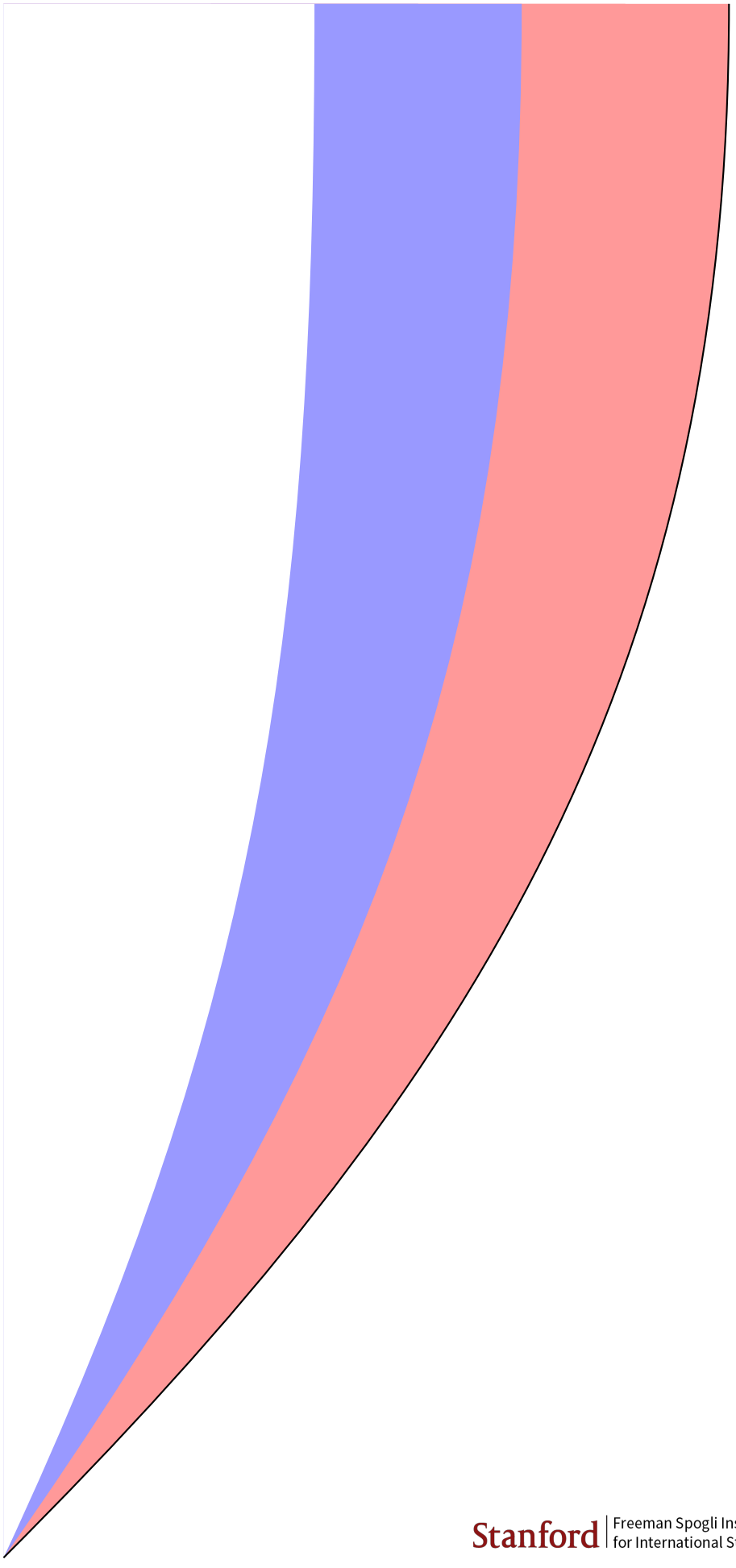

Countering Russian Cyber Operations

Scott Jasper

Stanford | Freeman Spogli Institute for International Studies

September 2020

Introduction

Russia has deployed cyber operations to interfere in foreign elections, launch disinformation campaigns, and cripple neighboring states—yet the regime has maintained a thin veneer of deniability and avoided strikes that cross the line into acts of war. How should a targeted nation respond? The international effort to counter Russian cyber operations by imposing sanctions and indictments, in combination with a new defend forward approach, has done little to alter Moscow's behavior. Therefore, nations should deploy robust solutions for resilience to withstand future attacks.

