LAWFARE

The Strategic Implications of SolarWinds

Benjamin Jensen, Brandon Valeriano, Mark Montgomery

December 18, 2020

Recent reports of a widespread Russian cyber infiltration across U.S. government networks are a sign of how great power competition will play out in the 21st century. The new great power game is digital, with the shadowy alleys and cafes of Cold War spy games replaced by massive data breaches and compromising corporate security. Some strategies see this world as dominated by offensive operations—but the SolarWinds case suggests the opposite. The U.S. Cyber Solarium Commission, on which we served, found that the future of cyber security strategy will come to rely on layered cyber deterrence to enable defensive denial operations, international entanglement and cost imposition when aggressors defy the norms of the international system. The SolarWinds hack emphasizes the importance of implementing this strategy.

It's simpler to list the agencies that have *not* been caught up in the SolarWinds infiltration, which was run by Russian hacking group APT29 under the umbrella of the Russian intelligence services, the SVR. So far, only the intelligence community has not been reported to have been breached.

The goal of the operation seems to have been exfiltrating data and digital tools from the targets. The attackers leveraged a supply chain vulnerability in the ubiquitous SolarWinds Orion program, a network monitoring tool, to insert backdoors into an update released months ago. Once inside the networks, the attackers were able to maintain a permanent presence. The operation was so devastating that SolarWinds employees appear to have engaged in a massive sell off of stocks prior to public disclosure of the vulnerability.

The impact of the operation is currently unknown. Overall, the likely outcome seems similar to that of the Office of Personal Management (OPM) Hack of 2015, which resulted in the massive theft of unclassified government data by China but without any clear use of the data by Beijing in the subsequent years. But the SolarWinds breach will have second and third order effects. Already, FireEye's Red Team tools have been stolen through the SolarWinds vulnerability and reused by the attackers on other systems. The key thing to remember at this point is that the operation seems likely to be able to extract information but not insert or destroy data within government systems.

The SolarWinds operation demonstrates the developing nature of modern great power competition, where rival states employ cyber strategies to steal secrets as well as to conduct limited operations meant to disrupt and degrade. Though media reports often characterize cyber operations as attacks, many operations are better thought of as instruments of political warfare and weak forms of coercion that do not seek destruction. Most cases involve stolen data or limited disruptive effects. There appear to be key firebreaks that limit escalation in cyberspace, keeping it a realm of covert and clandestine operations as opposed to decisive battles.

We have worked with Ryan Maness of the Naval Post Graduate School to compile the Dyadic Cyber Incident Dispute Dataset (DCID), which tracks all known cyber actions between rival nation-states from 2001 through 2016. Examining the SolarWinds operation alongside the other operations in this dataset, the operation appears similar to past Russian and Chinese network infiltrations like the aforementioned OPM hack or Russia APT29's prior operations against the State Department and other government agencies. Great powers use cyberspace to alter the balance of information and gain an advantage in long-term competition. In this manner, espionage supports broader coercive campaigns and crisis bargaining, helping each side either signal in the shadows or determine the capabilities and resolve of its rival.

The SolarWinds operation demonstrates that U.S. Cyber Command's vision of persistent engagement, which calls for preventively imposing costs as adversaries to shape competition in cyberspace, appears not to have worked as expected. Persistent engagement and hunting forward on Russian networks apparently did not do enough to change the cost-benefit or risk calculations of Russian hackers targeting U.S. networks and did not dissuade Moscow from conducting one of the largest data heists in history. This dynamic played out similarly with respect to election hacking. Despite actions aligned with the persistent engagement posture to stop foreign groups from waging sophisticated social media campaigns and probe U.S. election infrastructure, Russia, China and Iran all were caught trying to interfere with U.S. domestic politics.

Punishment strategies—that is, strategies seeking to impose costs—which include constant operations as a matter of public policy are self-defeating in cyberspace, because there is no wider conception how the adversary will react. Hunting forward in operation is no guarantee of preemptively disrupting ongoing operations—and it does not impose clear signaled costs on the opposition, as is needed to dissuade limited cyber operations in the realm of espionage.

In the future, what is required is a deeper focus on denial-based approaches: How can the U.S. limit the attack surfaces available to the opposition and harden targets to ensure resilience? The goal should be to make it more difficult for states to launch sophisticated, widespread cyber intrusions—and this can be done by reducing the attack surfaces available to the opposition.

That logic is at the core of the U.S. Cyberspace Solarium Commission, which called for implementing a new approach: layered cyber deterrence. Layered deterrence implies three coordinated sets of activities that work together to alter the cost and benefit calculation of launching large cyberattacks against American interests. There is no way to stop all activity in cyberspace, just as there is no way to stop all espionage, but it's possible to make this activity more costly—thus decreasing the severity and frequency of attacks.

Through entanglement strategies that seek to leverage international institutions, regulatory bodies and international law, the U.S. government works with partners, allies and international organizations to share information and facilitate global efforts to isolate and prosecute state officials and criminals linked to nefarious cyber activity. In the denial layer, U.S. government officials build deeper relationships with the private sector, harmonizing regulation and creating incentives to build security into networks. This requires collecting and standardizing data, as well as continual tests and validation to create a more functional cyber insurance marketplace.

Layered deterrence preserves the capability and capacity to defend forward and conduct targeted operations that signal capabilities and resolve. Because cyber operations take place in the shadows, this requires deliberate signaling and demonstrating network resilience—which can be

accomplished through actions such as establishing and testing continuity of government and economy procedures in the event of a massive attack. Rival states need to know the United States is testing and hardening its networks.

Implementing layered cyber deterrence requires extensive executive and legislative action. The FY21 National Defense Authorization Act, currently sitting on the president's desk, contains a number of provisions that can help address incidents like this.

In order to provide strategic leadership on cybersecurity from the White House, Section 1752 establishes a Senate-confirmed National Cyber Director within the White House to serve as the president's principal cyber advisor, ensure agency compliance with federal policies and lead interagency cyber contingency planning and incident response. The bill also contains several provisions that speak directly to preventing an event like SolarWinds. Section 1705, "Strengthening Federal Networks," authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to conduct threat hunting on federal networks (that is, everything ending in .gov). Section 1715 establishes a Joint Cyber Planning Office under CISA, to facilitate comprehensive planning of defensive cybersecurity campaigns across federal agencies and with the private sector. Section 1745 tasks the secretary of homeland security to conduct a comprehensive review of CISA's ability to fulfill its current missions and recommend appropriate authorities and resources to get the agency mission ready.

Finally, in order to better respond to a hack like SolarWinds, Section 1716 grants administrative subpoena authority to CISA so the agency can identify vulnerable systems and notify public and private system owners. And Section 1731 directs the executive branch to submit a report to Congress evaluating the federal cybersecurity centers and the potential for better coordination of federal cybersecurity efforts at a properly functioning integrated cybersecurity center within CISA.

The Biden administration should embrace these changes established by the NDAA and ensure their swift implementation. Beyond this, however, the Biden team also needs to pursue efforts to build a more effective defensive effort to deny adversaries the ability to execute hacks like SolarWinds. This will involve not only improving the federal government's cybersecurity readiness, but also building the elusive public-private collaboration on critical infrastructure protection that has eluded the past four administrations.

Brandon Valeriano is the Bren Chair of Military Innovation at the Marine Corps University and a Senior Advisor with the Cyberspace Solarium Commission. He is also a Senior Fellow at the Cato Institute. Dr. Benjamin Jensen is a Senior Research Director and leads the Strategic Initiative Group with the U.S. Cyberspace Solarium Commission. Mark Montgomery serves as the Executive Director of the Cyberspace Solarium Commission.