The American Conservative

The Russian 'Cyber Pearl Harbor' That Wasn't

Sean Lawson and Brandon Valeriano

December 18, 2020

For almost three decades, we have awaited a mythical "cyber Pearl Harbor," the harbinger of digital doom that the U.S. cybersecurity community assumes to be inevitable. Strangely enough, some believe this cyber Pearl Harbor already happened twice within the last two months.

Though warnings of cyber Pearl Harbor emerged as early as 1991, former defense secretary Leon Panetta is perhaps best known for promoting the idea, warning in 2012 of an impending "cyber-Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation." Such a grand event would be tough to miss.

Last week, Sidney Powell, a one-time member of the president's legal team, continued to promote her conspiracy theory that the Venezuelans, the Chinese, and "other countries" had exploited voting machines to rig the election for President-elect Joe Biden. This fictitious "attack," she told Fox Business host Lou Dobbs, amounted to nothing less than "cyber Pearl Harbor." Apparently the rest of us just missed it.

Cybersecurity experts, including Christopher Krebs, the former head of the Cybersecurity and Infrastructure Security Agency who was fired by President Trump in November, have refuted these claims. Krebs called them "farcical" and "nonsensical." Officials have said there was no interference with voting machines of the kind claimed by Trump supporters and that the election was "the most secure in American history."

This week began with the news of cybersecurity breaches at a growing list of private companies and government agencies, including the Department of Homeland Security and even the Pentagon, perpetrated by APT29, the Russian SVR. Dubbed SolarWinds after the company whose software served as the vector for the intrusions, the scope of the operation and the fact that it impacted defense and intelligence agencies sparked an online debate as to whether it had constituted an "attack" on the United States. Others did not wait to learn the extent of the damage before declaring that the United States had been "hit with 'Cyber-Pearl Harbor.'" Senator Richard Durbin went so far as to call the hack "virtually a declaration of war."

National Review's Jim Geraghty implied that the United States missed the SolarWinds intrusions because it failed to take the 2015 Office of Personnel Management (OPM) breach at the hands of Chinese hackers seriously enough, focusing instead on Russian disinformation in the wake of that country's interference in the 2016 presidential election. The OPM incident, he said, "was widely described as the 'cyber Pearl Harbor' and yet…most Americans didn't notice."

Calling any of these incidents "cyber Pearl Harbor" is inaccurate at best and inherently dangerous. The impacts of the OPM and SolarWinds hacks in no way approximate the kind of death and destruction most often associated with the use of the "cyber Pearl Harbor" analogy. The whole point of a cyber Pearl Harbor is that we would not miss the significance of such a major catastrophe since it would lead to an inevitable reconstitution of the cyber security threat environment.

This continued use of doomsday rhetoric is dangerous because it distorts our understanding of the cyber threats we do face, the implications of real incidents when they occur, and our possible response options. As Director of National Intelligence James Clapper said in 2015, the OPM breach was representative of the real cyber threats we face not because it was the fulfillment of a long-awaited "cyber Armageddon scenario," but because it was not. It was not an "attack," he said, but an incident of the kind of cyber espionage we witness regularly. That the cyber domain is dominated by espionage and represents a wider intelligence contest demonstrates the continuing misapplication of strategic thought surrounding cyber security violations.

Five years later, it is still unhelpful to frame incidents like SolarWind as the arrival of digital apocalypse instead of another major incident of cyber espionage. Continued hyperbole surrounding every new cyber incident encourages the kind of craven misappropriation of fears of cyber doom by those who seek to inflate threats for political gain.

We do not know the scope of SolarWinds mainly because the domain has no conception of measuring impact. In an arena obsessed with battle damage estimates, the Department of Defense simply has no interest in measuring the impact of their operations and the utility of defend forward operations that provide little leverage against espionage operations.

The FY2021 NDAA contains the most significant cyber security legislation to date. Helping the government organize in order to deny operations in the cyber environment is a critical task. There are provisions for threat hunting, organizational coordination, and more funding for cyber operations to maintain and defend cyberspace. Yet the deeper challenge is how we defend against espionage.

The real lesson of Pearl Harbor is the desperation of Japan to preemptively eliminate the United States as a threat to Japanese operations in the Pacific and the U.S. intelligence failures that enabled the attack in the first place. Taking the analogy in the correct direction suggests that the U.S. needs to seek to deny attack options to prevent infiltrations such as the SolarWinds event. The U.S. also needs to do better of understanding the strategic motivations of our adversaries. In this case, being distracted by the possibility of a major hack during the 2020 election led to a comprehensive violation of almost every government agency.

Hyperbole needs to stop and rational consideration of the impact of the SolarWind operation will take time and sober thought, not instant hot takes. Infiltration and extracting information is not an act of war, but evidence of the typical espionage operations that are conducted against near peer adversaries. Denying future operations will require a sober assessment of how to enable the defense when the attacker has many attack options. This will likely not come solely through government action, but collaboration between industry, the private sector, and government agencies that provide for collective defense.

Sean Lawson is associate professor of Communication at the University of Utah and non-resident fellow at the Krulak Center at the Marine Corps University.

Brandon Valeriano is the Donald Bren Chair of Military Innovation at the Marine Corps University located at the Krulak Center. He also serves as a senior fellow at the Cato Institute and a senior advisor to the U.S. Cyber Solarium Commission.