Defining the Thresholds of Attack

The 2017 U.S. National Defense Strategy asserts that Russia is using "areas of competition short of open warfare to achieve their ends (for example, information warfare, ambiguous or denied proxy operations, and subversion)."[1] Cyber operations are merely a nonmilitary means for Russia to obtain political goals and objectives. The United States intends to work with like-minded partners to attribute and deter their malicious cyber activities. The problem is that the Kremlin is adept at cyber operations that avoid thresholds for robust responses.

Specifically, Russian actors take advantage of the ambiguity in what constitutes an armed attack, as Article 51 of the Charter of the United Nations gives states the inherent right to use force in self-defense. According to the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, the threshold for an armed attack is measured based on the scale and effects of the cyber operation. The international group of experts that wrote the *Tallinn Manual* agreed that "a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement."[2] The terms "seriously" and "significant" open opportunity for debate on specific thresholds. The experts also concluded that cyber operations for intelligence gathering or theft, as well as brief interruptions of non-essential cyber services, do not qualify as an armed attack.

However, numerous cyber operations that fall below the threshold of armed attack are considered internationally wrongful acts, defined by Rule 14 of the *Tallinn Manual* as "an action or omission that both constitutes a breach of an international legal obligation applicable to that State; and is attributable to the State under international law."[3] The breach of an obligation may consist of a violation of treaty obligations or customary international law. The second condition is difficult to determine and prove, especially since cyber operations conducted by a person or group of persons are attributable to the state only when "acting on the instructions of, or under the direction or control of, that state in carrying out the conduct."[4]

How Cyber Operations Work, Who They Target, and Why They Haven't Stopped

Russia considers itself to be "engaged in full-scale information warfare" with the West, and cyber activity to be a subset or facilitator.[5] Russian cyber actors employ technical means for intrusion, evasion, and deception to maintain anonymity and avoid attribution. Examples of their attack vectors, or methods of intrusion into an information asset, include phishing, using stolen credentials, or posting watering holes. For instance, during the 2017 Bad Rabbit attack, visitors of infected Russian-language media websites fell for a fake pop-up to update the Adobe Systems Flash multimedia product. Fileless malware attacks are another sophisticated technique Russian actors use to evade detection. These attacks do not write an executable file to the disk drive, making them much harder to detect by antivirus software. Instead, they leverage stolen credentials for remote logins and trusted legitimate processes running on the targeted operating system.

As for deception, the Russians attempt to mislead, misdirect, and misattribute. For example, during the 2018 Winter Olympic Games, Russian hackers from the Main Intelligence Directorate, the GRU, used North Korean IP addresses to make an attack look like the work of North Korean hackers.[6] The Russians also divert or attribute blame to proxies such as patriotic hackers, criminal organizations, and advanced persistent threat groups.

Russian cyber operations and influence campaigns have repeatedly targeted the United States, most famously to alter the outcome of the 2016 presidential election. A report by the Senate Intelligence Committee found that "in 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency [the IRA] used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States."[7] The Russians also used hacks and leaks to interfere with the 2016 U.S. presidential election. Two state-sponsored groups hacked into the Democratic National Committee (DNC) computers. In late July 2016, Wikileaks dumped 20,000 emails from top DNC officials, revealing their preference for Hillary Clinton as Democratic candidate over Bernie Sanders. The release days before the DNC convention outraged Sanders supporters, who protested the entire convention.

How should these activities be categorized? The Russian influence campaign was not an initiation of armed conflict nor a violation of the UN Charter's prohibition on the use of force, yet the attempt to influence the election outcome probably violated international law barring intervention in a sovereign state's internal affairs. To qualify, an operation must affect the target state's domaine resérvé—or domestic activities outside the purview of international law, in this case the political system of democracy—and the process must be coercive, depriving freedom of choice. While slanted reporting by Russian-controlled media is not coercive, other activities impacted Americans' ability to make choices, such as cyber actors posing as American citizens, hacking, and the release of private data, and might

therefore justify countermeasures.[8]

In response, the Obama administration contemplated covert cyber action against Russia, but refrained due to worries over escalation.[9] Instead, President Obama signed a package of punitive measures consisting of sanctions, diplomat expulsions, and compound closures. The sanctions targeted the GRU, imposing travel bans and assets freezes, but were so narrow that their impact was "largely symbolic."[10] In addition, the expulsions and closures were originally devised to retaliate for harassment of American diplomatic personnel in Russia by security personnel and police, watering down the response to cyber actions.[11] More proactively, the US government released declassified technical information on Russian cyber activity to help defenders "identify, detect and disrupt Russia's global campaign of malicious cyber activity."[12] Reflecting on these responses, General Nakasone, the commander of US Cyber Command, told the Senate Armed Services Committee that adversaries like Russia are "willing to continue launching cyberattacks against the U.S. on account of the administration's subdued reaction to the alleged Kremlin-ordered hacking campaign waged against the 2016 White House race."[13]

