

# Russia's Hack Wasn't Cyberwar. That Complicates US Strategy

wired.com/story/russia-solarwinds-hack-wasnt-cyberwar-us-strategy

Erica Borghard, Jacquelyn Schneider

December 17, 2020



The list of US government agencies compromised in the SolarWinds hack continues to expand, with reports of infiltrations at Treasury, Commerce, Homeland Security, and potentially State, Defense, and the CDC. This is a big deal for national security: It is the largest known data breach of US government information since the Office of Personnel Management hack in 2014, and could give hackers a trove of inside information.

Though the scope of this hack is still being determined, such an extraordinary breach begs a fairly obvious question: Is US cyber strategy working? The US has historically relied on, first, a deterrence strategy and, more recently, the idea of “defend forward” to prevent and respond to malicious behavior in cyberspace. Is a failure of these strategies to blame? The answer (like all things political) is complicated.

First off, it's important to establish what this hack *was*. The fact that a purportedly nation-state actor (likely Russia) was able to compromise a third party (SolarWinds) to gain access to an as-yet-unknown number of US government networks and exfiltrate data is a significant espionage achievement. And it illustrates how third-party vendors can provide an avenue for threat actors to conduct espionage campaigns at a scope and scale typically not seen outside of cyberspace.

But to call this incident a cyberattack would be off the mark. At this point, the operation appears to have been espionage to steal national security information, rather than to disrupt, deny, or degrade US government data or networks. While it may seem like splitting hairs, terminology is important because it has policy, and often legal, consequences. Espionage is an accepted part of international statecraft, one that states often respond to with arrests, diplomacy, or counterintelligence. In contrast, an attack (even a cyberattack) has international and domestic legal ramifications that could allow states to respond with force. So far at least, this hack is not that.

The question of what this incident means for cyber deterrence, on the other hand, is less straightforward. To understand why this is a complicated question, it's helpful to understand how this strategy works (and doesn't). Deterrence is about convincing an adversary *not* to do something by threatening punishment or making it seem unlikely the operation will succeed. This is a hard thing to do for a few reasons. First, states need to threaten a response that is both scary and believable. A threat may not be credible because the state lacks the capabilities to carry it out. Or, as is more often the case with the United States, threats may lack credibility because adversaries don't believe there will be follow-through. For instance, the US might threaten to use nuclear weapons in response to cyber espionage, but no state would believe the US would actually launch a nuclear attack in response to a data breach. It's just not a credible threat.

To make matters even more complicated, it's also hard to tell when deterrence has actually worked because, if it does, *nothing* happens. So even if a state *was* deterred by a good defense, it's almost impossible to know whether the state didn't follow through with the attack simply because it wasn't interested in taking the action in the first place.

There are few if any, deterrence mechanisms that work to prevent cyber espionage. Because states routinely spy on one another—friends and foes alike—there are a very limited number of credible punishments states can use to threaten others into not spying. The US has tried using a handful of options for cyber deterrence, such as issuing warrants for state-sponsored hackers or threatening sanctions for cyber intelligence. But these have had limited success. This does not mean, however, we should throw out the deterrence baby with the bathwater. As Jon Lindsay, a professor at University of Toronto, points out, the success of deterrence outside of cyberspace can incentivize and shape state behavior within cyberspace. And, there is compelling evidence that deterrence *can* work in cyberspace. No adversary has ever conducted a cyberattack against the United States that created violence or sustained, significant effects on infrastructure or military capabilities. Arguably, this is because the US's large and lethal conventional military force is a credible deterrent at higher cyber thresholds. The more vexing strategic challenge for the US is in the space between national security espionage (where deterrence doesn't quite apply) and major cyberattacks (where deterrence seems to hold).

In terms of the SolarWinds incident, the deterrence game is not yet over. The breach is still ongoing, and the ultimate end game is still unknown. Information gleaned from the breach could be used for other detrimental foreign policy objectives outside of cyberspace, or the threat actor could exploit its access to US government networks to engage in follow-on disruptive or destructive actions (in other words, conduct a cyberattack).

But what about the Department of Defense's new defend forward strategy, which was meant to fill in the gap where traditional deterrence mechanisms might not work? Some view this latest incident as a defend-forward failure because the Defense Department seemingly did not manage to stop this hack before it occurred. Introduced in the 2018 Defense Department Cyber Strategy, this strategy aims to "disrupt or halt malicious cyber activity at its source." This represented a change in how the Defense Department conceptualized operating in cyberspace, going beyond maneuvering in networks it owns, to operating in those that others may control. There has been some controversy about this posture. In part, this may be because defend forward has been described in many different ways, making it hard to understand what the concept actually means and the conditions under which it is meant to apply.

Here's our take on defend forward, which we see as two types of activities: The first is information gathering and sharing with allies, partner agencies, and critical infrastructure by maneuvering in networks where adversaries operate. These activities create more robust defense mechanisms, but largely leave the adversary alone. The second includes countering adversary offensive cyber capabilities and infrastructure within the adversaries' own networks. In other words, launching cyberattacks against adversary hacking groups—like threat actors associated with the Russian government. It isn't clear how much of this second category the Defense Department has been doing, but the SolarWinds incident suggests the US could be doing more.

How should the US cyber strategy adapt after SolarWinds? Deterrence may be an ineffective strategy for preventing espionage, but other options remain. To decrease the scope and severity of these intelligence breaches, the US must improve its defenses, conduct counterintelligence operations, and also conduct counter-cyber operations to degrade the capabilities and infrastructure that enable adversaries to conduct espionage. That's where defend forward could be used more effectively.

This doesn't mean deterrence is completely dead. Instead, the US should continue to build and rely on strategic deterrence to convince states not to weaponize the cyber intelligence they collect. That effort could start with better signaling that the US is serious about these responding to significant cyberattacks, including a frank conversation with Russian President Vladimir Putin, reminding him that while he may have scored an intelligence coup in SolarWinds, Russia is still overmatched in economic and military power by the US.


The SolarWinds incident reveals an important truth about our cyber strategy: The US should focus less on convincing adversaries not to conduct intelligence, and focus more on making these efforts less successful. This means investing more in defense and information sharing, but it also means making it more difficult for threat actors, like those affiliated with Russia or China, to conduct both cyber espionage and cyberattacks by “defending forward” to degrade these countries’ offensive cyber capabilities.

---

WIRED Opinion *publishes articles by outside contributors representing a wide range of viewpoints. Read more opinions [here](#), and see our submission guidelines [here](#). Submit an op-ed at [opinion@wired.com](mailto:opinion@wired.com).*

---

### More Great WIRED Stories

-  Want the latest on tech, science, and more? [Sign up for our newsletters!](#)
- The best pop culture [that got us through 2020](#)
- A race car crash from hell—and [how the driver walked away](#)
- These 7 pots and pans are [all you need in the kitchen](#)
- Hacker Lexicon: What is [the Signal encryption protocol?](#)
- The free-market approach [to this pandemic isn't working](#)
- 🎮 WIRED Games: Get the latest [tips, reviews, and more](#)
- ✨ Optimize your home life with our Gear team’s best picks, from [robot vacuums](#) to [affordable mattresses](#) to [smart speakers](#)