The Case for Cyber-Realism: Geopolitical Problems Don't Have Technical Solutions

Published in: Foreign Affairs, 2022, Gale General OneFile

In September 2015, U.S. President Barack Obama stood beside Chinese President Xi Jinping in the White House Rose Garden and announced a historic deal to curb cyber-related economic espionage. The scope of the agreement was modest, committing China and the United States only to stop stealing or aiding in the cyber-enabled theft of intellectual property in order to boost domestic industry. It was an easy promise for the United States to make, since Washington had long prohibited U.S. intelligence services from conducting economic espionage for the benefit of private companies. But it was a groundbreaking pledge for China, whose military and intelligence agencies had for more than a decade engaged in massive cyber-enabled theft of U.S. intellectual property and state secrets in order to advantage Chinese companies.

The agreement was equally ground-breaking because of how it came about. In the weeks leading up to the Rose Garden ceremony, Obama had threatened to sanction Chinese companies and citizens who continued to target U.S. companies with cyberattacks or exploit stolen intellectual property for commercial gain. These threats, the first that an American president had ever issued in response to Chinese economic espionage, were calibrated to address not just Chinas cyber-activities but also its broader economic and strategic objectives. "We are preparing a number of measures that will indicate to the Chinese that this is not just a matter of us being mildly upset, but is something that will put significant strains on the bilateral relationship if not resolved," Obama told business leaders the week before Xi's visit. "We are prepared to take some countervailing actions in order to get their attention."

Initially, the agreement was a limited success. Intrusions from Chinese government-affiliated groups dropped to their lowest level in over a decade in 2016. And for the next two years, American companies enjoyed a brief respite from what had previously been an unrelenting assault by Chinese military- and intelligence-affiliated hackers. But the detente was short-lived. In 2018, U.S. President Donald Trump launched a trade war that undercut the United States' economic leverage over China and reduced Beijing's incentives to adhere to the pa

Later that same year, the National Security Agency accused China of violating the agreement, and the U.S. Justice Department proceeded to indict Chinese hackers on charges of cyber-enabled economic espionage. The Trump administration threatened to impose broad sanctions on Chinese companies, but it ultimately sanctioned only a few firms.

Although it failed in the end, the 2015 agreement between Obama and Xi offers a promising model for addressing cyberthreats. Until recently, the United States has tended to approach issues related to cyberspace as a narrow set of technical problems to be solved primarily with a combination of defensive and limited deterrence measures. Those defensive efforts have included funding the modernization of technology, regulating industries involved in critical infrastructure, and improving collaboration and information sharing between the government and industry. Deterrence has typically involved punitive actions by law enforcement or sanctions against individual perpetrators or their affiliated military and intelligence agencies. After North Korean hackers breached Sony Pictures in 2014, for instance, the United States sanctioned individual North Korean officials and indicted three North Korean intelligence operatives. Russia's interference in the 2016 U.S. presidential election occasioned a similar response: Washington imposed sanctions on Russian intelligence agencies, indicted Russian military officers, expelled Russian intelligence officers operating under diplomatic cover, and shut down several Russian facilities located in the United States. The United States has also sought to deter adversaries by threatening to take the offensive and carry out retaliatory cyberattacks. Yet despite all these steps, neither North Korea nor Russia--nor any other U.S. adversary, for that matter--has ceased targeting the United States.

That is because vulnerability to cyberattacks is not a technical problem that hardened defenses or narrow, cyber-focused deterrence can fix. Cyberattacks are a symptom, not a disease; the underlying conditions are broader geopolitical problems that demand geopolitical solutions--namely high-level negotiations with adversaries in the pursuit of agreements that all parties can live with.

As the range of cyberthreats multiplies and the frequency and severity of attacks increase, Washington needs a dose of cyber-realism. It must treat cyberthreats as a geopolitical and national security priority that demands hard-nosed diplomacy--backed by all of the United States' tools for gaining leverage--to entice or threaten U.S. adversaries into changing their behavior, as Obama did in 2015. The specific carrots and sticks will need to be tailored to

each adversary, taking into account its unique geopolitical ambitions. But the sticks will have to include more aggressive deterrence, aimed not just at the hostile military and intelligence agencies that perpetrate cyberattacks but at the regimes to which those agencies answer. Cyberspace is not an isolated realm of its own, after all, but an extension of the broader geopolitical battlefield.

DEFENSE AND DETERRENCE

For most of the last three decades, U.S. cybersecurity policy and cyberstrategy have treated cyberattacks as if they emerged from the ether, unconnected to the geopolitical conflicts and competitions that structure the global security order. As a result, much of U.S. cyberstrategy has focused on managing the effects of cyberattacks through defense and narrow deterrence of actors in cyberspace rather than addressing the causes of cyberattacks.

