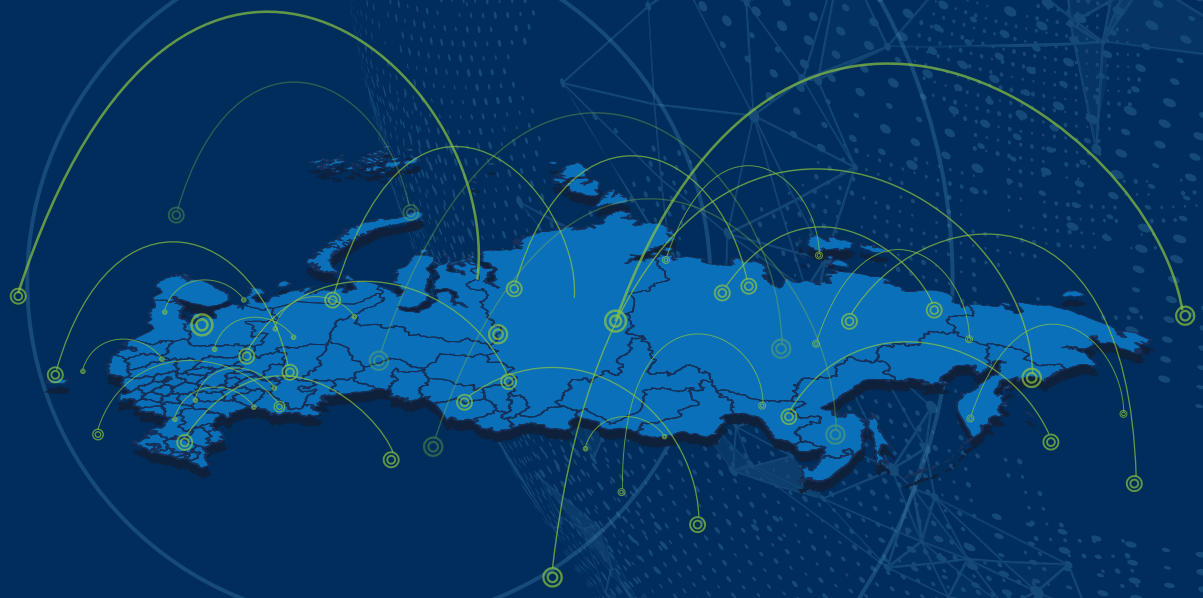
OPTIV



OPTIV THREAT ACTOR INTEL SERIES #1

RUSSIAN COMPUTER NETWORK OPERATIONS

Courtney Falk, Danny Pickens, Aamil Karimi

INTENT

The Optiv Threat Actor Intel report is a who's who primer of threat actors across the globe intended to educate readers. The report provides a synopsis of the threat actor, their history and their motivators for easier understanding.

Information in the report is a combination of intelligence gathered from public, third-party sources and Optiv's Global Threat Intelligence Center (gTIC).

INTRODUCTION

The past year saw Russian cyber operations go from the purview of intelligence professionals into the public discourse. Covert state-sponsored activities are making overt impacts on areas of everyday life. This report looks at the organization of modern Russian intelligence, focusing on those components with authority to conduct computer network operations (CNO). Russian CNO operations prove to be a concern not just of other governments but also of civilian organizations as well.

"Computer network operations" is an umbrella term used by western cybersecurity professionals. CNO covers three different types of cyber operation:

1. **Computer network exploitation (CNE**) – Networks are compromised with the goal of retrieving data for intelligence analysis.
2. **Computer network attack (CNA)** – Degrading or destroying networks and computing devices in order to affect an opponent's ability to conduct business.
3. **Computer network defense (CND)** – Defending friendly networks from the CNE and CNA actions of malicious actors.

What makes Russia an interesting CNO study are the distinctions between the nation-state actors and cybercriminal actors. There are several notable situations where cyberattacks were carried out by Russia-based cybercriminals. But at the same time, the goals and objectives of these attacks aligned with those of Russian political and military officials. Whether or not there is formal communication between the nation-state and cybercriminal sides remains a frequently discussed question without a firm answer.

