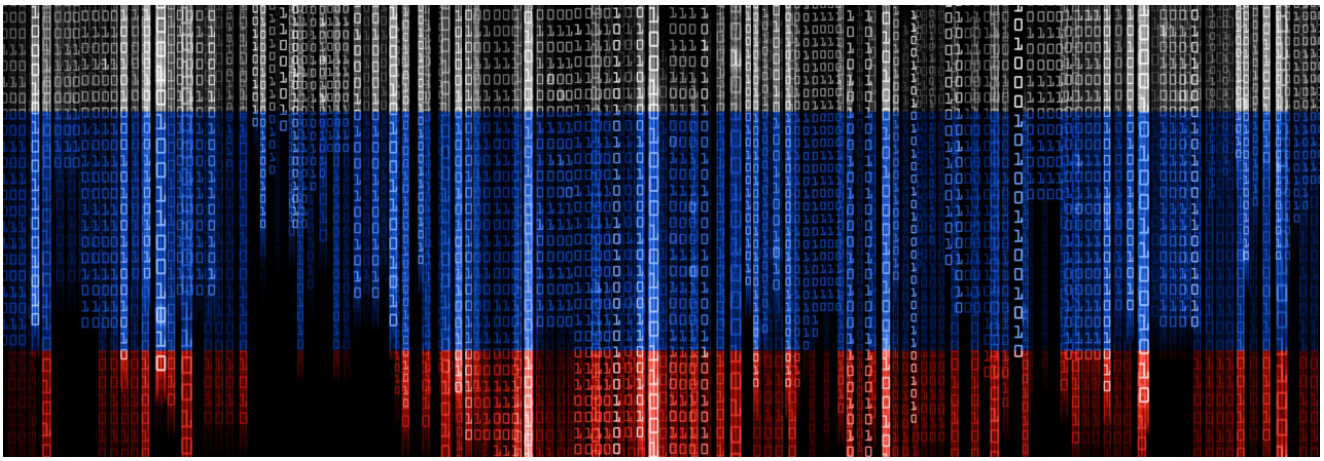
Understanding Russia's Cyber Strategy

fpri.org/article/2021/07/understanding-russias-cyber-strategy/



The Russian Federation's willingness to engage in offensive cyber operations has caused enormous harm, including massive financial losses, interruptions to the operation of critical infrastructure, and disruptions of crucial software supply chains. The variety and frequency of these operations, as well as the resulting attribution efforts, have offered an unusually vivid picture of Russia's cyber capabilities and tactics. While many other countries have relied heavily on vague strategies and threats to signal their emerging cyber powers, Russia has exercised its technical capabilities with relative impunity for more than a decade. This makes it possible to chart Moscow's increasingly bold forays into the cyber domain alongside the increasingly technically sophisticated specific vulnerabilities, techniques, and tactics that Russia has leveraged. This timeline reveals a shift towards more covert, targeted cyber capabilities in recent years, as well as an evolution away from phishing-based compromises to supply chain and service provider intrusions, in conjunction with a continued reliance on and reuse of the same infrastructure and malware across multiple operations.

Emphasis on Covert Capabilities

Going all the way back to the 2007 denial-of-service attacks directed at Estonian infrastructure, Russia's cyber activities have been more high-profile and deliberately publicly visible than those attributed to any other country, with the possible exception of North Korea. Many countries, including the People's Republic of China and the United States, have relied primarily on cyber capabilities for covert espionage or sabotage efforts that could be executed over the course of months, or even years, without detection. By contrast, Russia's exploits in cyberspace, including the 2016 breaches of the Democratic National Committee and the Democratic Congressional Campaign Committee and the 2017 NotPetya attacks, often drew immediate attention, by design. Bilyana Lilly and Joe

Cheravitch describe how the visibility of Russia's cyber operations increased over time with the gradual shift in leadership of those operations from the FSB, Russia's domestic security agency, to the GRU, Russia's military intelligence agency, which "brought with it a culture of aggression and recklessness" and a "high tolerance for operational risk" that was unusual in the cyber domain.

More recently, increased activity from Russia's civilian foreign intelligence service, SVR, has suggested a growing emphasis on long-term, covert cyberespionage operations. For instance, the SolarWinds compromise discovered in late 2020 went undetected for at least nine months, probably in large part because Russia exercised uncharacteristic restraint in targeting only a small subset of the victims that it had compromised. The malicious SolarWinds Orion software update that was used to establish an initial foothold in victims' computer systems was downloaded by roughly 18,000 SolarWinds customers, according to a December 2020 SolarWinds Securities and Exchange Commission filing. That initial foothold only offered very preliminary access to computer systems, and many of the organizations that did download the compromised software update have not reported further exploitation.

