RUSSIA'S LARGE UNIQUE PRESENCE IN THE LANDSCAPE OF CYBER WARFARE

By Collin Sweeney, Research Assistant, REDCOM

In current American discourse surrounding cybersecurity, we are often confronted with the idea of the Russian adversary. Whether it be botnets, malware attacks, network intrusions, or general disinformation, many are quick to pin malicious cyber activity on Russian operators. Immediately following the 2016 presidential election, Russia's influence in the realm of cyber operations became apparent even to those not well-versed in cyber-threat analysis. But before the watershed election interference, cybersecurity experts have known not only of Russia's deep involvement in cyber-warfare, but of the peculiar geopolitics that place Russia in a unique spot within the international cyber-landscape.

Despite Russia's advanced cyber capabilities, Russian geopolitics seem to be stuck in the past – or, at the very least, exceedingly traditional – with a large focus on their immediate periphery (Smith, 2019). This peripheral focus can be seen in some of Russia's latest large-scale military activity, namely their 2008 invasion of Georgia (Stratfor, 2013) and more recent 2014 annexation of Crimea (Pifer, 2019). However, Russian conflict is not entirely external; the internal Russian political structure deals with just as much (if not more) conflict (Smith, 2019). Political corruption is inherent to Russian politics, with government, crime, and business often operating in coordinated concert. Coined the Russian Nexus, this peculiar relationship between enterprise leaders, governmental figures, and crime syndicates allows for quick mobilization of distributed resources on cyber-related projects, but leaves ample room for internal tensions and complications. For example, consider two of the larger internal entities of the Russian political structure: the Main Intelligence Directorate (GRU) and the Federal Security Service (FSB) (Kelly, 2018). The GRU is responsible for handling Russian military intelligence. It is an outward-facing agency which has been in the news recently for its cyberattack on the Democratic National Committee (DNC) in 2016, among other large-scale incidents. The FSB is responsible for internal surveillance. It is an inward-facing agency which has faced international criticisms for its operations, specifically its authoritative treatment of political dissidents. In recent years under Vladimir Putin, the FSB has been shrinking in both size and scope of operations, while the GRU has seen substantial growth in these areas (Smith, 2019). The GRU essentially forcing the FSB out of the federal limelight has resulted in strong tensions between the two agencies, which have delivered interesting culminations. One of the more interesting products of these inter-agency tensions is that the CIA learned details about the GRU's operations against the 2016 United States presidential election via information provided by the FSB (Smith, 2019).

Even through the staggering amount of internal politics and unfriendly competition, the Russian Nexus is very efficient in keeping pace with the dynamic field of cyber-warfare. The Nexus serves as a "self-funded, self-training, and self-equipped" population that is capable of executing technical cyberattacks and developing new operational techniques, analogous to a "Cyber Warfare Reserve Force" (Smith, 2019). Within the Russian Nexus, funds can be rapidly exchanged between government, enterprise, and criminals, which not only dramatically increases overall

speed of operation, but allows individual parts of a project to be outsourced to different domestic and international parties. This outsourcing, combined with a rapid pace of production, introduces difficulty in recognizing the entirety of a Russian cyber endeavor and complicates attempts to attribute acts of cyber-warfare to a specific source. For example, an espionage campaign against a U.S.-based company may be orchestrated by a Russian agency like the GRU. However, the same campaign may employ malware developed by some Russia-based party that is implemented via spear-phishing done by a separate, Korea-based party that uses research done on U.S. personnel by yet another distinct party, and so on. This fractionation can be leveraged for faster production and implementation and could conceivably be used to help deny state-sponsored involvement in acts of cyber-crime. As well as higher production speed, this peculiar relationship fosters development of new techniques and technologies in a unique, straightforward way: because of the close operating relationships within the Russian Nexus, criminal advances lead directly to government advances and vice versa (Smith, 2019).

Many were given insight to Russia's position in cyber-warfare due to the fallout of their malicious actions during the 2016 U.S. presidential election cycle. However, Russia has been posturing themselves to be ready for the domain of information warfare since before the Gulf War (Smith, 2019). Marshal Ogarkov, USSR Chief of the General Staff from 1977 to 1985, was quick to recognize the influence that technological weapons and communications would one day have on the battlefield (Fitzgerald, 1986). He authored many articles and papers that stressed the need to keep up with the U.S. in terms of technological development, and claimed that conventional weapons systems of the future will one day rival the destructiveness of the most advanced nuclear arsenals. In 1982, Ogarkov asserted this belief and wrote, "A profound and revolutionary--in the full sense of the word--perevorot ['revolution', 'turn-about', 'upheaval'] in military affairs is occurring in our time..." (Fitzgerald, 1986). Following the first Gulf War, Ogarkov contended that the conflict was the first display of true Information Warfare and further argued that Soviet forces were falling drastically behind the capability of their rivals. Although one must consider many other factors, some experts assert that Ogarkov's attitude and urge to adopt and develop new technology has helped drive Russia's current ideology of cyber-warfare and operations (Smith, 2019). Although Russia's serious attitude and seemingly strong theoretical understanding of warfare in the cyber domain make them a serious threat and competitor, their vulnerabilities lie in overall poor execution and weak maintenance of their various cyber projects.