HISTORY

Russia has a long history with secret police and intelligence operations. Ivan the Terrible formed one of the first documented secret police organizations almost five hundred years ago. Since Ivan, leaders from the tsars to the general secretaries also used secret police forces to assert their authority.

The 1991 Russian coup d'état presaged the dissolution of the Soviet Union. Committee for State Security (KGB) members collaborated with others inside the Communist Party to seize control. After two days the coup failed.

In the aftermath, the KGB was broken up into five large pieces to decentralize the power they had previously abused.

1. **Federal Security Service (FSB)** – Responsible for domestic surveillance and intelligence operations, including counter-intelligence.
2. **Federal Agency of Government Communications and Information (FAPSI)** – Secures Russian government communications and conducts signals intelligence (SIGINT).
3. **Border Guard Service** – Protects Russia's coast, ports, and points of entry into the country.
4. **Foreign Intelligence Service (SVR)** – Intelligence collection and operations outside of Russia.
5. **Federal Protective Service (FSO)** – Protection of government officials.

There were other, lesser known intelligence agencies along with the KGB including the Main Intelligence Dorectorate (GRU). The GRU is a military organization with authority to conduct foreign intelligence operations. Intelligence products developed from GRU intelligence are used at the national level. In addition to military intelligence, the GRU also operates Russian special operations forces (Spetsnaz).

Russian Service	American Equivalent(s)
FSB	FBI
SVR	CIA
GRU	DIA and NSA
FAPSI	NSA
Border Guard Service	DHS
FSO	Secret Service + Federal Protective Service

Table 1: Comparisons between Russian intelligence agencies and their American counterparts.

Russia's current president, Vladimir Putin, has a personal connection to Russian intelligence. Putin himself was a KGB field officer stationed in Dresden, which at the time was the communist East Germany (GDR). After a stint in St. Petersburg politics, then-president Boris Yeltsin made Putin director of the FSB.

FEDERAL SECURITY SERVICE (FSB)

The FSB was the largest piece of the KGB to survive the 1991 split. Their original charter was to conduct domestic intelligence operations similar to the national security mission of the American Federal Bureau of Investigation (FBI). In 2003, under the direction of Russian president Vladimir Putin, the FSB reabsorbed two of the other KGB splinter organizations, the FAPSI and the Border Guard Service.

The FSB is relevant to any conversation about Russian CNO because the FSB assumed the authority to conduct cyber operations from their absorption of the FAPSI in 2003.

MAIN INTELLIGENCE DIRECTORATE (GRU)

While the KGB is the most easily recognized of the Russian intelligence services, there is another major player, the Main Directorate (GRU) of the Russian Armed Forces. The GRU has authority for a wide variety of intelligence activities, but focuses on matters of military importance. Like America's National Security Agency (NSA), which is also a military organization, the GRU has authority for conducting signals intelligence (SIGINT) collection.

BACKGROUND AND CONTEXT

A SOCIO-POLITICAL ANALYSIS OF RUSSIA

There are multiple frameworks that are used within defense and military circles to analyze an opponent. DICE and PMESII are two of the most common frameworks. Both frameworks cover similar subject matter just in varying degrees of specificity. Because PMESII explicitly defines areas for information and infrastructure, two topics critical to discussing CNO, this report will use the PMESII framework. Table 2 below includes a number of statistics useful in framing Russia against the United States. Each report has a different scoring system, measuring a different facet of the socio-political fabric of a country. Numbers included in this table are representative of the score issued by that report.