Speaking at an event in March 2021, Silverado Policy Accelerator Chairman Dmitri Alperovitch referred to the SolarWinds compromise as "a very precise operation" because Russia "did not exploit the vast majority of the 18,000 victims." He continued, "I don't think they did this to do us any favors, I think the primary reason for doing that was to actually remain stealthy." Stealth typically requires not just restraint in cyber operations, but also greater technical sophistication to avoid the growing number of intrusion detection and network monitoring tools. Furthermore, it can be difficult to carry out these types of long-term covert cyber operations alongside more destructive, public-facing ones like NotPetya, which tend to trigger increased scrutiny and attention to sensitive networks.

It's possible that the Russian shift to more covert cyber activity is merely a byproduct of the SVR finally developing the tools and techniques that it needed to carry out cyberespionage campaigns, rather than an indication of a long-term shift in Russia's overall cyber strategy. It's also plausible that the relative inactivity of the GRU in the cyber domain since 2018, when the SVR began ramping up its efforts to access cloud resources, is a deliberate, strategic choice on Moscow's part to draw less attention to its online operations. In the future, that balance could swing back in the other direction, with the GRU executing more disruptive cyberattacks, but given the shared reliance on some of the same infrastructure, malware, and techniques, such a shift might well jeopardize some of the SVR's operations.

Tactics, Vulnerabilities, and Technical Sophistication

Russia's shift to more covert operations means that it is relying less heavily on techniques like traditional phishing and denial-of-service attacks. Instead, the focus is on more advanced intrusion tactics like credential harvesting, supply chain compromises, and

infiltrating critical service provider platforms. Russia's growing technical sophistication is evident in its growing reliance on customized malware rather than tools and programs purchased from the black market. Security firm Crowdstrike has traced this progression across different Russian groups, identifying how Russian threat actors have developed custom plug-ins for commodity malware products like Black Energy and then moved to developing entire families of custom malware, including Snake, Chinch, Skipper, Kazuar, and Gayzer.

Recent custom malware has also exhibited advanced implementation of cryptographic techniques as well as anti-analysis protections to help shield it from detection by anti-virus software. Russia has leveraged existing popular platforms, including social media sites and the Tor relay network, in designing and delivering its malware to victims. This suggests an increasing ability and willingness to make use of the broader online ecosystem in cyber operations. Still, Russian cyberattacks continue to use open source and commercially available tools with a recent Department of Homeland Security alert flagging the SVR's use of both the open-source credential dumping tool Mimikatz and the commercially available exploitation tool Cobalt Strike.

As Russian malware has become increasingly complex, so too have the vulnerabilities that Russia is able to exploit in victims' computer systems. The 2017 NotPetya attacks famously relied on the exploitation of the EternalBlue vulnerability in Windows' Server Message Block protocol that was developed by the National Security Agency and then leaked in April 2017 by a group calling itself the Shadow Brokers. Not only did Russia not identify the EternalBlue vulnerability, but it also was not even the first to exploit the vulnerability—North Korea launched the WannaCry attacks that made use of the same vulnerability earlier in 2017, though the later NotPetya attacks proved much more damaging. Similarly, attempts by Russia to compromise computer networks in 2020 through virtual private network (VPN) infrastructure used some previously identified and patched vulnerabilities, rather than novel zero-day vulnerabilities. This move suggests that Russia had not devoted significant resources to develop or purchase its own vulnerabilities, choosing instead to rely largely on those already identified. This model limited the reach of Russia's cyberattacks, in some cases, and perhaps partly motivated the shift to relying on supply chain and service provider-based infiltration tactics that enabled broader access to a larger number of victims.

Expanding the reach, as well as the covertness, of its online intrusion activities has been a central theme of Russia's cyber operations in 2020, accomplished largely through infiltrating third parties, rather than targeting victims directly. These third-party intrusions make compromises more difficult for breached entities to detect—because they are introduced through trusted sources like a company's security dashboard or email provider—and allow for targeting many more victims simultaneously, through the compromise of a single company. In its 2021 Global Threat Report, Crowdstrike notes that targeted malware and phishing campaigns have become less central components of Russian cyber operations. According to the report, "While various Russian adversaries continue to employ malware as

part of their operational toolkits, they have also increasingly sought to shortcut traditional operational workflows and focus directly on intelligence collection from third-party services used by their targets, including direct access to cloud-based network resources such as email servers."

