In cyber espionage, U.S. is both hunted and hunter

axios.com/american-cyber-warfare-solarwinds-d50815d6-2e03-4e3c-83ab-9d2f5e20d6f5.html

January 27, 2021

Jan 27, 2021 - World

Zach Dorfman of the Aspen Institute, author of Codebook

Illustration: Eniola Odetunde/Axios

American outrage over foreign cyber espionage, like Russia's SolarWinds hack, obscures the uncomfortable reality that the U.S. secretly does just the same thing to other countries.

Why it matters: Secrecy is often necessary in cyber spying to protect sources and methods, preserve strategic edges that may stem from purloined information, and prevent diplomatic incidents.

> But when the U.S. is only portrayed as a victim of nation-state cyber activity and not as a perpetrator in its own right, it creates a false impression of the state of play and invites calls for vengeance that could prove misguided or self-defeating.

The big picture: The U.S. is stronger in cyberspace than any other country, with world-spanning digital snooping capabilities, buttressed by American technological ingenuity and some of the planet's most talented hackers and daring overseas operators.

> Yet hacking performed by the U.S. — or our Five Eyes allies — is artificially hidden from view. Not only do U.S. officials not disclose it, neither do most private threat intelligence firms (insofar as they have insight), for reasons of patriotism, pedigree and profit.

Generally, only foreign-owned private cyber firms like the Russia-based Kaspersky, the object of deep distrust by U.S. intelligence officials, have treated U.S. threat actors like others: by naming them, describing their targets, and detailing their tactics, techniques and procedures.

Between the lines: The greater visibility, and heated rhetoric, surrounding cyber operations targeting the U.S. leads to more ink being spilled on the subject, which, in an escalatory spiral, further raises the public temperature.

- Many within the halls of government — including in Congress, where most lawmakers are not regularly privy to classified information regarding U.S. government hacking — are also taking their cues from public reporting.
- That means U.S. officials are themselves absorbing, and then often further amplifying, this distorted view.

Even when officials do acknowledge American cyber spying, it's often in coded language or to describe a specific subset of U.S. actions.

> Officials will talk of "defending forward" — that is, U.S. activity meant to raise the costs for adversaries to be successful in cyberspace — rather than speaking clearly and frankly about cyber espionage for traditional intelligence collection purposes.

Yes, but: "Russia launched SolarWinds — the latest in a long series of hostile Russian cyber operations — not because the U.S. has engaged too proactively in cyberspace," Gary Corn, a former senior Cyber Command official, wrote in Lawfare. "Quite the opposite; it did so, very simply, because it could."

> The U.S.' own cyber operations neither explains nor justifies the actions or motivations of America's adversaries. But a clearer public understanding of what the U.S. does in cyberspace would mean a clearer understanding of what other countries are up to.

The most measured reactions to SolarWinds have therefore often come from top U.S. intelligence officials, who know too much about the country's own activities to pretend otherwise.

So while lawmakers like Sens. Dick Durbin (D-Ill.) and Mitt Romney (R-Utah) compared SolarWinds to a Russian act of war, current and former intel officials were more muted.

"Good on them, bad on us," said former acting CIA director Michael Morell to news of the Russian hack. Morell emphasized that SolarWinds appears to have "just" been espionage and not, apparently, some type of prelude to destruction.

- Paul Kolbe, a former senior CIA official, decried the “indignant howling” over SolarWinds in a provocative and clear-eyed essay in the New York Times.
- In a statement about the hack, CISA, FBI, NSA and ODNI also underlined their assessment that SolarWinds “was, and continues to be, an intelligence gathering effort.”

The bottom line: The question isn’t whether U.S. cyber operators are, for example, targeting major Russian government agencies, but how successful these ventures have been and continue to be.