Defensive measures can be either proactive or reactive, seeking to protect networks from intrusions or to trying to limit the damage when intrusions inevitably occur. But neither of these types of defensive measures has proved equal to the increasing cyberthreat--as Russia's recent and extensive hack of U.S. government networks via network-monitoring software made by the Texas-based company SolarWinds, among other major incidents in cyberspace, has made clear. Attackers have an inherent advantage in cyberspace: when the cost of each attempted hack is low and the penalties are effectively nonexistent, hackers seeking to infiltrate even hardened targets can afford to spend months and sometimes years trying to find a way in. That asymmetric advantage makes aggressors quite likely to succeed eventually, since they need to get lucky only once, whereas defenders must discover and stop each hacking attempt.

Even if the U.S. government could sufficiently harden its own defenses, moreover, it would not be able to prevent all or even most cyberattacks, many of which are directed against smaller entities, such as schools, hospitals, police departments, small businesses, and nonprofit organizations, which have neither the resources nor the knowledge to implement complex cybersecurity strategies. These organizations will have little chance of fending off sophisticated cyberattacks from hostile countries no matter how effective U.S. government defenses become.

Deterrence, as it has traditionally been practiced, has been similarly ineffective at preventing cyberattacks. In the past four years, the U.S. government has sanctioned and indicted government officials and contractors from all its four primary adversaries: China, Iran, North Korea, and Russia. Yet these states regard the cost of such measures as relatively minor, and they continue to carry out or condone cyberattacks at an unrelenting pace. More aggressive sanctions that would threaten the underpinnings of economic growth in these countries, such as sanctions against industrial national champions, would likely achieve a greater effect. But because the United States does not approach these attacks in their broader geopolitical contexts, it has failed to mount appropriately tailored responses.

On occasion, the United States has gone on the cyberoffensive. Ahead of the 2018 U.S. midterm elections, for instance, U.S. intelligence agencies sought to disrupt the Internet Research Agency, Russia's infamous Internet troll factory. Such offensive measures have occasionally succeeded on a tactical level, impeding or slowing adversaries' attacks for a time. But they have done nothing to change the basic calculus of U.S. adversaries in cyberspace or to make the United States less vulnerable to cyberattacks in the long term.

THE GEOPOLITICS OF CYBERSPACE

The vast majority of cyberattacks against U.S. entities, whether by criminal groups or governments, emanate from the four countries--China, Iran, North Korea, and Russia--that also pose the greatest conventional military threats to the United States. To effectively counter the cyberthreat from these countries, Washington must consider their broader geopolitical goals.

China is the United States' most formidable adversary in cyberspace, as well as in the conventional military domain. It has made no secret of its ambition to surpass the United States as the world's leading economic and military superpower, and its activities in cyberspace follow logically from this goal. The vast majority of Chinese cyberattacks are instances of traditional and economic espionage. Between 2010 and 2015, for instance, state-sponsored Chinese hackers systematically targeted U.S. and European aerospace companies, stealing valuable information that China then funneled to its state-owned aerospace manufacturers. This hacking campaign was an enormous success; by the time it was discovered, in 2018, Chinese manufacturers had already built commercial jets based in part on the stolen intellectual property.

China's cyber-espionage has been especially aggressive in sectors that Beijing deems critical to its economic and national security objectives. Last July, for instance, the National Security Agency, the FBI, and the Cybersecurity and Infrastructure Security Agency released a joint report warning that Beijing-linked hackers were continuing to target U.S. companies and institutions in strategically important areas, including defense and semiconductor firms, medical institutions, and universities. Compared with other U.S. adversaries, however, China has engaged in relatively little cybercrime and has carried out few destructive cyberattacks. This, too, fits with China's broader strategic agenda, since such activities could undercut China's standing on the international stage.

Russia has its own set of geopolitical goals that its cyber-activities aim to advance. Like Beijing, Moscow is motivated by a pugilistic sense of national pride. But unlike China, Russia does not have the economic capacity to compete with the United States. It is increasingly isolated internationally and struggles to maintain its influence in its so-called near abroad. Nevertheless, it is striving to retain its status as a great power, a goal that its leaders believe they can achieve by strengthening their position at home while undercutting the reputation of the United States and its allies and frustrating their international ambitions.

Like its Soviet predecessor, the Russian government carries out traditional spying and economic espionage. Today's Kremlin uses both cybertools and conventional means for this purpose. But Russia's cyber-activities also focus on sowing political and economic turmoil in the West, undercutting Westerners' faith in democratic government, and weakening the influence of Western countries in Russia's neighborhood. Moscow's interference in the 2016 U.S. presidential election, its 2017 malware attack that took down networks in Ukraine before spreading around the world, and its 2018 hack of the International Olympic Committee all served this broader agenda.

