Cybersecurity requires international cooperation, trust

April 13 2020, by Melanie Lefkowitz

Credit: CC0 Public Domain

Most experts agree that state-sponsored hackers in Russia are trying to use the internet to infiltrate the U.S. electrical grid and sabotage elections.

And yet internet security teams in the U.S. and Europe actively seek to cooperate with their Russian counterparts, setting aside some of their differences and focusing on the issues where they can establish mutual trust.

"Even though they recognize that there are actors in the shadows in those countries whom they don't trust, they have a shared goal of keeping the infrastructure running," said Rebecca Slayton, associate professor of science and technology studies in the College of Arts and Sciences.

Slayton is first author of "Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989-2005," which was published April 13 in the journal *Technology and Culture*.

"These teams are generally regarded as fairly effective," she said, "and if you want them to continue to be effective in keeping the internet running, then we need to overcome the barriers to cooperation that some governments are putting in place."

Slayton's article, co-authored with Brian Clarke, a doctoral student in the field of science and technology studies, provides a historical case study of the rise of computer security incident response, shedding light on how experts—and nations—can more effectively combat cyberwarfare when they foster trust and transcend politics.

"To maintain this infrastructure for coordinating incident response, you have to constantly maintain relationships," said Slayton, who is also director of Cornell's Judith Reppy Institute for Peace and Conflict Studies. "People often think of infrastructure as a set of technologies just sitting there, but in fact they're living technologies—socio-technical systems that are constantly being maintained by people, and trust is central to that."

The field of incident response began after the internet was struck by "an attack from within" in November 1988. A self-replicating program—a "worm"—infected thousands of connected computers, causing them to stop processing and communicating normally.

The outage was unintentionally caused by Robert Tappan Morris, then a Cornell graduate student, conducting an experiment. It became a wake-up call, leading the Defense Advanced Research Projects Agency, the internet's sponsoring organization, to establish the Computer Emergency Response Team Coordinating Center as a centralized, reliable contact for computer emergencies.

Although computer scientists realized that the connected nature of the internet required international cooperation, global participation in these efforts was initially limited. But that began to change in the early 1990s, with the formation of the Forum of Incident Response and Security Teams (FIRST), which remains the leading global organization of security experts.

To help ensure that members were trustworthy, FIRST required prospective members to be nominated by existing members and voted on by the steering committee.

Today, with nearly all information and systems relying on digital networks, internet attacks have the potential to cause far more harm. Trusting each other on some issues—and not others—can potentially both enhance computer security and help otherwise antagonistic nations work together.

"Teams in the U.S. and in Europe very much want to cooperate with teams in Russia, and they see that as a way of having influence they might otherwise not have in that space," she said. "It just underscores the importance of having this kind of trust develop across borders." The

paper also addresses cooperation across regional conflicts in Asia, such as between China, Japan and Korea.

"People who work for networking organizations are committed to keeping the technology working no matter what," Slayton said.

Previous research on the history of computer and network security focused largely on development of new technology, rather than repair or maintenance. In the paper, Slayton wrote that without the efforts of incident responders, the internet as we know it wouldn't exist.

"It's one thing to come up with a new algorithm or a new technique for, say, intrusion detection, but actually making it work and operate requires people to implement and maintain it on an ongoing basis," Slayton said. "It's nice to think some innovative technology will fix everything. But in practice, people have to keep things up to date, particularly when you're dealing with an intelligent adversary. You have to stay ahead of that."

More information: Rebecca Slayton et al, Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005, *Technology and Culture* (2020). DOI: 10.1353/tech.2020.0036

Provided by Cornell University