Russian Threats and Cybersecurity

Beth George | May 13, 2022

Beth George is a Non-Resident Senior Fellow at the Reiss Center on Law and Security at NYU School of Law. She is a partner in the Silicon Valley Office of Freshfields Bruckhaus Deringer, where she leads the strategic risk and crisis management practice. Previously, she was a partner in the San Francisco office of Wilson Sonsini Goodrich & Rosati, where she led the firm's cybersecurity team. Beth served as Acting General Counsel of the Department of Defense in the Biden-Harris Administration. For her work, she was awarded the Department of Defense Medal for Distinguished Public Service, the highest honor the Department of Defense awards to civilians. Previously, Beth served as the Deputy General Counsel at the Department of Defense, as an Associate Counsel in the Office of the White House Counsel, and in various roles at the National Security Division of the Department of Justice.

Should we expect to see an increase in Russian cyber-attacks against the United States and other countries providing support to Ukraine as the crisis draws on? If so, what kinds of attacks would you predict we'll see, and do you think potential targets—particularly private companies—are sufficiently prepared?

Since the earliest days of the Russian invasion of Ukraine, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has been issuing prominent warnings about the potential for an increase in Russian attacks against U.S. companies. They launched a campaign called "Shields Up" to provide warning and guidance to companies regarding potential Russian threats.

Interestingly, in the private sector, what we noticed around the time of the Russian invasion was a decrease in attacks that cybersecurity professionals generally attributed to Russian state-sponsored and state-affiliated hacking organizations, particularly regarding ransomware. Last fall, ransomware attacks appeared to be at their highest, with attacks against private companies happening on a routine basis, although many of the attacks were not existential for the company involved or didn't compromise major systems. (Anecdotally, in October 2021, multiple forensic companies I work with reported that they were at capacity for ransomware attacks and were unable to take on additional clients.) But by the time of the invasion, ransomware attacks had significantly dropped off, and those of us who work in the private cybersecurity sector remarked quietly among ourselves that it was disconcertingly quiet. It is unclear—at least based on publicly available information—whether this is related to Russian state-sponsored and state-affiliated hackers focusing their efforts on the war in Ukraine or if there has been some other type of disruption in their operations, perhaps due to efforts by the U.S. government to address ransomware gangs.

Regardless of how quiet it has generally been for the U.S. private sector in the past few months, Russia is clearly not out of the hacking game. Earlier this week, the U.S. and U.K. governments formally attributed an attack against ViaSat – a private internet satellite company—to the Russian government. In that case, the attack appeared largely intended to disrupt Ukrainian military activity, but it has secondary effects in several countries including, for

example, disabling remote access to thousands of German windmills that relied on the same technology.

As to whether private companies are sufficiently prepared for Russian cyber operations, the reality is that it is incredibly difficult for companies to pivot quickly to protect themselves from sophisticated state sponsored attacks. Building cybersecurity controls is a multi-year, and, in some cases, multi-million dollar investment. For companies that have underinvested in cybersecurity for years, getting basic controls in place to prevent or mitigate an attack is not something that can be done in a matter of days or weeks. That said, CISA is doing an excellent job of putting out information about known, exploited vulnerabilities putting out industry-specific and actionable threat intelligence. All companies would be well-advised to review CISA's public guidance and digest it into their cyber risk management processes.

"[T]he reality is that it is incredibly difficult for companies to pivot quickly to protect themselves from sophisticated state sponsored attacks. Building cybersecurity controls is a multi-year, and, in some cases, multi-million dollar investment."

How serious are the potential threats to critical infrastructure in the United States from hostile cyber operations, and do you anticipate Russia targeting U.S. critical infrastructure?

There have been efforts across multiple administrations to raise awareness of cybersecurity threats to critical infrastructure, to share threat information with companies that own or operate critical infrastructure, and to improve private-public partnerships to further harden and protect these companies. Most recently, on Mar. 15, 2022, President Biden signed into law the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (within the Consolidated Appropriations Act), which will require entities determined to be critical infrastructure to report substantial cyber incidents within 72 hours and ransomware payments within 24 hours to CISA. But it's unlikely that it will have an impact any time soon—the statute allows the CISA director until September 2025 to establish implementing regulations. And because passage of the bill was strongly criticized by the Department of Justice and the FBI, there could be significant interagency fighting about the scope and content of the proposed rulemaking.