Predicting the direction in which Russian cyber-warfare is headed is difficult, but experts have suggested a few areas which would be attractive to Russian adversaries. It is the current sentiment of the U.S. Army that U.S. cybersecurity assets "do not operate at the speed required for Information Dominance" (Fogarty, 2019). This slow operating speed coupled with a singular-focus of cyber defenses leaves vulnerabilities when considering attacks from multiple directions. Again, in the context of the 2016 U.S. presidential election, the United States was left "cybernetically vulnerable" to Russian interference due to U.S. cyber capabilities being largely focused on ISIS fighters and communications infrastructure at the time. It is theorized that Russian actors will continue to attempt to exploit the "one-track mind" of U.S. cyber defense via distributed attacks against IoT devices, specifically ones used in various supply chains (Smith, 2019). Evidence has also shown that Russian adversaries are becoming increasingly interested in malware attacks and the capability to spread malwares through entire networks via infection of a small collection of end users. Further evidence suggests that the Russian military is preparing to develop propaganda and disinformation at record levels. After seeing marginal success of disinformation campaigns like during the 2016 U.S. election and troll farms like the ones used during the Spain-Catalonia conflict, Russia is investing even more time and power into "forming public opinion", using disinformation and propaganda to sow tension and political unrest between communities (Smith, 2019).

The decentralized operating structure of Russian cyber-warfare poses a large threat to the cyber assets of the U.S. and its allies. When faced with a cyberattack on its infrastructure, the U.S. is burdened by slow mobilization of resources due to suboptimal policy and bureaucratic decision-making, roadblocks which are entirely alien within the Russian Nexus. From an operational standpoint, this siloed methodology leaves us more vulnerable to the fractionated structure of Russia's cybernetic forces; Russian actors would be funding and executing their next cyberattack while we are still working to formulate a response to the first one. The combination of cyberspace's dynamism and this ill-prepared cyber defense structure provides an opportunity for Russia (among other actors) to find tactical successes via cyberattacks against the U.S.. When considering factors such as budget, personnel, and training, it is unlikely that Russia will be able to outmatch the U.S. in terms of conventional military power. However, Russia has no need for advancing their conventional prowess when they can accomplish their goals through cyber avenues. The cyber domain is attractive to Russian operations not only because of their decentralized operating structure or our impaired defense methodology; it provides ample opportunity for low-risk, high-reward investments in Russian military and political advances.

Russia's unique place in the domain of cyber-warfare can be further understood by looking at their history and current attitude toward technology, the state of their modern geopolitics, and by understanding the Russian Nexus. The inherent corruption of Russia's political system allows for covert, malicious cyber operations to be carried out with relative anonymity and rapid development speed via versatile funding and project outsourcing. While this outsourcing is efficient at obfuscating operations and compartmentalizing different parts of a project, it can lead to poor execution, implementation, and maintenance of more complex cyberattacks. Since the first Gulf War, Russia has seen itself as lacking in conventional military capability and has been eager to catch up to its adversaries. Like many other nations, Russia sees the importance of Information Warfare in being able to win battles and exercise political will without physical war deployments. The landscape of cyber-warfare is dynamic, and Russia's clear advantage in this landscape is their operating speed, accomplished by taking advantage of the Russian Nexus to circumvent bureaucracy and jump straight to developing results. However, this strength has the potential to become a weakness due to the vast amounts of internal conflict and general disconnection between Russian agencies fueling operational problems on both the domestic and international stage. Regardless of relative strengths and weaknesses, one thing is clear: Russia is all-in regarding the domination of cyber-warfare. We should be too.

References

DoD. SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY 2018, SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY 2018 (2018).

Fitzgerald, M. C. (1986). Marshal Ogarkov on Modern War: 1977-1985. Revision. Center for Naval Analyses. doi: 10.21236/ada176138

Fogarty. (2019, August). TechNet Augusta 2019. TechNet Augusta 2019. Augusta.

Gaskew, B. (2019, February 21). Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget – Third Way. Retrieved from https://www.thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget

Kelly, E. (2018, July 19). Here's your guide to GRU and other Russian agencies that spy on America. Retrieved from https://www.usatoday.com/story/news/politics/2018/07/19/guide-gru-and-other-russian-agencies-spy-america/800334002/

Pifer, S. (2019, March 18). Five years after Crimea's illegal annexation, the issue is no closer to resolution. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2019/03/18/five-years-after-crimeas-illegal-annexation-the-issue-is-no-closer-to-resolution/

Smith, D. J. (2019, August). Utica College - Cyber Security Residency. Utica College - Cyber Security Residency. Utica.

Stratfor. (2013, August 8). 5 Years Later, Reflecting on the Russia-Georgia War. Retrieved from https://worldview.stratfor.com/article/5-years-later-reflecting-russia-georgia-war

©2019 REDCOM Laboratories, Inc. REDCOM, the REDCOM logo, and Sigma are registered trademarks of REDCOM Laboratories, Inc.
All other trademarks are property of their respective owners. Subject to change without notice or obligation.

REDCOM®

www.redcom.com

20191113