The same is true of Russian ransomware attacks, which, despite being carried out by criminal gangs, represent an important part of the Kremlin's strategy. The cybercriminals that have targeted thousands of U.S. organizations and extracted over $1 billion in ransoms in recent years have sometimes been protected by Russian security forces, and regardless, the Kremlin's refusal to crack down on them amounts to a tacit endorsement of their activities. Although cybercrime does not advance Russia's core national interests, it does serve a strategic purpose: disrupting the U.S. economy and sowing fear among American business leaders. Cybercriminals are also valuable bargaining chips in international negotiations:

Russia can offer action against ransomware gangs in exchange for important concessions, without having to address its more strategically important, state-sponsored cyber-activity.

The United States' other two major adversaries, Iran and North Korea, have also used cybertools to advance their domestic and international goals, although less ably than China and Russia. Both countries have done so primarily to circumvent Western sanctions that are squeezing their domestic economies. The North Korean regime has financed itself with tens of millions of dollars accumulated through cybercrime, and Iran has used cyber-enabled economic espionage to get around Western sanctions on defense technologies, petrochemical production, and other strategic sectors. Both countries have also used cyberattacks to weaken their regional rivals, with North Korea launching attacks against South Korea and Iran targeting Israel and Saudi Arabia.

GRAND BARGAINS

Better defensive measures might help insulate U.S. government agencies, private U.S. companies, and individual Americans from the consequences of major cyberattacks carried out by these U.S. adversaries. But neither defense nor deterrence as it is currently practiced can mitigate these threats on its own. Washington's capabilities might improve, but so, too, will those of its rivals.

To halt China's malign cyber-activity, the United States and its allies will have to convince Beijing to make a deal. In exchange for a de-escalation of the trade war, Beijing might agree to remove market-distorting industrial subsidies, halt the forced transfer of technology, and curb intellectual property theft. Likewise, if the United States wants to check Russia's nefarious cyber-activities, it will need to ease Moscow's concerns about U.S. interference in Russian domestic and regional affairs. Addressing the cyberthreat from Iran and North Korea will similarly require making progress on negotiations over their respective nuclear programs, which are by far the most pressing concern for both countries.

This might seem like cause for gloomy fatalism about the chances of resolving issues related to cyberspace. In fact, the opposite is true. Like all complex geopolitical challenges, cyberthreats can be addressed using the right combination of incentives, disincentives, and compromises. The question for the United States and its allies is whether they are willing to prioritize progress on issues in cyberspace over progress on other geopolitical objectives.

and what they are willing to give up for the sake of that progress. Considering the recent slew of major ransomware attacks and supply chain hacks, the Biden administration must urgently answer that question. Then it must back up its rhetoric on cyberspace with hard-nosed diplomacy that can change its adversaries' behavior.

Part of what it will take to force these countries to make a deal will be broader deterrence, including measures that raise the costs to hostile regimes of carrying out cyberattacks while denying them the benefits of doing so. In addition to military and spy agencies, the United States should sanction and prosecute companies and executives in countries, such as China, that benefit from cyber-enabled economic espionage, sending the message that the theft of intellectual property and trade secrets comes at a hefty price. Since anonymous cryptocurrency transfers now fuel so much global cybercrime, the United States should also work with its allies to sanction and shut down cryptocurrency exchanges that cater to criminal operations or that do not perform due diligence on the transactions they facilitate.

To be sure, as long as grand bargains remain elusive, the United States will have to harden its defenses and make itself more resilient. The U.S. government has a poor record on cybersecurity, so it needs to step up its game and lead by example--for instance, by centralizing all civilian cybersecurity operations within the Cybersecurity and Infrastructure Security Agency. It must also incentivize public and private investment in defensive measures, including by subsidizing the costs of defense for municipalities, nonprofits, and small businesses and by holding companies that do not take responsible security measures accountable for negligent failures. Although these measures can only ever be a partial fix, they can limit the damage done by hackers and other cybercriminals until Washington can forge a more lasting diplomatic solution.

When the United States faces a military threat from a hostile nation, it does not tell its citizens and businesses to fund their own private armies or to negotiate their own peace deals. Many cyberthreats are not meaningfully different from military or economic threats, and yet the United States allows much of the burden of defending against them to fall on individual companies and citizens. In the short term, the United States must do more to harden its defenses and to help companies and citizens do the same. Ultimately, however, Washington must accept that cyberattacks are primarily an effect, and not a cause, of geopolitical tensions. Unless the United States treats the underlying disease, it will never fully recover from the symptoms.

~~~~~~~~

By Dmitri Alperovitch

DMITRIALPEROVITCH is Co-Founder and Chair of Silverado Policy Accelerator and Co-Founder and former Chief Technology Officer of the cybersecurity firm CrowdStrike.

~~~~~~~~