The New National Cybersecurity Strategy—A Strategic Step Forward

By Frank J. Cilluffo director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security

Published Mar 02, 2023 at 12:34 PM EST
Updated Mar 02, 2023 at 7:17 PM EST

The much-anticipated National Cybersecurity Strategy has now been released by the Office of the National Cyber Director. With so many equities at play, it's no surprise that the Strategy took time to see the light of day.

The five pillars of the strategy—defend critical infrastructure; disrupt and dismantle threat actors; shape market forces to drive security and resilience; invest in a resilient future; and forge international partnerships to pursue shared goals—build on good work that has been done already. Ultimately, however, the value of the strategy will be determined by the extent to which it is implemented, and desired outcomes are actually achieved.

Although all five pillars of the strategy are intertwined, the first two are foundational to the overall.

The top strategic objective within pillar one is to scale public-private collaboration. For cyber domain, this is truly the holy grail, because the vast majority of U.S. critical infrastructure is owned and operated by the private sector. Without meaningful and sustained public-private partnership, cybersecurity and resilience of our most critical assets—from older to newer such as commercial space—will fall short.

A man takes part in the Summer School of the intelligence agencies AIVD and MIVD in Zoetermeer, Netherlands on August 1, 2022. - For two weeks, interested parties can get to know the work of... Sem van der Wal/AFP via Getty Images

The strategy commits to collaborating with industry to

identify and address sector-specific needs, and leverage technology such as "machine-to-machine data sharing" to counter threats in real time. This will build a bedrock of trust—the coin of the realm—for effective response.

But trust takes a long time to earn and only a nanosecond to lose.

Recognizing the need to harmonize and synchronize regulations will go a long way. More work in this area is plainly needed. Hopefully, the strategy's emphasis on regulation will, in practice, balance sticks with carrots and not lock us into the starting blocks. Industry must also look hard at itself to identify and understand interconnections between IT and operational technology (OT) and the vulnerabilities inherent in supply chains.

By focusing on and investing in sector risk management agencies (SRMAs) that take point, day to day, on security and resilience within designated critical infrastructure sectors, the strategy takes an important step. SRMAs vary substantially when it comes to capabilities and resources. The energy sector is light years ahead of the water sector, for instance, although we all have a vested interest in their ability to deliver. A concerted effort to lift all boats is laudable and past due.

The strategy also recognizes that a push is needed to

"strengthen and integrate the Federal Government's operational capabilities" as this is the engine that powers support to outside partners. Failing to marshal and mobilize ongoing but disparate efforts on the government side leaves the nation short of where it could be and does no favors to the companies upon which we rely the most.

There is also good news, such as the standup of the Joint Cyber Defense Collaborative (JCDC) under the auspices of the DHS Cybersecurity and Infrastructure Security Agency (CISA). The strategy cited the JCDC as an example of progress "to integrate cyber defense planning and operations across the Federal Government and with the private sector and international partners." This marks the beginning of what a shift in the landscape could look like—where defense gives our adversaries a genuine run for their money. For a country that has a lot (if not the most) to lose in cyber domain, that's significant.

This point is closely connected to the second pillar of the strategy, which speaks to threat actors and how to thwart them. Here the strategy underscores the need for greater public-private collaboration to "improve intelligence sharing" and "execute disruption campaigns at scale." In the past, joint (public-private) operations have been more the exception than the rule. We must work to flip that script. The FBI, Secret Service, and broader law enforcement

community are integral, as we have seen. These efforts must be redoubled.

With the private sector at the tip of the spear on a battlefield that they never chose to join, companies are instrumental to national strategy. We now have a document that not only acknowledges this reality but lays out an ambitious roadmap for making the most of federal capabilities and leveraging them to better support those on the frontlines defending our most critical of infrastructures.

Read more

- Let's Bring Greater Transparency to Foreign Influence on Policy Making
- FBI Gaslights America Over Twitter Files
- When States Buy Chinese, America Is Put at Risk

Creating a resilient system of networks that is costlier to attack than defend is an ambitious goal, but we need to think big because there is so much at stake. Pushback here is about so much more than ones and zeroes. Democracy itself is on the line as autocrats the world over—including in China, Russia, Iran, and North Korea—seek to shape the internet to conform to their own ends and vision.

The new strategy lifts cyber up to meet the challenge, taking it mainstream and aligning it with more traditional instruments, such as our game plans for national security, defense, diplomacy, and economic security. It aims to impose costs and consequences on hostile actors and

recognizes that we will never be able to simply defend our way out of the problem—embracing the defend forward concept that the Department of Defense has successfully put into practice.

Frank J. Cilluffo is director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security and served as a commissioner on the U.S. Cyberspace Solarium Commission.

The views expressed in this article are the writer's own.