Source	Metric	Russia	United States	Best
Transparency International	Corruption Perceptions Index 2017	135th of 180	16th of 180	New Zealand
ITU	ICT Development Index 2017	45th of 176	16th of 176	Iceland
World Economic Forum	Global Competitive Index 2017-2018)	38th of 137	2nd of 137	Switzerland
Portland	Soft Power 30	26th of 30	3rd of 30	France
Reporters without Borders	2017 World Press Freedom Index	148th of 180	43rd of 180	Norway

Table 2: Comparing Russia and the United States using multiple indices published by non-governmental organizations.

Comparing the different indices for Russia and the United States might lead one to assume that Russia was operating from a position of disadvantage. But this assumes that Russia values things the same way that liberal Western democracies do. Alexander Klimburg, a fellow at the Atlantic Council, makes an interesting observation based on his interactions with non-Western governmental authorities: They do not believe in the existence of a civil society (Klimburg, 2017). While this might be a hyperbolic statement, another version of it seems reasonable: Western nations and Russia have differing views on the role of their civil societies. Liberal Western democracies expect civil society to be a partner and participant in the governing process. Russia views civil society as subordinate to the will of the government. Similar attitudes are apparent in nations like China and Turkey.

POLITICAL

Russia is nominally a presidential/parliamentary democracy (Reuter & Remington, 2009). However, Russia is a de facto one-party state with the United Russia party in control of the presidency and three quarters of the Duma, Russia's parliament.

MILITARY

The Russian military is a large and fairly modern organization. Investment in large weapons development programs stagnated with the fall of the Soviet Union. Submarines rusted at docks and military units went unpaid.

Recent years show a marked change in the posture of the Russian military. In 2012, Putin announced a plan to phase out the conscript military, creating a fully professional force by 2020. The goal is a smaller, more highly trained and motivated force (Thornton, 2011).

The last decade has seen an uptick in the development of sophisticated, modern weapons systems. New, stealthy, fourth-generation fighter planes are being tested. Meanwhile strategic missile and ballistic missile submarine development has resumed. Russia is also testing its ability to project power in venues such as Syria.

ECONOMIC

Russia enjoys vast natural resources such as timber, natural gas, and petroleum. 2016 gross domestic product (GDP) for Russia tops $1.2 trillion. The depressed value of oil over the last several years has undercut the value of petroleum reserves, which in 2012 constituted 16% of GDP. Economic growth is hampered by corruption and economic sanctions levied by Western nations. Transparency International's Corruption Perception Index places Russia in 135th place .

SOCIAL

The Russian language is the eighth most commonly spoken language in the world. But Russia is far from being a monoculture. Russia is the largest nation in the world in terms of geography and that geography covers a diverse collection of peoples.

This diversity creates a degree of internal friction as demonstrated by the different conflicts in the Caucasus region.

INFRASTRUCTURE

Infrastructure in Russia has suffered from the same lack of long-term investment as the military. As shown in Table 2, information and communications technology (ICT) development trails the United States and all other Western nations.

INFORMATION

Media in Russia is controlled by the state. This includes print media like the Russian Gazette and television channels like RT (formerly known as Russia Today). Internet control is monitored by federal authorities.

Reporters without Borders, an international non-governmental organization dedicated to journalists and the media, gives Russia 148th place in its World Press Freedom Index (see Table 2), which is among the worst. This is due in part to the large number of deaths of Russian journalists. Novy Den reporter, Maxim Borodin, recently died due to a suspicious fall (BBC, 2018).

BACKGROUND AND CONTEXT

PRIVATE ENTERPRISE

Private companies exist at the whim of the state in Russia. It is not uncommon for one employee to be known to be an embedded FSB agent (Krebs, 2014).

It is in this environment that Kaspersky Labs was born. The story of Kaspersky Labs is that its namesake, Eugene Kaspersky, found himself diagnosing and fixing so many computer viruses that he put out his shingle to do so professionally. In 1987, Kaspersky graduated with a degree in mathematical engineering and computer technology from the Technical Faculty of the KGB Higher School. This education background is a part of the concern about Kaspersky's connection to Russian intelligence services.

