11 May 2020

The Coronavirus Pandemic Shows the Need to Finally Take Cyber Resilience Seriously

Ian Wallace

When the final report of the U.S. Cyberspace Solarium Commission was released in Washington on March 11, just thirty people had been reported to have died as a result of the coronavirus pandemic in the United States, and the unemployment rate for March was a relatively low 4.4 percent. With the exception of those related to election security, relatively little attention was paid to the report's recommendations aimed at strengthening national cyber resilience, including two key ones on developing a better understanding of the national cyber risk and enabling rapid recovery from a cyber incident. Nearly two months later, however—with an estimated 20 million Americans finding themselves jobless and forecasts of over twice the number of deaths as the United States experienced from combat during the Vietnam War—it is clear that the United States needs to evolve its thinking about security.

With cyber regularly ranked alongside pandemics as a major threat to the nation in the threat reports of the intelligence community, that section on resilience —defined as "the capacity to withstand and quickly recover from attacks"—deserves more attention. It could prove the most prescient and important set of recommendations in the entire report. Once the initial crisis is over, Congress and the White House should finally get serious about national resilience, including to cyberattacks, as a key component of national security.

The commission was mandated by Congress to "develop a consensus on a strategic approach to defending the United States in cyberspace." Its big idea turned out to be a deceptively simple proposal for a U.S. policy of "layered deterrence," combining strong military capability with international engagement and a greater resilience at home. Yet, while presented as a coherent package for Congress, the danger is that members will dine à la carte on the recommendations, promoting some and quietly parking others. It is also unclear whether anyone has the political will to fight for the cyber resilience package. Sadly, history is not encouraging. Protected by two great oceans, the United States has rarely had to prioritize resilience to attack in security policy (with the exception of the nuclear deterrent). Superficially, 9/11 did much to shake the country out of a cozy sense of invulnerability, leading to the establishment of the Department of Homeland Security. However, the conduct of U.S. national security policy did not change as much as it might have. Costly wars in Afghanistan and Iraq as well as the wider global counterterrorism operation can be seen as attempts to keep potential harm to the United States "over there." Meanwhile, the primary focus of the Department of Homeland Security has become to keep out the United States' enemies, especially terrorists. By comparison, despite the 2017 National Security Strategy identifying "priority actions" like "Improve Risk Management," "Build a Culture of Preparedness," and "Improve Planning," resilience has been afforded a relatively lower priority.

Opportunity in Crisis

The coronavirus crisis presents an opportunity to change that and to establish a much more balanced national cyber strategy. There are clearly differences between health and cyber risks, but they have in common that the dangers that they pose are magnified by the nature of the modern world, with its levels of connectivity, globalization, and even urbanization. Other novel risks such as disinformation campaigns and extreme weather caused by climate change also fall into this category. All are hard to contain within national borders and, in different ways, have the potential to wreak havoc for the general population. But they are also all risks that can be mitigated with prudent risk management, contingency planning and preparation, and deliberate policy choices on things like supply chains—much of which will be common across multiple scenarios. As several Asian countries have shown in the coronavirus pandemic, learning lessons from past experience (either real or simulated) pays dividends in crisis response.

None of this should be news to national security leaders. The Cybersecurity & Infrastructure Security Agency within the Department of Homeland Security exists in part to help build national resilience to cyberattack, including through its National Risk Management Center, working with sector-specific agencies to build the resilience of the sixteen critical infrastructure sectors. The problem, as set out in the Solarium Commission report, is that, while cyber resilience is a well-established discipline within the best companies, these organizations simply do not have the resources or the appropriate human capacity to do the job that is needed at the national, especially economic, level. That is a damning conclusion and one even less acceptable than it was two months ago.

Building resilience at home should not be taken as an abandonment of a global approach. America First did not work in the 1930s, and it will not work again. As the commission has recognized, the United States needs a layered approach to cyber defense. In fact, it is even arguable that it has been the very lack of resilience at home that has inhibited U.S. leaders from taking strong action in cyberspace (for example, in response to election interference by Russia in 2016). Resilience creates flexibility to decide how to engage internationally.

The United States should think of support for cyber resilience in the same way as Defense Secretary Robert Gates famously argued for more funding for the State Department—as a necessary complement to military power.

Nor should a greater focus on resilience at home be seen as being weak on defense. It might well require shifting resources from the Pentagon to other agencies like the Department of Homeland Security. But especially in a post-pandemic world that has forever increased the use of technology in daily lives, from online education to 3D printing and more, if that technology can be held at risk by an adversary, that has the potential to seriously undermine the effectiveness of the rest of the Pentagon's arsenal. The United States should think of support for cyber resilience in the same way as Defense Secretary Robert Gates famously argued for more funding for the State Department—as a necessary complement to military power.

Plenty can be done to enhance national resilience to cyberattack. In the medium term, the authorities should be looking to ensure that such resilience is recognized as a priority in the effort to recover and respond to the coronavirus crisis, including getting people back to work. For example, in recent years the U.S. economy has suffered from a significant shortfall in trained cybersecurity professionals. While over time artificial intelligence will fill some of that gap, the continuing growth in the use of information systems across all aspects of

work and life means that need will endure. Using government funding to reskill unemployed workers could be a shrewd way to boost resilience while also rebuilding the economy. More broadly, though, consideration should be given to making cyber part of other legislative efforts. For example, if Congress once again turns its attention to healthcare reform, as seems likely, better cybersecurity in that sector should be part of the agenda.

In the longer term, U.S. leaders should be encouraged to think much more broadly about how resilience generally, and cyber resilience specifically, should feature in the conception of national security. That could include working more closely with allies on enhancing resilience (for example, through NATO) and through working to realign defense research and development priorities.

In the short term, however, Congress needs to act boldly and finally get serious about resilience to cyberattack by adopting as many as possible of the fifteen resilience-focused recommendations in the Solarium Commission's report, along with others that could follow in a recently announced post-pandemic annex to it.