Indeed, the Russians were undeterred in their behavior. To provide only a few examples of further Russian cyber operations:

- In 2017, Russian cyber actors proceeded to hack and leak documents and emails from Emmanuel Macron's French presidential election campaign, while Twitter bots amplified the rhetoric around the leaks.

- In June 2017, the NotPetya worm launched a global ransomware attack, which was designed not to process ransoms, but to wipe out data on infected computers. The majority of NotPetya infections occurred in Ukraine, with targets including government ministries, the power grid, the Kiev airport, civilian healthcare networks, and a major Ukrainian bank, whose network was infected in just forty-five seconds.[14] NotPetya moved laterally at lightning speed, spreading unabated across Europe and into the United States. Maersk reported interruptions in shipping container operations for over a week,[15] while Merck shut down production of vaccines for HPV and hepatitis B.[16]

- An October 2019 cyberattack on the country of Georgia has been blamed on the GRU by the U.S. and nearly a dozen other nations. The attack took two Georgian television stations off the air and disabled or defaced thousands of government websites. However, the blame fell short, as the national statements did not provide the basis for attribution, delineate the exact rules violated, or outline any consequences to hold Russia accountable for their attempt to undermine Georgia's sovereignty.[17]

- Utility systems have also been targeted. In March 2018, the Department of the Treasury announced that for over two years, cyber actors controlled by the Russian government have "targeted U.S. government entities and multiple U.S. critical infrastructure sectors,

including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."[18] A corresponding Technical Alert characterized the activity as a "multi-stage intrusion campaign" through which Russian actors "staged malware, conducted spear phishing, and gained remote access."[19] The Russian campaign demonstrated proficient use of legitimate processes (PowerShell, PsExec), batch scripts, and public tools (Mimikatz, Hydra) with the aim of gaining control of operational systems for two dozen or more utilities.

Policy responses to these operations have been spotty at best. In 2018, the Department of Justice indicted GRU officers and the IRA for interfering with the 2016 U.S. presidential election. That March 2018, the United States issued sanctions on the GRU for the NotPetya attack. The next month, the Treasury Department designated seven Russian oligarchs, and twelve of their companies, for their role in malicious cyber activities, freezing assets and prohibiting U.S. persons from dealing with them. The impact in Russia on stocks and currency was immediate, but sanctions were lifted months later on two of the firms, including, Rusal, the second-largest producer of aluminum in the world, because of soaring prices.[20] This signal from the Trump administration only bolstered President Putin's belief that the methods of pressure used by other countries "are ineffective, counterproductive and harmful to all."[21]

With Russian cyberattacks and intervention showing no sign of abating, the broader concern is that the risk frameworks, best practices, and threat-sharing mechanisms that have been in place in many cases have essentially failed. More robust solutions for resilience—defined as the capacity to withstand an attack if it penetrates defenses and continue operation—are necessary to deny the Russians the benefit of their attacks.

Policy Recommendations

The United States must use every instrument of national power to deter Russian cyber operations. Policymakers should focus on measures of deterrence, but most importantly, develop greater cyber resilience.

1. Cyber defense initiatives must be pursued and implemented, especially around elections. For instance, U.S. Cyber Command created a Russia Small Group task force to protect the 2018 US midterm elections from foreign interference in a defend forward approach. The Group targeted Russian trolls to try to deter them from spreading disinformation on US social media platforms. The trolls persisted, and on Election Day, and during the vote count, Cyber Command took the Agency servers offline by blocking Internet access. While U.S. senators from both political parties praised the operation, the Russian Federal News Agency said the cyberattack "disabled two of its server's four hard drives but did not stop work entirely."[22] More impactful U.S. cyber activity along these lines is important, though

it is notable that while it might be necessary for deterrence, there is a possible risk of escalation.

2. U.S. whole-of-government efforts must be undertaken in a name-and-shame strategy to identify and condemn Russia's continued cyber operations to influence or disrupt democratic societies and to penetrate or damage critical infrastructure. Ensuring accurate media reporting and public education on identifying disinformation is a part of this. Deliberate, unambiguous denunciations of Russian cyber operations can help demonstrate that cyberattacks, like armed attacks, are taken seriously.