Perhaps more importantly, in June 2021, after the Colonial Pipeline ransomware attacks, Biden warned Russian President Putin that 16 critical infrastructure sectors should be off-limits from cyberattacks. Although it is not clear what the Biden administration has planned or specifically warned in the event of a critical infrastructure attack attributed to Russia, the presidential notice clearly raises the stakes for Russia: Putin must certainly expect that such attacks will have a significant response from the United States. In that warning, however, the administration took pains to differentiate between "destructive" hacks and "conventional digital espionage operations carried out by intelligence agencies worldwide."

In March of this year, Deputy National Security Advisor Anne Neuberger issued a public warning that the U.S. government is observing "threat intelligence that the Russian government is exploring options for potential cyberattacks on critical infrastructure in the United States." One can imagine that what the United States is observing is Russia conducting the very espionage activities that the United States was careful to distinguish as not off limits, but whether the Kremlin decides to exploit any vulnerabilities it has found or accesses it has established is what matters.

Regardless of Biden's warning, Putin certainly understands that there is a big difference between hacking private email accounts of administration officials and dumping the emails for an embarrassment campaign, compared to an attack that impacts water, electricity, or communications systems in the United States. Russia will always want the option to disable the critical infrastructure in the United States—much the same way other countries proactively seek to understand weaknesses in their adversaries' defenses. But I would be surprised if Putin were to take action against U.S. critical infrastructure because of the potential for it to result in significant escalation, whether of the conflict in Ukraine or more generally.

So despite the necessary focus on preparing for critical infrastructure cyberattacks, I would be more concerned about attacks on private companies or further disinformation campaigns. For companies that have made a noisy exit from Russia, Putin may wish to exact revenge or seek to embarrass them, not unlike North Korea's attack on Sony. For the Biden administration and the country, the November elections will be critical, and Russia has spent years honing its disinformation activities around U.S. elections. Seeking to further punish Democrats for their support of Ukraine through electoral losses would be an easy tool in Putin's toolbox, for which the response from the United States is highly unlikely to be as severe (or as bipartisan) as a response for an attack on critical infrastructure.

You have served in several high-level legal positions in the U.S. government, in two administrations, including most recently as Acting General Counsel of the Department of Defense at the start of the Biden administration. When the U.S. government conducts cyber operations, how do the lawyers for the departments or agencies involved think about evaluating the legality of the proposed operation? How much technical expertise is required?

The U.S. government has a deep bench of lawyers who have been thinking about these issues for a long time. Retaining that crucial, long-term memory and experience that exists in the civil service is incredibly important; and, under the current administration, it is complemented by a tech-savvy and seasoned political appointee team.

It is my experience that the vast majority of the lawyers in this area do not necessarily have technical backgrounds. Although having technological knowhow certainly helps, it is arguably far more important to have honed legal skills, including the ability to develop a full factual understanding of the scenario at issue. Often, as is the case in many areas of law, your clients provide you only with the facts that they think you need, and perhaps not the entire picture (usually in an effort to be efficient with your time or because they may not have sufficient understanding of the law to appreciate what other facts truly matter).

One of the key issues in applying law to cyber operations is grappling with the effects, both intended and foreseeable-but-unintended. Understanding that a particular activity doesn't start or end with the 1s and 0s being transmitted across the wire is a must; and it is crucial to have enough experience to ask the probing, and sometimes iterative, questions needed to evaluate fully what effects a particular operation is intended to have, or could unintentionally produce. There can be challenges in what can get lost in translation between the policy and legal worlds—for example, a client's use of the word "metadata" cannot be assumed to equal "noncontent" information under the Fourth Amendment. In the case of a complex cyber operation, it's imperative to ask enough questions to determine whether an activity is likely to merely affect one small portion of complicated machinery, for example, or could have follow-on effects. And in some cases, it's incumbent upon the lawyers to push back on clients when the operational uncertainty is too great; when it's not possible to fully understand the range of potential impacts of a cyber operation, it may not be possible to ascertain its legality. Simply wishing for the best possible outcome is not an appropriate course of action.

"Understanding that a particular activity doesn't start or end with the 1s and 0s being transmitted across the wire is a must; and it is crucial to have enough experience to ask the probing, and sometimes iterative, questions needed to evaluate fully what effects a particular operation is intended to have, or could unintentionally produce."

But all of these things are true for non-cyber operations as well. Whether it's lawyering traditional kinetic use of force, or merely delving into an area of a complex litigation regarding an intellectual property or financial dispute, basic lawyering skills are about understanding your clients, the language that they use, how to communicate with them, and how to get the facts you need to best advise them. These skills translate across subject matter.