FIFTH DOMAIN
CYBER

Why more research is needed to craft good cyber policy

Mark Pomerleau

February 13, 2020

How cyber operations fit into geopolitics and act as a tool of statecraft is still largely not understood despite decades of cyber activity, experts said Feb. 12.

A flood of large scale hacks, data dumps, espionage, sabotage and cyber-enabled information warfare have driven academics and policy makers to better understand the nuances of cyberspace and the application of cyber tools in political affairs. But much work remains, experts said during an event hosted by the Atlantic Council Feb. 12.

“We’re trying to build a field in cybersecurity. I don’t think we’ve done that well enough,” said Brandon Valeriano, a senior fellow at the Cato Institute and Bren Chair of Military Innovation at the Marine Corps University. “I don’t think we have enough empirical background. A lot of people make too many guesses. Too many claims about evidence. There’s a lot of ‘I think, I believe,’ we want to get towards some sort of version of ‘I know,’ and doing that through empirical truth claims. A way to do that is through multi-method research.”

Valeriano and Benjamin Jensen, nonresident senior fellow at the Scowcroft Center for Strategy and Security at the Atlantic Council and professor of strategic studies at the Marine Corps University, presented the findings of a study they published in November on cyber escalation. The study surveyed participants from the United States, Russia and Israel, proposed different scenarios to understand baseline escalation risks and examined differences of how others in the international community approach cyber operations.

The conventional wisdom in the cyber world has been that cyber operations can escalate situations unnecessarily, more so than physical or kinetic responses. But many academics now disagree.

“Doing all this work, what do we really find? We find that cyber conflict and competition is not what you’re seeing in the headlines. It’s not what it’s being made out to be,” Jensen said. “If anything, cyber operations proved to be a de-escalation mechanism. It was a way that players opted to try to manage complex interactions underneath the threat of escalation.”

Jacquelyn Schneider, Hoover fellow at the Hoover Institution at Stanford University argued in an October 2019 op-ed in the Washington Post that cyberattacks aren’t likely to deter adversaries for the same reasons they aren’t likely to lead to escalation: in order to deter, one needs to send a signal that there will be consequences for actions. But given that cyberattacks are difficult to

attribute and often rely on vulnerabilities that can be eliminated, it can be a troublesome way to send diplomatic signals and thus makes it less escalatory.

“What’s been fascinating is that these cyber operations seem to create space for almost de-escalation,” she said at a January event. “I believe that the U.S. can actually take more risks in cyberspace than it has been taking in the past.”

Valariano said he wants to see less guessing.

“More often than not, people believe things are happening in this domain or in this field without really knowing. I think we really need to have a firm baseliner of understanding of how cybersecurity operates,” he said.

The results of the survey led Jensen to note that “cyber is just political warfare for the 21st century.”

“It’s a vehicle for espionage, sabotage, propaganda, manipulating beneath the threshold of armed conflict. It’s not this decisive super weapon, it’s not the proverbial bomber [that] will get through … It’s something distinctly different,” he continued.

One such parallel effort to help craft better understanding, and even lead to policy outcomes, is the Cyberspace Solarium Commission. The commission is a bipartisan organization created in 2019 to develop a multipronged U.S. cyber strategy. It expects to deliver a report in early March.

The panelists at the Atlantic Council event played a role on the commission and one speaker leads what is called Task Force 1. That group examined more aggressive postures such as deterrence and “defend forward,” the Department of Defense’s charge to confront cyber threats outside U.S. networks before they reach the United States.

In order to develop a stronger strategy, Jensen said, one must start by acknowledging differences and building them out. He added that the studies and work that focuses on escalation is important for the commission

“If I do take a more offensive posture in this domain, what does it do? That’s a critical question,” he said.

This type of empirical research is valuable for having frank discussions about topics such as escalation and can help to better work through thorny questions such as when is cyber the right tool in that competition, is it better than other tools of government such as indictments, sanctions or demarches and when is it useful to increase cyber operations in a particular region versus a cyber event that might not clearly send the intended message?

“What did we did we find about escalation? There’s not that much to see there yet and it’s actually a good news story,” he said, “But it’s also a dangerous story because it shows how modern great powers use connectivity to engage in this broader political warfare competition to achieve a position of advantage.”