How the United States is Losing the Fight to Secure Cyberspace

Jared Bowman

(Postgraduate scholar, pursuing MA-Science Degree, National Security Studies – Information Protection and Security Concentration at the University of New Haven, West Haven, CT, USA)

Publication date: 17 January 2021

Note: The article reflects the opinion of the author and not necessarily the views of the Research Institute for European and American Studies (RIEAS)

Carl von Clausewitz was famous for his description of the changing character of warfare. As nation-states evolve over time, the manner in which war manifests itself has also evolved. To many Americans, the concepts of cyberwarfare and cyber espionage are mostly foreign. With the world of fiberoptic cables and technical jargon being less attractive as seeing a bomb blow up enemy combatants, many Americans, including those within the federal government, have often put cybersecurity concerns on the backburner. While the United States has some of the most innovative minds within the world of cybersecurity, our cybersecurity infrastructure is far inferior to that of some of our greatest adversaries (Forgotson & Gerard, 2021). This was proven true once again in December, when the cybersecurity firm FireEye discovered that hostile actors were able to hack into SolarWinds' cyber supply chain and upload malware onto tens of thousands of government computers, resulting in the worst breach of government data in years (Borghard, 2020).

For those unaware, a hacking group named Cozy Bear (APT29) hacked into the software supply chains of Solarwinds back in March 2020 (Dilanian et al., 2020). APT29 managed to plant a trojan horse into the software updates to a SolarWinds' network monitoring software called Orion. As the federal government, multiple state governments, and many private companies continued updating their Orion software, APT29, with the suspected backing and support of the Russian government, was able to manipulate these updates using malicious computer code (malware) in order to gain access to that network's contents (Craig Timberg, 2020).

To use an analogy, this type of attack would be the equivalent of a hacker implanting a virus into a regular iOS update. When someone goes to update their device that uses iOS, that virus travels with that update. Through this hypothetical iOS update, a hacker can create something called a 'God door', which would allow that hacker access to all of that individual's private data on their phone or computer. While the average person's iPhone may have embarrassing messages or pictures, APT29 managed to access sensitive public and private information, some of which belonged to the CDC, the Department of Justice, and others. Some of the information that was accessed could include medical records, personal identification information (including social security numbers), and government communications that may have contained classified information (Sanger et al., 2020).

The exact impact of this data breach is still being investigated. However, there are several things that we know so far. According to the New York Times, while this data breach had the Russian government's backing, hackers from APT29 launched their attack from servers within the United States. By hacking from servers within the United States, APT29 avoided many of the cyberdefenses set up by the Department of Homeland Security. These vulnerabilities allowed APT29 to operate more covertly than if they had attempted to deploy these attacks from foreign servers (Sanger et al., 2021). It is also possible that our focus on other domestic security priorities distracted national security officials from identifying this problem earlier. For example, while the government's emphasis on election security was critical and necessary, it may have inadvertently diverted attention and resources away from the now undeniable problem posed by not protecting these software supply chains (Sanger et al., 2021). Companies that were involved in prioritizing election security, such as Microsoft and FireEye, were among those that were breached in this supply chain attack.

Because of the ease in which APT29 accessed these critical supply chains, there has been vigorous debate as to what strategic implications this data breach may have on U.S. cybersecurity policy. Some experts, such as Dr. Benjamin Jenson at the U.S. Cyberspace Solarium Commission, have called for increased cyber deterrence through entanglement strategies and denial-based approaches (Jensen et al., 2020). However, cyber espionage, by its very nature, is extremely difficult to deter. The barriers to entering our critical cyber infrastructure are too low, and the incentives provided by having access to confidential material are too high (Newman, 2020). Thus, a more forceful and deliberate response must be taken by the federal government. First, the federal government must prioritize and routinely conduct security audits on all critical I.T. platforms. These audits would help find nefarious actors within these systems and provide direct feedback on whether our current security strategies are adequate (Newman, 2020). Obtaining the upper hand over these adversaries will only occur when I.T. experts have definitive facts to work with. Secondly, we must work closely with our allies overseas to develop a collective defense-dominated strategy designed to secure cyberspace more effectively. This partnership can be achieved by the United States signing on to the Paris Call for Trust and Security in Cyberspace, and also the Global Commission on the Stability of Cyberspace (Schneier, 2020). Both of these frameworks would provide the United States with an opportunity to provide better security throughout cyberspace (Schneier, 2020). These agreements would also accelerate innovation, economic progress, and cultural development by sharing and accessing newly secured information. A successful cybersecurity strategy necessitates having a multi-pronged approach that can address the problems posed by the Internet's decentralized nature while also allowing a digital space that is free enough to share and access information.

The unsecure nature of our current cybersecurity infrastructure has enabled hostile actors to infiltrate some of the most powerful institutions on the planet. The United States has faced many national security challenges in the past, but we have more than likely never faced a threat that is so inexpensive to create, yet so destructive in its potential. If the federal government fails to adapt to this new environment, the same technology that provides comfort to our daily lives as a pandemic rages may slowly become something that makes daily life impossible.

References

Borghard, E. (2020, December 17). Russia's Hack Wasn't Cyberwar. That Complicates US Strategy. Retrieved January 11, 2021, from https://www.wired.com/story/russia-solarwinds-hack-wasnt-cyberwar-us-strategy/.

Craig Timberg, E. N. (2020, December 14). Russian hack was 'classic espionage' with stealthy, targeted tactics. Washington Post. https://web.archive.org/web/20201214201505/https://www.washingtonpost.com/technology/2020/12/14/russia-hack-us-government/.

Dilanian, K., Lederman, J., Stelloh, T., &amp; Collier, K. (2020, December 15). Russian hackers breach U.S. government, targeting agencies, private companies.

https://www.nbcnews.com/news/us-news/russian-hackers-breach-u-s-government-effort-aimed-agencies-private-n1251057.

Forgotson, E., Morrison, R., Parkins, R., & Rosner, A. (Producers) (2021, Jan 3). *CBS Sunday Morning: The threats arising from the massive solarwinds hack* [Television broadcast]. CBS News.

Jensen, B., Valeriano, B., &amp; Montgomery, M. (2020, December 22). The Strategic Implications of SolarWinds. Lawfare. https://www.lawfareblog.com/strategic-implications-solarwinds.

Newman, L. H. (2020, December 16). Russia's Hacking Frenzy Is a Reckoning. Wired. https://www.wired.com/story/russia-hack-supply-chain-reckoning/.

Paris Call for Trust and Security in Cyberspace. Paris Call. (2018, November 12). https://pariscall.international/en/.

Sanger, D. E., Perlroth, N., &amp; Barnes, J. E. (2021, January 2). As Understanding of Russian Hacking Grows, So Does Alarm. The New York Times. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Sanger, D. E., Perlroth, N., & Schmitt, E. (2020, December 15). Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit. The New York Times. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

Schneier, B. (2020, December 23). The US has suffered a massive cyberbreach. It's hard to overstate how bad it is | Bruce Schneier. The Guardian. https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols.