CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE | THE CHICAGO COUNCIL ON GLOBAL AFFAIRS

TASK FORCE ON U.S. POLICY TOWARD RUSSIA, UKRAINE, AND EURASIA

RUSSIA AND CYBER OPERATIONS: CHALLENGES AND OPPORTUNITIES FOR THE NEXT U.S. ADMINISTRATION

BEN BUCHANAN AND MICHAEL SULMEYER

On October 7, 1996, well before such things were commonplace, the Colorado School of Mines suffered a digital break-in. The intruders gained access to a computer nicknamed "Baby_Doe" in the school's Brown Building. To do this, they exploited vulnerabilities in the machine's Sun OS4 operating system. From there, they hopscotched to NASA, the National Oceanic and Atmospheric Administration, the U.S. Navy and Air Force, and a long list of other computers spread across American universities and military installations. The operation went on for years, with the intruders collecting sensitive information as they went.

A later investigation would conclude that the data taken during this period, if printed out, would stretch as high as the towering obelisk of the Washington Monument. The investigators noticed something else: the bulk of the intruders' activities took place at night. From this fact, and from the tangled international web of hop points through which the intruders carried out their operations, the case acquired a name—Moonlight Maze. As the investigation proceeded, the perpetrators came more clearly into view: Russian operators.

In the strictest sense, Moonlight Maze has since ceased to exist.[1] Once the code name became public—splashed onto magazine covers and even T-shirts worn by the investigators—the U.S. government devised a new one. But the activity described by the name—Russian cyber operations against a wide variety of American targets—continues to this day. Indeed, the challenges of the late 1990s have only grown.

Russian cyber operations should be a key concern for the next administration. In general, the potency of cyber operations has increased over the last two decades. Russia has proven itself capable of keeping up with, and in some cases innovating within, the trends in cyber operations. In light of this, the next U.S. administration must develop and implement a course of action for protecting American networks against a significant Russian threat.

The threat can be subdivided into two areas: the collection of information and intrusions designed to hold targets at risk. Each of these is the subject of a section that follows. The third section develops recommendations for possible ways to approach these threats.

COLLECTION OPERATIONS

Espionage predates the modern state. Yet, as the Moonlight Maze case showed, cyber capabilities enable intelligence agencies to conduct espionage in new and innovative ways. Espionage via cyber operation is often more scalable, more discreet, and faster than espionage by traditional means. Both the United States and Russia use these cyber means to gather information, and both will continue to do so for the foreseeable future.[2]

ABOUT THE AUTHOR

Ben Buchanan *is a post-doctoral fellow at the Belfer Center's Cyber Security Project.*

Michael Sulmeyer *is the director of the Belfer Center's Cyber Security Project.*

Russian operators have engaged in a broad series of collection operations, continuing the precedent set by Moonlight Maze. In 2014 and 2015, a string of intrusions into key parts of the U.S. government came to light. The intruders targeted the State Department, the Pentagon, and the White House. Each time, they eventually met with some form of success, copying sensitive documents and communications. The intrusions attracted enormous attention within the U.S. government, and were mentioned by Secretary of Defense Ash Carter in a major speech in April 2015 on the importance of defending American networks.[3]

These and other Russian operators have developed a wide array of advanced tricks to carry out their missions. One particularly striking innovation illustrates the level of creativity. In order to disguise their electronic command and control messages—a key indicator used by network defenders to spot malicious activity—the operators instructed infected computers to place dummy calls over satellite phone networks operating in certain areas. Though the fake calls would not connect, Russian agents with satellite dishes would be able to receive the downlink messages in a fashion that was difficult for network defenders to spot.[4]

The Russians have gone well beyond merely gathering information, however. While other states might use that information to guide their decisionmaking under the quasi-accepted norms of espionage, Russia also appears willing to deploy collected information in overseas influence operations. It appears that hackers, quite likely with ties to the Russian government, broke into the servers of George Soros' Open Society Foundations and released documents. In some cases, the operators doctored the stolen files to make it appear that the foundation had been aiding particular members of the Russian opposition.[5]

For the United States, the most significant example of this kind of influence operation is the array of leaks in the summer and fall of 2016 of emails from Democratic Party officials. Russian intrusions into entities like the Democratic National Committee, the Democratic Congressional Campaign Committee, and the personal email accounts of top staffers on Hillary Clinton's presidential campaign yielded a great deal of information. The information taken included internal campaign deliberations on a variety of subjects, such as campaign messaging, crisis response, and unvarnished views of political opponents. The intrusions into the Democratic networks also gathered information about internal party discussions about tactics and strategies in both congressional and presidential races. Emails that appeared to show a preference among some staffers for Hillary Clinton over her primary opponent Vermont Senator Bernie Sanders led to the resignation of then Democratic National Committee chairwoman Debbie Wasserman Schultz. Other breaches provided access to the personal information of members of Congress, including cell phone numbers, and personal data on donors. All told, the scope of the intrusions underscores just how much information is accessible via network intrusions, and how adept the Russians were and are at collecting it.

Once the information was collected, the Russians chose to pass this pilfered information to outlets like WikiLeaks and news organizations. They also published emails and documents through what appear to be two cut-outs, a website called DCLeaks and a hacker using the pseudonym of Guccifer 2.0. A series of reports by private sector forensic analysts and an official assessment from the United States intelligence community tie these operations to very senior levels of the Russian government.[6] Even if the Russians did not have the capacity to swing the election from one candidate to another—a subject of great debate—it is apparent that they sought to cause disruption and perhaps doubt about the legitimacy of the contest;[7] their comments via Guccifer 2.0 about the system being rigged indicate as much. While electoral influence in general is not new—both the United States and the Soviet Union carried it out in third-party states during the Cold War—it is deeply unusual for the United States to be on the receiving end of it.[8]

Together, the intrusions against the Open Society Foundations and the various components of the Democratic Party reveal the high priority the Russians place on information operations. Warning about extensive Russian investment in this area, which includes but extends beyond cyber operations, former NATO Supreme Allied Commander General Philip Breedlove said that Russia had built an apparatus capable of "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare." While in the past information gathered through espionage was usually kept secret, the Russians have made it clear that they believe those rules no longer apply.[9]

HOLDING TARGETS AT RISK

Not all Russian cyber operations seek to gather information. Key missions seek to develop offensive capabilities against possible future targets—what strategists sometimes refer to as holding targets at risk. These operations, and the demonstrated Russian willingness to utilize the access gained for destructive effect, deserve a great deal of attention.

Holding key targets at risk is an important part of many modern military strategies. The idea is that, in the event of hostilities or other contingencies, one has the ability to destroy or disable key targets. This can be done either as a means of denying an adversary the capacity for action or of imposing costs on an adversary. In conventional operations, many of the capabilities used to hold targets at risk do not require extensive preparation on a per-target basis; cruise missiles and air strikes can be quickly retargeted and launched with impunity in permissive environments. In cyber operations, however, this is not the case. Gaining digital access to the target often requires time, as does developing a capability that can have a tailored effect on the target. Nations that desire bespoke offensive capabilities, therefore, often need to launch their intrusions early.[10]

Russian activity bears this out. Operators linked to Russia have carried out a variety of operations into critical infrastructure and other key targets. A piece of Russian-linked malicious code known as BlackEnergy—itself converted from criminal malicious software—has been found in a variety of key targets, especially across Europe.[11] Speaking generally about sophisticated adversaries, which almost certainly includes Russia, National Security Agency Director Michael Rogers said in September 2015 that foreign states are "spending a lot of time and a lot of effort to try to gain access to the power structure within the United States, to other critical infrastructure . . . with a purpose, doing this as a way to generate options and capabilities for themselves should they decide that they want to potentially do something."[12]

Sometimes the Russians have seen fit to act on their access. Two prominent cases deserve attention. One is an attack on TV5 Monde, a prominent French television station. On April 8, 2015, hackers rendered inaccessible key parts of the channel's network. The targets included email and administrative systems, as well as critical hardware, such as components that encoded video for transmission. Technicians needed more than three hours to restore even partial broadcast capacity and more than a day to restore full service. The estimated damage was five million euros, plus several million euros per year in new cybersecurity measures.[13]

The other notable example is the attack on the power grid in Ukraine. On December 23, 2015, the region of Ivano-Frankivsk in western Ukraine was plunged into darkness. As the digital intruders manipulated almost sixty circuit breakers and substations throughout the system, more than 230,000 people lost electricity to their homes and businesses. In a well-timed move, the operators launched a coordinated telephone denial-of-service attack against the power company itself, making it much more difficult to communicate with customers. They similarly disabled the company's backup generators, leaving the technicians themselves in the dark. The outage lasted only six hours; the fast recovery time was due to the Ukrainian systems' ability to function with manual operation, a feature not present in some U.S. systems.[14]

Though attribution to the government has not been definitively done, it appears as if there was some level of Russian involvement.[15] Attribution itself is a complex question to unpack in cybersecurity. There has long been a view that it is impossible in cyber operations, though that belief has started to fade. There are also varying levels of attribution, including technical attribution to a machine, personal attribution to an operator, and political attribution to a state or other motivating entity; even so, for political entities like states, there are varying degrees of responsibility.

These two attacks together demonstrate a few important dimensions of Russian cyber operations designed to hold targets at risk. Both operations revealed a patient nation capable of carrying out a mission over time. In the case of TV5 Monde, the intruders scoped out the network for months, gaining access and developing customized malicious code capable of doing a great deal of damage to a wide variety of network components. After-action damage assessments confirm the potency of this sort of operation; it was only the serendipitous presence of technicians on-site that day, and the quick thinking response of one technician in particular, that averted much greater damage. As the director-general of TV5 Monde said, "We were a couple of hours from having the whole station gone for good."[16]

In the case of Ukraine, a great deal of the operation's potency came from the extensive reconnaissance the intruders conducted in the network. This took months to achieve. The knowledge gained over time by the intruders enabled them to have a tailored and powerful effect when the time came to strike. An after-action analysis concluded that, "the strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack."[17]

Both operations also were reasonably ambitious in their intended scope. The TV5 Monde attack, in addition to targeting a variety of key pieces of the station's equipment, also tried to dupe investigators into believing the attack was not Russian in origin. The messages sent by the attackers on the day of the strike claimed that the so-called Cyber Caliphate carried out the operation. Since the attack took place just a few months after the shootings at France's *Charlie Hebdo* magazine, a digital strike from the self-proclaimed Islamic State might have seemed plausible. Nonetheless, despite the attempt at a false flag, investigators eventually determined that the operation was Russian in origin. The underlying motive, possibly to test out cyber capabilities or assess Western intelligence agencies' ability to spot such misdirection, remains unknown.[18]

The Ukraine attack is significant in that it is the first publicly-reported case of a blackout caused by cyber operation. The risk to the power grid had long been theorized, and indeed electricity facilities had been infected—likely inadvertently—with malicious code before,[19] but the Russian operation demonstrated in public the capacity of sophisticated actors to successfully disable critical infrastructure in another country at a time of their choosing. This demonstration of harm makes intrusions designed to hold targets at risk all the more threatening and concerning.

Both attacks fall short of fully integrated military operations. Even as patient and ambitious as both attacks were, they do not demonstrate a capacity for truly joint missions that pair modern cyber attacks of higher potency with a broader military effort. It remains an open question whether, in an all-out shooting conflict, the Russian state would be capable of integrating highly sophisticated tailored-effect cyber capabilities into a battle plan. Evidence indicates that during the conflict with Georgia in 2008, there was some coordination between cyber and military attacks, even if the attacks were not conducted by the military.[20] Whether Russia is capable of such joint efforts joining modern cyber attacks of higher potency with a broader military effort remains to be seen. The two kinds of operations are usually carried out by different agencies, often with different command structures and sometimes even with competing interests. Bureaucratic politics aside, conducting joint cyber operations requires synchronization and skill; it is unclear the degree to which the Russians have mastered this in modern conflict.

RECOMMENDATIONS

To better position the United States against increased Russian cyber operations, an approach designed to improve American operations in three areas is essential: defense, detection, and deterrence. Implementing these recommendations in these areas will enable U.S. policymakers to have greater confidence in the baseline level of security in key networks, a better chance of quickly identifying and thwarting Russian intrusions when they do occur, and a clearer posture for limiting Russian behavior.

The standard of baseline defenses must improve, both in government networks and in privately operated critical infrastructure. Network defenders should prioritize deploying audited code—software that has been checked for vulnerabilities—and applying security updates in order to minimize the opportunities for intrusion as much as possible. Ideally, such efforts will minimize the percentage of successful intrusion attempts, enabling defenders to focus their time on more sophisticated threats, such as those potentially posed by Russia. This will likely involve replacing older so-called legacy systems that were not built with security in mind. In the case of federal networks, Congress should authorize the modernization of important information technology infrastructure; the 2016 budget request from President Barack Obama contains initiatives that are a useful starting point.[21]

A related component of defense is detection. The faster adversaries can be spotted and removed from a network, the less damage the adversaries will be able to do. Better perimeter defenses are a fundamental part of cybersecurity, but they are not by themselves sufficient. Within both the private and public sector, networks should be designed or, where applicable, redesigned to increase the

visibility defenders have into all activity taking place. With better network visibility, defenders should monitor their own networks for anomalous activity that could indicate the presence of an intruder.[22] Older systems will likely have to be replaced over time in order to achieve this; President Obama's proposal for information technology modernization in government is also a good start.[23]

To aid this effort, the United States government should increase its information sharing with the private sector. It should prioritize efforts to declassify as much as possible threat intelligence on sophisticated foreign actors, including Russian operators, and share this data with the relevant sector-specific information sharing and analysis organizations. When this threat intelligence is married with better network architecture, ongoing detection of malicious activity becomes a more tractable problem. Where appropriate, the United States should increase its intelligence collection in order to inform this effort.

In addition, the U.S. government should lead or encourage a widespread effort to detect adversaries already lurking in American critical infrastructure. This mission, which will likely involve a private-public partnership in some areas, should seek to identify intrusions that have already taken place and remove them from the affected networks. The goal should be to reduce, as much as possible, the Russian ability to perform ongoing collection and to hold key U.S. targets at risk. Decontamination of networks is a challenging and resource-intensive undertaking, but it is vital.

The last recommendation relates to deterrence. The United States should make it clear that there are costs for intrusive cyber operations, especially when those operations exceed acceptable norms of behavior. In order to make this deterrent credible, the United States must be prepared to retaliate for activities it deems inappropriate. But this response does not need to be limited to cyber operations. Indeed, there is already a precedent for non-cyber-operation responses to intrusions, a concept known as cross-domain deterrence.

In response to cases like the hacking of campaign officials and the leaking of their personal emails, the United States should identify the perpetrators and consider an unambiguous public rejoinder. The Department of Justice has obtained indictments against Chinese and Iranian cyber operators; where appropriate, it should consider using that tool against Russian actors. This naming and shaming, combined with the possible restrictions on travel—due to fear of arrest—that accompany indictments indicates to operators that the United States is capable of doing attribution and that there perhaps will be consequences for their actions. In addition, sanctions in response to cyber activity may also be merited. The 2015 executive order signed by President Obama enables the United States to impose sanctions on other nations for their behavior in cyberspace. With Russia, there are already sanctions in place due to the conflict in Ukraine, but additional targeted sanctions for cyber activity may be warranted.[24]

Cyber operations might have a role to play in deterrence and retaliation as well. The U.S. government should consider exploring additional creative and unorthodox means of cost imposition. The United States has already used some cyber operations capabilities against the Islamic State. If appropriate, it could conceivably use these or other capabilities against Russian targets. The guiding principle in these efforts should be to target areas of unique Russian vulnerability. One possibility is to target those entities threatening the territorial integrity of neighboring allies; another potentially very punishing option would be to manipulate the System of Operative Investigative Activities (SORM), the Russian domestic surveillance system for monitoring Internet and telephone communications. Such steps should certainly not be taken lightly, but may be tools worth considering if the situation warrants.

As the new administration comes into office, it can be tempting to pursue new initiatives cut from whole cloth. But patience is warranted. The administration should take time to generate options, establish a clear position on what cyber activity is impermissible, and communicate its seriousness about cyber operations to its Russian counterparts. All told, the Russian cyber threat is significant but hardly catastrophic. It is neither new nor unprecedented. The triad of better defense, better detection, and better deterrence can meaningfully improve the U.S. position. These goals are attainable with careful policymaking and investment. Even if the dangers posed by Russia's operators can never be fully solved, they can be managed in a way that protects American interests.

The authors would like to thank the Belfer Family and the Hewlett Foundation for supporting this research.

NOTES

1. For the definitive account of Moonlight Maze, see Thomas Rid, *Rise of the Machines* (New York: WW Norton, 2016).
2. Sydney J. Freedberg Jr., "DNI, NSA Seek Offensive Cyber Clarity; OPM Not an 'Attack,'" Breaking Defense, September 10, 2015, http://breakingdefense.com/2015/09/clapper-rogers-seek-cyber-clarity-opm-not-an-attack/
3. Michael Schmidt and David Sanger, "Russian Hackers Read Obama's Unclassified Emails, Officials Say, " *New York Times*, April 25, 2015; Ash Carter, "Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity" (Stanford University), Department of Defense, April 23, 2015.
4. Stefan Tanase, "Satellite Turla: APT Command and Control in the Sky," SecureList, September 9, 2015.
5. Elias Groll, "Turns out You Can't Trust Russian Hackers Anymore," *Foreign Policy*, August 22, 2016.
6. Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike, 2016; Thomas Rid, "All Signs Point to Russia Being Behind DNC Hack," *VICE*, July 25, 2016; "US Accuses Russia of Political Hacking, War Crimes in Syria," *New York Times*, October 7, 2016.
7. Adam Entous, Ellen Nakashima, and Greg Miller, "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House," *Washington Post*, December 9, 2016.
8. Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly* (2016).
9. Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016.
10. For more on this, see Ben Buchanan, *The Cybersecurity Dilemma* (New York: Oxford University Press, 2017), chapter 2.
11. Dennis Fisher, "Sandworm APT Team Found Using Windows Zero Day Vulnerability," October 14, 2014; Kurt Baumgartner and Maria Garnaeva, "Be2 Custom Plugins, Router Abuse, and Target Profiles," SecureList, November 3, 2014.
12. Damian Paletta, "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent," *Wall Street Journal*, September 8, 2015.
13. Gordon Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers," BBC News, October 10, 2016.
14. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016; "Cyber-Attack against Ukrainian Critical Infrastructure," Industrial Control Systems Emergency Response Team: Department of Homeland Security, 2016; Robert Lee, Michael Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Electricity Information Sharing and Analysis Center, March 18, 2016.
15. For two overviews of the issue, see Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Atlantic Council, 2011; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, 39, no. 1 (2015).
16. Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers.'"
17. Lee, Assante, and Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid, " Electricity Information Sharing and Analysis Center, 2.
18. Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers.'" For more on false flags, see Juan Andres Guerrero-Saade and Brian Bartholomew, "Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks," Kaspersky Lab, October 2016.
19. For example, see Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," Security Focus, August 19, 2003.
20. "Overview by the US-Ccu of the Cyber Campaign against Georgia in August of 2008," United States Cyber Consequences Unit, 2009.
21. Tami Abdollah, "Obama Seeks Cybersecurity Boost to Replace 'Ancient' Tech," Associated Press, February 9, 2016.
22. For an overview of this key idea, known as network security monitoring, see Richard Bejtlich, *The Practice of Network Security Monitoring* (San Francisco: No Starch Press, 2013).
23. Abdollah, "Obama Seeks Cybersecurity Boost to Replace 'Ancient' Tech."
24. For more on sanctions with regards to Russia, see Andrew S. Weiss and Richard Nephew, "The Role of Sanctions in U.S.-Russian Relations," Carnegie Endowment for International Peace, July 11, 2016, http://carnegieendowment.org/2016/07/11/role-of-sanctions-in-u.s.-russian-relations-pub-64056.

TASK FORCE ON U.S. POLICY TOWARD RUSSIA, UKRAINE, AND EURASIA

The task force will assess the strengths and weaknesses of U.S. and Western policy toward Russia, Ukraine, and Eurasia since the end of the Cold War and offer a set of guiding principles for a durable U.S. policy framework. The task force is a joint effort with the Chicago Council on Global Affairs and is supported, in part, by the Carnegie Corporation of New York.

@CarnegieRussia facebook.com/CarnegieRussia

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance the cause of peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

@CarnegieEndow facebook.com/CarnegieEndowment