Now Kaspersky Labs is an international computer security company. Their software runs on thousands of computers around the world. Then in 2015, Israeli nation-state hackers broke into Kaspersky Lab's corporate network (Nakashima, 2017). What they found caused them to contact their counterparts at the American NSA. What the Israelis found was an NSA CNO toolkit – specialized software designed for breaking into other computers. An NSA employee had copied the classified tools onto his/her home computer, which ran Kaspersky for anti-virus protection. Apparently, the Kaspersky software downloaded this user's files, inadvertently grabbing a copy of the sensitive software. Whether this was an opportunistic find or a part of a larger, targeted intelligence gathering operation remains unknown.

TODAY'S LANDSCAPE

CYBERCRIMINAL ACTORS

Cybercrime is a lucrative business in Russia. The former Soviet state built a strong STEM curriculum into its education and the result is a cadre of well-trained mathematicians and computer scientists with uncertain job prospects.

Russian cybercriminals span the gamut of targets and TTPs as seen in Table 3. The Russian Business Network (RBN) was known for its bulletproof hosting services, which were computers serving up botnet C2, carding forums, and illicit forms of pornography. The bulletproof part of the hosting was RBN's refusal to shutter these services when international police agencies sent take down requests. Many Russian cybercriminal groups go nameless, or perhaps are referred to using their malware of choice. FIN7 is a banking theft ring with a lengthy history whose credential stealing malware, Carbanak, is well known to reverse engineers.

Actor	Threat Actor Score[2]	Type	Status	Notable Attack(s)
Russian Business Network	53	Bulletproof hosting	Defunct	Estonian DDoS
Severa	47	Spam	Arrested	Operated the Waledac botnet
CyberVor	37	Credential theft	Active	Stole 1+ billion unique credentials
FIN7	87	Banking theft	Active	Carbanak infections

Table 3: A sample of Russian cybercriminal gangs (for more details, please reference Appendix A: Expanded Threat Actor Scores).

SOCIAL INFLUENCE/INFORMATION

Russian concepts regarding psychological warfare and information warfare differ from those of American military and intelligence agencies. Russian military thinkers refer to an idea they call, "reflexive control." The motivation behind reflexive control is that instead of directly asserting oneself via force, the controller creates a situation such that the target reacts in a calculated way.

The Internet gave a name to Russian influence operations long before their identity was made public. "The Trolls from Olgino" were known to spam forums and social media with pro-Russian messages (Olgino is a neighborhood of St. Petersburg). Recent revelations connect these professional trolls to the Internet Research Agency. The Internet Research Agency bought social media ads on both sides of inflammatory American political issues and created fake personas to espouse divisive political views. While the American presidential election of 2016 was the best known instance of Russian trolls at work, several other elections held in liberal western democracies witnessed influence operations and other "fake news."

Dates	Location	Election
June 2016	United Kingdom	European Union membership referendum ("Brexit")
Nov. 2016	United States	Presidential election
May 2017	France	Presidential election
Sept. 2017	Germany	Federal elections
Oct. 2017	Spain	Catalan independence referendum

Table 4: Elections thought to have seen Russian influence operations.

Some Russian operations go beyond just words. In what the American Department of Homeland Security and Federal Bureau of Investigation are calling GRIZZLY STEPPE, suspected Russian threat actors broke into email servers belonging to the Democratic National Committee. The emails they exfiltrated were filtered through an online persona called "Guccifer 2.0," a name which invokes an earlier cybercriminal who called himself "Guccifer" and publicly released the copied emails of prominent personalities. Guccifer 2.0 is likely a fake construct, masking sophisticated intelligence operations. The GRIZZLY STEPPE report points the finger at the Russian GRU intelligence agency. This same group is tracked by public threat intelligence firms under names such as "Fancy Bear," "Pawn Storm," and "APT28."

