DAILY BEAST

NSA Opens Door to Domestic Internet Spying, Privacy Advocates Say

Spencer Ackerman

Mar. 29, 2021

The establishment of the NSA's twin, Cyber Command, also created a Chekhov's gun: broad access to the American internet. Now the SolarWinds hack has NSA's finger on the trigger.

The latest king-sized, disastrous hack into U.S. government and corporate data servers is prompting the head of the National Security Agency to suggest that a surveillance giant built to look at foreign threats might need even greater powers to spy on internet usage domestically.

Doing so, privacy advocates say, jeopardizes an already weakened four-decade old compromise of national-security surveillance. NSA access to the digital trails of U.S. persons and foreigners transiting domestic communications infrastructure is supposed to require a warrant from a secret court specifying specific suspected worrisome activity. But it's unclear how early detection of foreign-borne digital threats, particularly at scale, could operate within the same legal paradigm.

"Like clockwork," said Sen. Ron Wyden (D-OR), a member of the intelligence committee, "advocates of expanded surveillance are trying to exploit an intelligence failure."

"Like clockwork... advocates of expanded surveillance are trying to exploit an intelligence failure."

— Sen. Ron Wyden

Gen. Paul Nakasone, the director of the National Security Agency and its conjoined military twin Cyber Command (CYBERCOM), did not offer any such answers in recent congressional testimony about the devastating SolarWinds hack, in which malware inserted into IT software used by several U.S. government agencies resulted in data exfiltration that Microsoft's Brad Smith has called "the largest and most sophisticated" cybertheft yet. Instead, Nakasone highlighted to legislators what he described as a dangerous blindness in cyberspace created by holding the domestic internet off-limits to him.

"We truly need to look at the ability for us to see ourselves and right now it's difficult for us to see ourselves," Nakasone testified on Thursday to the Senate Armed Services Committee. Adversaries like China and Russia "are operating with increased sophistication, scope [and] scale, including operations that can end "before a warrant can be issued," he warned.

"If we have a problem where we only see our adversaries when they operate outside of their country and we don't see them when they operate inside our country it's very difficult for us to be

able to—to, as I say, connect those dots," Nakasone said. "That's something that—that the administration and obviously, others are addressing right now."

Nakasone didn't elaborate. As a general matter, he suggested "driv[ing] a better partnership between what the public needs and what the private sector can offer," particularly in terms of information sharing. But he left unspecified what form that would take.

The NSA insists that Nakasone, who caveated his testimony by saying that new internet-security authorities need "not necessarily" go to Fort Meade, was not sending up a trial balloon. "General Nakasone did not ask nor advocate for additional authorities for U.S. Cyber Command or NSA during his testimony, which he gave in his capacity as the commander of U.S. Cyber Command, and was clear in highlighting the domestic authorities of the FBI and DHS in cyber defense and incident response," said Charlie Stadtlander, an NSA spokesperson, who continued: "Any additional discussions on new authorities, policies, responsibilities, or laws fall within the purview of policymakers."

Stadtlander also pointed to a recent statement by a senior administration official: "We're not looking at additional authorities for any government agencies to do additional monitoring within the U.S. at this time."

Nakasone's observations come at a time when the government agency responsible for protecting the civilian internet, the Department of Homeland Security, appears to have thoroughly failed, creating the prospect of government overhauls.

Since 2015, NSA has shared information about potential threats with DHS, which then in turn routes it to private companies. That arrangement involves the government informing private entities of novel digital dangers, rather than actively receiving or outright collecting intrusion data from those American companies. The process is hardly without criticism—particularly as foreign-originated digital intrusions have only mounted in the six years since. In September, an inspector general's report described DHS making only "limited progress improving the overall quality of information it shares." Rather than spotting SolarWinds, DHS was one of the government agencies SolarWinds penetrated, to the point where former DHS acting secretary Chad Wolf had his emails snatched.

Nakasone did not testify that NSA or CYBERCOM was able to detect malicious campaigns like SolarWinds or Microsoft Exchange abroad before they entered American digital infrastructure, making it questionable whether expanding such detection across the domestic internet would be effective.

"The intelligence community already has visibility on the federal systems that were the primary targets of the SolarWinds hack, and they failed to spot it," said Julian Sanchez of the Cato Institute. "So it's unclear why we're discussing expanding their collection authority when the system hasn't even proven effective in their own backyard. SolarWinds is a particularly bad example to use to press this argument, because—as is often the case for the most sophisticated attacks—they used U.S. server infrastructure to mount the attacks and bespoke malware that's not going to trigger detection systems based on known malware signatures."

But suggesting a need for expanded access over the U.S. internet fits a long pattern from Fort Meade. When the Pentagon established CYBERCOM in 2010, it represented the Chekhov's gun of cybersecurity: while CYBERCOM's digital potency is unquestioned, longstanding

privacy concerns about government access to private data kept it focused away from nongovernmental domestic networks. The acceleration and impact of intrusions onto those networks is causing respected former officials to reach for the gun.

On Sunday, Robert Gates, the defense secretary who presided over CYBERCOM's founding, proposed "new arrangements giving [DHS] authority to use NSA's incomparable resources with appropriate structural and regulatory safeguards"—something that would entail giving a department responsible for immigration deportations and analysis of domestic extremists expansive access to American internet activity. NSA's former top attorney, Glenn Gerstell, told the *Washington Post* last week that it was unacceptable to consider this "a tough Fourth Amendment problem and we're going to have to pay the price of being online and let the Chinese, Russians, North Koreans and Iranians do whatever they want." In other words: NSA needs to be able to spy on Americans, too, if you all want to keep using the internet.

"We're being told to give them more authority and ignore that they've allowed their surveillance missions to take priority in the past."

— University of Colorado Law School's Amie Stepanovich

"We knew this was coming when CYBERCOM went to the NSA," said Amie Stepanovich, executive director of the Silicon Flatirons Center at the University of Colorado Law School. "They let their surveillance mission take priority over their information-assurance mission. Now we're being told to give them more authority and ignore that they've allowed their surveillance missions to take priority in the past."

A decade before CYBERCOM existed, a different threat prompted the NSA into outright violation of the 1978 Foreign Intelligence Surveillance Act (FISA): terrorism. Less than a month after 9/11, the NSA under Director Michael Hayden—a future hero of the #resistance to Donald Trump—began collecting Americans' domestic phone and internet communications data in bulk, in secret and without warrants. The panoply of warrantless surveillance activities, known as STELLAR WIND, stopped few terrorist attacks, but succeeded at loosening democratic constraints placed on the NSA after the 1970s revelations of widespread domestic spying. Several STELLAR WIND activities persist to this day.

"The federal government failed to catch the SolarWinds hackers in any of the nine federal agencies that were hacked, where it had full legal authority to monitor every bit of activity on its own networks," Wyden said. "The government spent more than $6 billion on [threat-detection software] EINSTEIN, which spectacularly failed to detect this hacking operation, years after GAO warned that the government needed to shore up the system to detect the use of novel malware and 'clean' servers. Congress needs to be focusing on how to shore up the government's cyber defenses and how to ensure that the government stops wasting taxpayer money on insecure software."