Cybersecurity Solarium Commission Previews Upcoming Report at RSA

The report, to be issued March 11, will outline a national and allied effort to defend in cyberspace.

James Mersol
Wed, 02/26/2020 - 20:02

President Eisenhower cooking quail in the White House solarium. Photo Credit: National Archives.

A Congressionally mandated group aimed at tackling how the U.S. will approach a national strategy for cyberspace gave a peek at what's to come ahead of the release of its recommendations next month.
In 1953, President Dwight Eisenhower, recognizing that the rise of the Soviet Union following World War II represented a fundamental shift in the geopolitical landscape, convened Project Solarium, a strategic exercise designed to shape U.S. strategy to this new reality. The exercise formed the beginnings of what became containment strategy during the Cold War and is considered by many to represent the urgency for the U.S. to “get it right” for its foreign policy toward the Soviet Union.

Nearly 70 years later, the fiscal year 2019 National Defense Authorization Act authorized the convention of a second Solarium focused on cybersecurity, again recognizing that cyber threats represent a fundamental shift in how the U.S. government approaches its foreign policy. Ahead of the Cybersecurity Solarium Commission’s report, which will be released March 11, members of the commission spoke at the 2020 RSA Conference to talk about the commission’s process and offer an outline of the report.

“You’ll read a case for action right up front,” said Chris Inglis, distinguished visiting professor of cyber studies at the U.S. Naval Academy and one of the commissioners. “You’ll then read the commission’s summary statement [that says] while we don’t think the collective approach has been working — deterrence has not been working, that order and discipline have been fading away in cyberspace — our declared intent [is to] put together a set of recommendations that say we can in fact deter adversaries in cyberspace.”

Some may wonder how this commission differs from recent federal cybersecurity initiatives.

“The thing I think was really unique was having the executive branch sitting on the commission as actual commissioners,” said Suzanne Spaulding, who is the former director of the Department of Homeland Security’s National Protection and Programs Directorate (NPPD), senior adviser on homeland security to the International Security Program at the Center for Strategic and International Studies (CSIS) and another of the commissioners. “[They were] present for every meeting and fully engaged in the conversations. That made a significant difference.”
Spaulding added that commissions often act outside the executive branch, causing months of delay between recommendations and action while the executive branch reviews the report — a significant loss of time that often leads to nothing happening during the same administration.

“Having the executive branch on there means they are already informed,” she underscored. “They know exactly how we got where we got.”

Just as importantly, the report will not lay out an “aspirational approach” to cybersecurity, but instead closely focus on “achievable” procedures and policies. The commissioners shared that the report will include an appendix that features actual draft legislation to accelerate change in Congress.

Another important feature of the Cybersecurity Solarium Commission is that, unlike the 1953 exercise, the commission featured a representative from the private sector and interacted with international partners, said Inglis.

“We engaged upwards of a dozen foreign nations,” he said, “who all have various strategies — some ahead of ours — in terms of the sophistication, the applicability to our problems. We engaged academia. We engaged the private sector ... Our job was not to come up with the new ideas — they were already on the table, offered by that robust and diverse group of people. Our job was to figure out how to actually integrate them into a fabric so we could achieve integration and in the human dimension, collaboration.”

While the commissioners declined to preview specifics about their report, they did discuss some of the broad strokes that the report will cover.

“When you look at the report you will really see that what really dominates and has pride of place in the report is the resilience,” said Spaulding. “As you’re trying to alter the bad actors’ behavior, you want to both raise the costs and also reduce their sense of what they’re going to be able to accomplish.”

Echoing CISA director Chris Krebs’ remarks earlier in the day, Spaulding added that resiliency includes “analog solutions” including paper backups for voting machines, but the report will go beyond just elections to develop the idea of a “resilient society.”
“We genuinely tried to go beyond the same old, same old ‘identify the problem and talk about the public-private partnership,’” said Frank Ciluffo, director of Auburn University’s McCrary Institute for Cyber and Critical Infrastructure Security and also one of the commissioners, “but really to translate some of those nouns into verbs and really understand how we can move from where we are from where we want to be ... and you’ll see a number of findings along those lines.”

Naturally, the report also covers federal agencies, especially each agency’s role in the broader federal cybersecurity posture.

“You will have a series of recommendations in terms of how the executive branch can better unify some of its capabilities,” Ciluffo said. “You’re going to see some real emphasis on doubling down and enhancing certain agencies’ capabilities right now ... At the end of the day, it’s really about how we get FBI, NSA, DOD and DHS — how does that triad [sic] come all together? We spent a lot of time looking at ways to enhance that synchronization.”

In total, the report will recommend 75 actions across six “very specific pillars” of action. The majority of these actions will include a legislative component, ideally “executed within a legislative year,” Inglis said.

Following the report’s release, the commissioners plan to appear before the armed services and intelligence committees in both houses of Congress to testify on their recommendations and explain what appropriate resource allocations for these recommendations might be.