CROSSOVER OPERATIONS

The world of spies is sometimes described as being that of smoke and mirrors. If that is the case then the world of cybercriminal actors is murkier still. Cyber security firm, Cybereason, describes the close and continuing relationship between Russian intelligence and cybercriminal groups where the nation-state organizations task and direct the international activities of the criminal organizations (Cybereason Intel Team, 2017). It is interesting to note how the major cyberattacks of the last ten years that advanced Russian political interests were ostensibly carried out by independent criminals. What follows are a few notable examples.

ESTONIAN DDOS

Estonia existed as a Soviet Socialist Republic within the Soviet Union for decades until it regained its independence in 1991. In 2007, the Estonian government opted to relocate the graves of several Russian soldiers killed in the Second World War along with an accompanying monument. This offended the nationalist sensibilities of the Russian state. What followed was a DDoS of unprecedented scale.

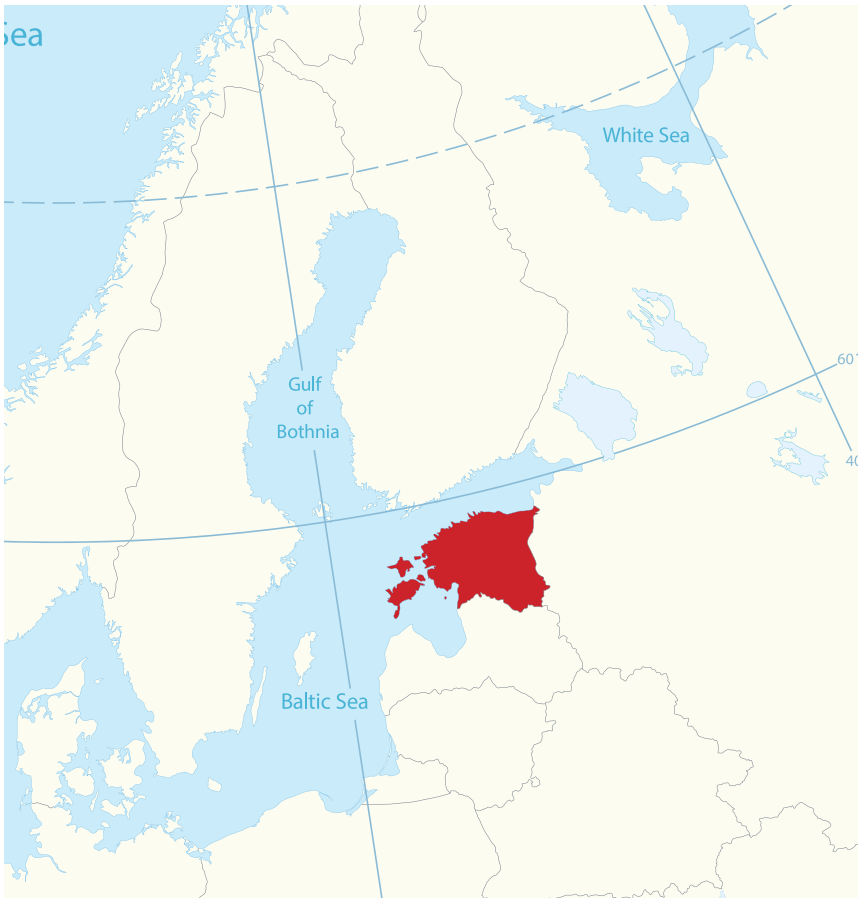


Table 5: Estonia (in red) surrounded by Russia, Scandinavia, and the other Baltic countries.

Estonia, despite being a small, formerly Soviet country, is highly informatized. National marketing campaigns advertise Estonia as a destination for high-tech software start-ups. Voting, banking, and other civil tasks can all be done online via the X-Road system. This X-Road system ground to a halt under the DDoS attack, but was effectively restored when Estonia temporarily disconnected itself from the wider Internet.

Now Estonia hosts the NATO cyber security center where soldiers from across Europe and North America gather to practice cyber defense skills. The government also formed a "cyber militia" who are able to help respond to large-scale cyberattacks in the future. This semi-professional force is a necessary step for a country that doesn't have the resources to field a CNO capability similar to that of America's National Security Agency of the United Kingdom's Government Communications Headquarters.

