Deterring Cyberattacks from Russia and China in the Era of Digital Great Power Competition

Alyza Sebenius and Brittany Carter

When President Joe Biden took office, the new administration's cyber team had its work cut out. A month earlier, in December 2020, a cybersecurity company had discovered a sprawling attack on the United States of America, in which Russian hackers[1] compromised widely-used SolarWinds software, delivering malicious software updates to as many as 18,000 software users, and breaking into 100 American companies as well as nine American agencies.[2] The breach of the federal government through SolarWinds' software was a widespread and sophisticated hacking campaign that prompted changes to policy and operations in a heightened effort to rid foreign entities from federal networks. But the task of removing Russian hackers from federal networks was only the beginning for the new administration. In a separate cyber campaign discovered in March, Chinese attackers[3] exploited vulnerabilities in Microsoft's Exchange Server for email to hack tens of thousands of organizations.[4]

These incidents were anything but isolated. Cyberattacks by adversaries, competitors, and criminals have been, for years, an all-too common feature of the American digital landscape. Importantly, however, the recent attacks also serve as a reminder that the renewed great power competition that the United States faces with China and Russia has a critical cyber dimension. While it is clear that deterring attacks on American networks is crucial to addressing China's rise and Russia's renewed aggression, viewing the cyber threat in terms of great power competition may also provide a mechanism for bridging the partisan divide in order to legislate and govern in a manner that protects American networks.

The intelligence community has been clear on the cyber threat posed by these powers. "China's cyber pursuits and proliferation of related technologies increase the threats of cyberattacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its internal ideological control, and the expansion of technology-driven authoritarianism around the world," Biden's Director of National Intelligence (DNI) Avril Haines wrote in April.[5] "Moscow will continue to employ a variety of tactics this year meant to undermine U.S. influence, develop new international norms and partnerships, divide Western countries and weaken Western alliances, and demonstrate Russia's ability to shape global events as a major player in a new multipolar international order." This assessment echoed President Donald Trump's DNI Daniel Coats who wrote in 2019 that "at present, China and Russia pose the greatest espionage and cyberattack threats."[6]

While recent administrations have been significantly divided on many ideological and national security issues, these assessments nevertheless reflect intelligence consensus on the contours of the cyber threat. Even so, cyber has been a politically charged topic: after the American intelligence community found that Russia interfered in the 2016 election to Donald Trump's benefit and to Hillary Clinton's detriment,[7] President Trump cast doubt on the finding.[8] In the wake of Russia's election meddling and the domestic fallout in America, protecting U.S. elections became a key–and politically fraught–cybersecurity priority. However, zooming out and reframing American cybersecurity in terms of broader geopolitical threats to the homeland can be both a source of common ground for politically divided Americans as well as a strategically beneficial vantage point from which to approach the growing cyber threat.

In order to come together to combat the cyber threat, law and policy makers should approach the defense, deterrence, and retaliation against Russia and China in cyberspace through the lens of great power competition. This is a promising strategy given that there is already a consensus in Washington that great power competition is once again defining America's role in the world.

Both of the recent administrations have described this reality in their national security strategies. "China and Russia want to shape a world antithetical to U.S. values and interests," the Trump administration wrote in its 2017 National Security Strategy.[9] It went on to warn that the two countries "are contesting our geopolitical advantages and trying to change the international order in their favor."[10] Correspondingly, the Biden administration's interim National Security Strategic Guidance, published in March 2021, described challenges posed by "an increasingly assertive China and destabilizing Russia."[11] The following month, the White House elaborated on a call with reporters: "The past two administrations chose to focus on what they saw as the predominant national security challenges facing the country: transnational threats in one instance, and great power competition in the other," a Biden official explained. "Our view is that we don't have that luxury to choose between those challenges."[12]

In Congress, efforts to frame the cyber threats from Russia and China in terms of great power competition–coupling the commonalities in understanding the threat posed by their hackers and elements of shared understanding on the geopolitical threat posed by the two countries–have been productive. For example, the Cyberspace Solarium Commission, a bipartisan group of lawmakers, intelligence officials, and others, published a 2020 report that sought to find a "consensus" on how the United States should strategically defend itself from major cyberattacks.[13] Many of its recommendations–which ranged from government reorganization, to setting international norms, and building collaboration among the public and private sector–have been implemented, including through legislation and executive order.[14] With respect to Russia and China, the commission framed the issue in terms of the broader geopolitical struggle: "Great powers like China and Russia use cyber operations to enable their warfighting capabilities, advance their interests short of armed conflict, and undermine American economic strength, political will, and military might."[15]

