific Northwest National Laboratory)

Co-author: GOYCHAYEV, Rustam (Pacific Northwest National Laboratory)

Presenter: GERHRIG, Lindsey (Pacific Northwest National Laboratory)

Session Classification: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification: CC: Information and computer security considerations for nuclear security