# Self-Delusion on the Russia Hack

thedispatch.com/p/self-delusion-on-the-russia-hack

Jack Goldsmith

## The U.S. regularly hacks foreign governmental computer systems on a massive scale.

Jack Goldsmith

Dec 18, 2020

(Photograph by M. Borchi/Getty Images.)

As the news about Russia's broad digital espionage operation against the U.S. Defense, Treasury, and Commerce Departments, nuclear laboratories, and other governmental systems grows more ominous, prominent voices are calling for a vigorous response. "[A]ll elements of national power," including military power, "must be placed on the table," proclaimed Thomas Bossert, the former senior cybersecurity adviser in the Trump administration, in a *New York Times* op-ed. The United States must "reserve [its] right to unilateral self-defense," and "allies must be rallied to the cause" since such coalitions will be "important to punishing Russia and navigating this crisis without uncontrolled escalation." Sen. Richard Durbin had a similar but pithier assessment: "This is virtually a declaration of war by Russia on the United States."

The lack of self-awareness in these and similar reactions to the Russia breach is astounding. The U.S. government has no principled basis to complain about the Russia hack, much less retaliate for it with military means, since the U.S. government hacks foreign government networks on a huge scale every day. Indeed, a military response to the Russian hack would violate international law. The United States does have options, but none are terribly attractive.

The news reports have emphasized that the Russian operation thus far appears to be purely one of espionage—entering systems quietly, lurking around, and exfiltrating information of interest. Peacetime government-to-government espionage is as old as the international system and is today widely practiced, especially via electronic surveillance. It can cause enormous damage to national security, as the Russian hack surely does. But it does not violate international law or norms.

As the revelations from leaks of information from Edward Snowden made plain, the United States regularly penetrates foreign governmental computer systems on a massive scale, often (as in the Russia hack) with the unwitting assistance of the private sector, for purposes of spying. It is almost certainly the world's leader in this practice, probably by a lot. The Snowden documents suggested as much, as does the NSA's probable budget. In 2016, after noting "problems with cyber intrusions from Russia," Obama boasted that the United States has "more capacity than anybody … offensively."

Because of its own practices, the U.S. government has traditionally accepted the legitimacy of foreign governmental electronic spying in U.S. government networks. After the notorious Chinese hack of the Office of Personnel Management database, then-Director of National Intelligence James Clapper said: "You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute." The same Russian agency that appears to have carried out the hack revealed this week also hacked into unclassified emails in the White House and Defense and State Departments in 2014-2015. The Obama administration deemed it traditional espionage and did not retaliate. "It was information collection, which is what nation states—including the United States—do," said Obama administration cybersecurity coordinator Michael Daniel this week.

Some argue that it is time to end this accepting attitude. This seems to be President-elect Joe Biden's view. "A good defense isn't enough; we need to disrupt and deter our adversaries from undertaking significant cyberattacks in the first place," he said yesterday. But this is much easier said than done, even beyond the hypocrisy in punishing others for doing to us what we do to them. The main lawful options—economic sanctions, criminally charging and trying to arrest those involved, recruiting adversary hackers, and the like—have been tried for years in related contexts, and failed to stop the digital carnage. Anything more than these rather modest retaliatory steps threatens an escalatory response by the Russians that might leave the United States—deeply dependent on weakly defended digital networks—in a more vulnerable position. This in a nutshell is why the Obama administration was so paralyzed in responding to various cyber intrusions.

The Trump administration overcame these worries and asserted a more aggressive posture that is called “Defend Forward.” The basic idea is that U.S. Cyber Command will maintain a persistent presence in adversary governmental networks so that it can “confront our adversaries from where they launch cyber attacks,” as NSA Director Paul Nakasone put it. Defend Forward was deemed a success in preventing interference in the 2018 and 2020 elections. But it utterly failed to even detect the recent Russia hack. It is not hard to see why. Even Cyber Command has limited resources. It cannot monitor, detect and prevent all possible major cyber threats.

But there are other problems with Defend Forward as a potential response to the Russia hack. It requires the United States to do the very thing it is trying in part to prevent—massive spying inside government networks. And it requires an additional and more controversial step beyond mere espionage: disruption of the adversary system to stop the attack before it succeeds. In 2018, this involved shutting down the Russian Internet Research Agency’s internet access.

This additional step is legally much more contestable than mere espionage. And more importantly, now that the United States has widely touted this practice, nothing in principle prevents other countries from engaging in analogous disruptions in our systems following extended espionage. Some worry that the Russian presence in U.S. networks “might allow them to conduct destructive attacks or change data inside government systems.” But this is very much like what Defend Forward purports to do in order to prevent attacks on the United States.

The United States has spent “billions of dollars to assemble the world’s most potent arsenal of cyberweapons and plant them in networks around the world,” as the *New York Times* reported last year. It also reported that that as part of Defend Forward, the United States had deployed “potentially crippling malware” inside the Russian electric grid and other Russian computer systems, “at a depth and with an aggressiveness that had never been tried before,” in order to warn and deter the Russians for meddling in our computer systems. This effort at deterrence appears not to have worked, but it highlights the dangers of Defend Forward. The United States and Russia have been involved in escalating tit-for-tat cyber operations against one another for a long time. Perhaps this year’s Russians hack is in part a responsive “defend forward” operation to warn and deter the United States from further action. It is hard to know where we are in the retaliatory cycle, but it is pretty clear that the United States has more to lose from escalating retaliation.

The larger context here is that for many reasons—the Snowden revelations, the infamous digital attack on Iranian centrifuges (and other warlike uses of digital weapons), the U.S. “internet freedom” program (which subsidizes tools to circumvent constraints in authoritarian networks), Defend Forward, and more—the United States is widely viewed abroad as the most fearsome global cyber bully. From our adversaries’ perspective, the United States uses its prodigious digital tools, short of war, to achieve whatever advantage it can, and so adversaries feel justified in doing whatever they can as well, often with fewer scruples. We can tell ourselves that our digital exploits in foreign governmental systems serve good ends, and that our adversaries' exploits in our systems do not, and often that is true. But this moral judgment, and the norms we push around it, have had no apparent influence in tamping down our adversaries' harmful attacks on our networks—especially since the U.S. approach to norms has been to give up nothing that it wants to do in the digital realm, but at the same time to try to cajole, coerce, or shame our adversaries into not engaging in digital practices that harm the United States.

Despite many tens of billions of dollars spent on cyber defense and deterrence and Defend Forward prevention, and despite one new strategy after another, the United States has failed miserably for decades in protecting its public and private digital networks. What it apparently has not done is to ask itself, in a serious way, how its aggressive digital practices abroad invite and justify digital attacks and infiltrations by our adversaries, and whether those practices are worth the costs. Relatedly, it has not seriously considered the traditional third option when defense and deterrence fail in the face of a foreign threat: mutual restraint, whereby the United States agrees to curb certain activities in foreign networks in exchange for forbearance by our adversaries in our networks. There are many serious hurdles to making such cooperation work, including precise agreement on each side's restraint, and verification. But given our deep digital dependency and the persistent failure of defense and deterrence to protect our digital systems, cooperation is at least worth exploring.

*Jack Goldsmith is Henry L. Shattuck professor of law at Harvard University and a senior fellow at the Hoover Institution at Stanford University.*