To be sure, the cyber threat transcends Russia and China. The United States has suffered significant cyberattacks from North Korea, Iran, and non-state actors. In a vivid example of the power of cybercriminals, Russian-based criminals[16] conducted a ransomware attack on Colonial Pipeline last year, raising gas prices as it caused fuel shortages along the East Coast of the U.S.[17]

Yet, the intelligence community has made it clear that Russia and China are the prevailing priorities and that the U.S. will not be safe until these countries are convinced that the benefits of attacking American infrastructure are not worth the costs. This means a combination of network defense, imposing costs on bad actors, and a concerted bipartisan effort to integrate the U.S. cyber strategy into its renewed approach to great power competition. Reframing the cybersecurity competition with Russia and China in terms of great power competition will allow the United States to sidestep partisan differences. Furthermore, it may also be a unifying first step that leads to a greater strategic emphasis on American defense, deterrence, and retaliation in cyberspace.

Major Brittany S. Carter is the Chief of Air Force Cyber Programs and Weapon Systems within the Secretary of the Air Force (SECAF) Legislative Liaison directorate.

Alyza Sebenius is a current law student at Harvard University. She previously wrote about the intersection of foreign policy and technology as a cybersecurity reporter for *Bloomberg News*.

[1] The White House attributed this hack to Russia's Foreign Intelligence Service, saying that "the scope of this compromise is a national security and public safety concern. Moreover, it places an undue burden on the mostly private sector victims who must bear the unusually high cost of mitigating this incident." See "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government," The White House, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[2] Alyza Sebenius, "Biden's Security 'Dream Team' Has a Nightmare First Assignment," *Bloomberg News*, February 24, 2020, https://www.bloomberg.com/news/articles/2021-02-17/solarwinds-hacks-perpetrated-from-inside-u-s-white-house-says.

[3] The Biden Administration, along with U.S. allies attributed this attack to China's Ministry of State Security, saying "MSS-affiliated cyber operators exploited these vulnerabilities to compromise tens of thousands of computers and networks worldwide in a massive operation that resulted in significant remediation costs for its mostly private sector victims." See: "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," The White House, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

[4] Alyza Sebenius, “Microsoft Server Flaws Raise Alarms at White House, DHS,” *Bloomberg News,* March 5, 2021, https://www.bloomberg.com/news/articles/2021-03-05/microsoft-server-flaws-raise-alarms-at-white-house-dhs.

[5] “Annual Threat Assessment of the U.S. Intelligence Community,” Office of the Director of National Intelligence, April 9, 2021.

[6] “Annual Threat Assessment of the U.S. Intelligence Community,” Office of the Director of National Intelligence, January 29, 2019.

[7] “Assessing Russian Activities and Intentions in Recent U.S. Elections,” Office of the Director of National Intelligence, January 6, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

[8] For example, in a 2018, press conference with Russian president Vladimir Putin in Helsinki, President Trump said of the attack on the 2016 elections: “My people came to me—[DNI] Dan Coats came to me and some others—they said they think it’s Russia. I have President Putin; he just said it’s not Russia. I will say this: I don’t see any reason why it would be.”

[9] “National Security Strategy of the United States of America,” The White House, December 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[10] Id.

[11] “Interim National Security Strategic Guidance,” The White House, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[12] “Background Press Call by Senior Administration Officials on National Security and Foreign Policy in President Biden’s First 100 Days,” The White House, April 27, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/04/27/background-press-call-by-senior-administration-officials-on-national-security-and-foreign-policy-in-president-bidens-first-100-days/.

[13] Alyza Sebenius, “U.S. ‘Dangerously Insecure’ in Preparing for Major Cyber-Attacks,” *Bloomberg News,* March 3, 2020, https://www.bloomberg.com/news/articles/2020-03-11/u-s-dangerously-insecure-in-preparing-for-major-cyber-attacks.

[14] “2021 Annual Report on Implementation,” United States of America Cyberspace Solarium Commission, August 2021, https://www.solarium.gov/public-communications/2021-annual-report-on-implementation

[15] Final Report, United States of America Cyberspace Solarium Commission, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view and https://www.solarium.gov/.

[16] As President Biden explained, “We do not believe—I emphasize, we do not believe the Russian government was involved in this attack. But we do have strong reason to believe that criminals who did the attack are living in Russia. That’s where it came from—were from Russia.” See “Remarks by President Biden on the Colonial Pipeline Incident,” The White House, May 13, 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/.

[17] Alyza Sebenius and Ryan Gallagher, “Colonial Hacker Group Seeks to Shift Blame for Ransomware,” *Bloomberg News,* May 9, 2021, https://www.bloomberg.com/news/articles/2021-05-10/white-house-creates-task-force-to-deal-with-pipeline-breach.