In May 2021, six months after the discovery of SolarWinds, Microsoft announced that it had identified another Russian espionage campaign that relied on accessing a United States Agency for International Development (USAID) account. The attack distributed phishing emails to 3,000 email accounts at more than 150 different government agencies, think tanks, consultants, and non-governmental organizations. Unlike traditional email phishing attacks that rely on tricking a recipient into believing they've received an email from someone they know or trust based on a spoofed or misleading sender address, the Russian campaign that Microsoft identified made use of an intermediary service for email marketing called Constant Contact. This tactic makes it more difficult for recipients to identify the true sender and easier to disguise malicious links and attachments. Just as the compromise of SolarWinds' Orion software update allowed Russian adversaries to infiltrate thousands of victims undetected, the Constant Contact email compromise enabled a similarly large-scale, covert intrusion by relying on a widely used third-party service.

Infrastructure and Malware Reuse

While the technical tactics and sophistication of Russian cyber operations have evolved, many of these exploits continue to rely on shared infrastructure and malware families that enable attribution of new attacks and suggest that Russia relies on a limited circle of suppliers and software developers in this domain. Executing cyber operations often requires considerable infrastructure deployed across many countries. For instance, Russia registers domain names that are very close to the names of legitimate websites in order to set up phishing websites. It also rents virtual private servers (VPS) to conduct password spraying attacks, in which commonly used passwords are tested on different accounts to see if any of them work. Since login attempts from foreign countries are often flagged as suspicious, this infrastructure generally must be in the same country as the victim, so that the login attempts go undetected. The Department of Homeland Security noted that this local VPS infrastructure was typically procured from a network of VPS resellers by Russian threat actors using false identities. The temporary email accounts and Voice over IP (VoIP) numbers associated with those identities could often be traced back to a small number of "low reputation infrastructure" providers and domains, so there were clear, persistent patterns across these efforts even as the technical implementation of Russia's cyber capabilities expanded and evolved.

Russia's growing emphasis on covert capabilities in recent years has necessitated the development of more sophisticated and novel intrusion capabilities, particularly those focused on compromising third-party companies that could then be used as a platform for infiltrating other victims. However, Russia's development of more technically sophisticated

intrusion tactics and malware has not yet been matched by similarly advanced detection and exploitation of novel vulnerabilities or the establishment of more robust underlying infrastructure for these compromises. This has enabled continued attribution of cybersecurity incidents to Russia and has provided an unusually detailed picture of where exactly Russia has chosen to invest its resources in developing cyber capabilities and which elements of its online tactics and techniques are most—and least—advanced.

Moving forward, it will be interesting to watch whether the Russian government continues to avoid directly targeting critical infrastructure in favor of operating covert cyberespionage campaigns. If this trend does continue, then it will also be important to track whether Russia continues to allow criminal organizations based within its borders to launch destructive attacks on overseas critical infrastructure targets, as happened in May 2021 when the DarkSide cybercrime group hit Colonial Pipeline with a ransomware attack, causing a shutdown of thousands of miles of a pipeline, and when the REvil group hit meatpacking company JBS with a similarly disruptive ransomware attack. In some ways, these attacks are reminiscent of NotPetya in their impacts, except that they are financially motivated and therefore comparatively more narrowly targeted and more easily reversible. If Russia's government agencies back off initiating destructive cyberattacks but continue to condone Russian cybercriminals launching similar attacks, then it's unlikely that the tensions between the United States and Russia over the acceptable use of cyber capabilities will ease, despite some small signals that the two countries may be willing to try to reach an agreement on not targeting critical infrastructure. That agreement would have to include a serious commitment by Russia to police cybercriminals and cooperate with international law enforcement investigations to stem destructive cyberattacks in any meaningful way. So far, at least, there are no clear signs that Russia is interested in making any such commitment.

The views expressed in this article are those of the author alone and do not necessarily reflect the position of the Foreign Policy Research Institute, a non-partisan organization that seeks to publish well-argued, policy-oriented articles on American foreign policy and national security priorities.

Josephine Wolff
Josephine Wolff is Assistant Professor at The Fletcher School of Tufts University.