Wall Street Journal (April 19, 2021)

In Punishing Russia for SolarWinds, Biden Upends U.S. Convention on Cyber Espionage

Administration said Moscow breached bounds of acceptable online spying with hack's size and attack on U.S. private sector

The Austin, Texas, headquarters of SolarWinds Corp., whose software was exploited by Russia to break into scores of computer networks at government agencies and companies.

By **Dustin Volz**

WASHINGTON—President Biden's decision this week to punish Russia for the SolarWinds hack broke with years of U.S. foreign policy that has tolerated cyber espionage as an acceptable form of 21st century spycraft, analysts and former officials said.

In announcing a suite of punitive measures against Moscow, including financial sanctions and diplomatic expulsions, the White House made clear its actions were in response to "the full scope of Russia's harmful foreign activities."

The administration specifically highlighted what it said was Russia's yearslong meddling in U.S. elections. It also said U.S. intelligence had "high confidence" that Russia's foreign intelligence service, the SVR, was behind last year's SolarWinds hack, which compromised at least nine federal agencies and about 100 private-sector organizations.

The administration said both campaigns were unacceptable and demanding of a forceful response.

The U.S. has punished Russia for election interference in the past, notably after its multipronged operations during the 2016 election. But previous administrations typically refrained from retaliating for cyber intrusions they classified as political espionage—no matter how broad or successful—in part because the U.S. and its allies regularly engage in similar conduct, current and former officials said.

Both the Obama and Trump administrations sought to forge international agreement that cyberattacks that stole intellectual property, damaged computer systems or interfered in elections were out of bounds—while generally accepting espionage as fair play. In 2015, for example, after the U.S. learned the Chinese had ransacked the federal government's personnel files and made off with sensitive records on more than 20 million Americans, James Clapper, then the director of national intelligence in the Obama administration, paid begrudging respect.
"You have to kind of salute the Chinese for what they did," Mr. Clapper said at the time. "If we had the opportunity to do that, I don't think we'd hesitate for a minute."

Western intelligence operations have also launched large cyber espionage operations against foreign private sectors, as the SolarWinds hack did, said Thomas Rid, an expert on Russian cyber operations and a professor at Johns Hopkins University.

Some U.S. officials advised the Biden administration not to justify sanctions specifically on the SolarWinds operation, as that move could open up the U.S. to foreign censure for its own activities, said people familiar with the situation.

"The hard question therefore is this: How was SolarWinds different from high-end Five Eyes intelligence operations?" asked Mr. Rid, referring to the name used for a cadre of Western intelligence powers.

Administration officials deemed the SolarWinds hack beyond the boundaries of acceptable cyber operations because of its scope and scale. A senior administration official said Thursday the retaliation was additionally justified because the burden of repairing the

damage largely fell on private companies and because Russia had shown in the past it can turn an espionage operation into something more destructive.

"The speed with which an actor can move from espionage to degrading or disrupting a network is at the blink of an eye, and a defender cannot move at that speed," the official said. "And given the history of Russia's malicious activity in cyberspace and their reckless behavior in cyberspace, that was a key concern."

Many Democrats, including Senate Majority Leader Chuck Schumer of New York, as well as Republicans praised the actions Mr. Biden took Thursday, and urged him to be even more forceful.

Others, however, were less sanguine. Rep. Jim Langevin (D., R.I.), a leading cybersecurity voice in Congress who generally praised Mr. Biden's actions against Russia, said the sanctions slapped on the SVR for the SolarWinds hack needed more explanation.

"The SolarWinds incident that the administration today attributed to the SVR has had all the trappings of traditional espionage that, while unfortunate, has not historically been outside the bounds of responsible state behavior," Mr. Langevin said. Mr. Biden and Secretary of State Antony Blinken should "explain the contours of their new policy," Mr. Langevin said.

"Most intrusions can be used for destructive ends," Mr. Painter said. Even if the attack was purely espionage, though, the U.S. is still within its rights to react "not to enforce a global norm but to demonstrate displeasure," he said.

In an analysis for the national security blog Lawfare, Bobby Chesney, a national security law professor at the University of Texas, said the Biden administration had not declared all cyber espionage is off limits. Rather, in announcing its response to Russia, the administration outlined a vague matrix of conditions that, if met, could elevate certain "malicious cyber activities" to a level that warranted retaliation, he wrote.

"Is it clear that there is an answer to the question of what line SolarWinds crossed?" Mr. Chesney asked. "Not really."