3. As of now, the Russians seem not to believe that malicious operations will be punished under international law. From a legal standpoint, a ruling on the respect of sovereignty vis-à-vis the emplacement of malware would be a major step forward.[23] Such a ruling would raise the threshold on what is considered an attack to ensure that malign cyber operations, with proven attribution, would be defined as an international wrongfully act. This would make the risks of cyber intervention outweigh the benefits.

4. Beyond deterrence, resilience must be a central focus of U.S. policymaker and engineers. Russian hacking groups have demonstrated increasing technical complexity in their intrusion methods and evasion capabilities, showing them to be prolific, skilled, and the fastest of state-sponsored actors.[24] Their advantages in cyber operations can be diminished only by the deployment of robust solutions for resilience that capitalize on data correlation technologies, which protect against malware, script-based, and fileless attacks by using machine learning and behavioral analytics to identify not just exploit signatures, but also exploit techniques.[25] These technologies would prevent initial infection and hinder the propagation of malware and password-cracking tools. One such tool is the Palo Alto Networks Cortex XDR, installed at the Naval Postgraduate School, which uses a child process protection module and DLL hijacking rules, local analysis, and WildFire cloud threat intelligence query—enabling the termination of live processes in a live environment and thus allowing users to continue to work without disruption or downtime. Such tools would contribute greatly to the resilience of the U.S. cyber sphere.

References

[1] Jim Mattis, Secretary of Defense, "Summary of the National Defense Strategy of the United States of America," Department of Defense, January 2018: p. 3.

[2] Schmitt, editor, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, second edition (Cambridge University Press, 2017): p. 341.

[3] Schmitt, *Tallinn Manual* 2.0: p. 84.

[4] International Law Commission, "Draft Articles on Responsibility of States," 2001: p. 34.

[5] Keir Giles, "The Next Phase of Russian Information Warfare," NATO Strategic Communications Centre of Excellence, May 20, 2016, p. 4.

[6] Ellen Nakashima, "Russian Spies Hacked the Olympics and Tried to Make it Look like North Korea, U.S. Officials Say," *The Washington Post*, February 24, 2018.

[7] Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views, October 8, 2019.

[8] Michael Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law*, vol. 19, no. 1, article 2, August 16, 2018: pp. 50-51.

[9] Michael Isikoff and David Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump* (New York: Hachette Book Group, 2018).

[10] Greg Miller, Ellen Nakashima, and Adam Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," *The Washington Post*, June 23, 2017.

[11] Miller, Nakashima, and Entous, "Obama's Secret Struggle."

[12] The White House, Office of the Press Secretary, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment," December 29, 2016.

[13] Andrew Blake, "Foreign Hackers Don't Fear Retaliation, Trump's Nominee for NSA Director Warns," *Washington Times*, March 2, 2018.

[14] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018.

[15] Doug Olenick, "NotPetya Attack Totally Destroyed Maersk's Computer Network: Chairman," *SC Magazine*, January 29, 2018.

[16] Paul Roberts, "NotPetya Infection Left Merck Short of Key HPV Vaccine," The Security Ledger, November 1, 2017.

[17] Mark Pomerleau, Aaron Mehta, and Andrew Eversden, "Why The U.S. Chose To "Name and Shame" Russia Over Cyberattacks," *Fifth Domain*, February 20, 2020.

[18] U.S. Department of the Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," press release, March 15, 2018.

[19] US-CERT, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," alert TA18-074A, March 15, 2018.

[20] Donna Borak, "Treasury Plans to Lift Sanctions on Russian Aluminum Giant Rusal," *CNN Business*, December 19, 2018.

[21] Nataliya Vasilyeva and Jim Heintz, "Putin Says Russian Military Not Building Long-Term in Syria," AP News, June 7, 2018.

[22] Maxim Shemeipu, "Russian Troll Farm: Yes, the Pentagon Hit Us in Cyber Op. But it Was a Complete Failure," *The Daily Beast*, February 28, 2019.

[23] Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law* 54, no. 3 (2014): pp. 704–5.

[24] Lee Matthews, "Russia's State-Sponsored Hackers Are the World's Fastest," *Forbes*, February 20, 2019.

[25] Infogressive, "The Complete Guide to Endpoint Detection and Response," blog post, 2019.