GEORGIAN WAR

Within the borders of the modern-day state of Georgia are two ethnic enclaves known as Abkhazia and South Ossetia. The central Georgian government is unable to directly assert their control over these regions. In fact, the Russian government not only recognizes them as independent, but has Russian soldiers stationed in both locations as peacekeeping forces.

Table 6: Georgia and the breakaway regions of Abkhazia and South Ossetia.

When Georgian forces clashed with South Ossetian forces in 2008, the Russians reacted in support of their Ossetian allies. What resulted was a rout of the Georgian army within the borders of Georgia itself. Preceding this military action was a cyberattack against Georgian government and public web sites.

The cyberattack was allegedly carried out by "patriotic Russian hackers." The fact that the attack immediately preceded a kinetic military action, and degraded the digital capabilities of the Georgian government, aligns with Russian goals. The fact that the attacks were carried out by non-state actors gives the Russian government plausible deniability.

CRIMEA/UKRAINE

Crimea was the second time that cyber operations occurred seemingly in concert with kinetic military operations. Russian military forces occupied the Crimean Peninsula, and instigated ethnically Russian Ukrainian rebels to take up arms against the government in Kiev. All this was caused by the fall and exile of the pro-Russian president of Ukraine.

Table 7: Ukraine (in purple) with Russia to the east and Crimea (in red) on the Black Sea.

CONCLUSIONS

Russia utilizes CNO as a component of a wider information operations strategy. The Russian philosophy and mindset behind information operations and psychological operations differ significantly from those found in Western military circles. Russia employs its CNO capabilities on a wider scale than other nation-states because CNO is an asymmetric capability, which is a way for Russia to compensate for its diminished conventional military capabilities.

Public exposure doesn't necessarily dissuade Russian threat actors. A January 2018 spear phishing campaign targeted the United States Senate with the goal of stealing emails. The attacks were attributed to the Russian "Fancy Bear" threat actor group by security firm, Trend Micro (Hacquebord, 2018). If this sounds similar to the hack of the Democratic National Committee, Trend Micro agrees. Trend Micro attributes this US Senate campaign to the same actors who perpetrated the DNC attack. DHS and FBI attributed the DNC attack to the GRU.

A word of caution: Russian information operations have become a kind of boogeyman. Such hypothetical operations may be invoked with little or no proof as political rhetoric. We anticipate with high confidence that Russian information operations will continue targeting political, military, and critical infrastructure objectives for the foreseeable future. Organizations doing business in Russia, in areas of Russian interest such as Ukraine, or in industries important to the Russian economy such as petroleum, could inadvertently find themselves targeted by the hybrid Russian CNO machine.

REFERENCES

BBC. (2018, April 16). Russian reporter Borodin dead after mystery fall. Retrieved from BBC: http://www.bbc.com/news/world-europe-43781351

Brandom, R. (2014, May 29). Cyberattacks spiked as Russia annexed Crimea. Retrieved from The Verge: https://www.theverge.com/2014/5/29/5759138/malware-activity-spiked-as-russia-annexed-crimea

Cybereason Intel Team. (2017, June 5). Russia and nation-state hacking tactics: A report from Cybereason Intelligence Group. Retrieved from Cybereason: https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity

Department of Homeland Security and Federal Bureau of Investigation. (2016). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved from https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Emmott, R. (2017, November 13). Spain sees Russian interference in Catalonia separatist vote. Retrieved from Reuters: https://www.reuters.com/article/us-spain-politics-catalonia-russia/spain-sees-russian-interference-in-catalonia-separatist-vote-idUSKBN1DD20Y

Fried, D. (2017, December 14). McMaster Accuses Russia of Subversion, Kremlin Reacts. Retrieved from Atlantic Council: http://www.atlanticcouncil.org/blogs/new-atlanticist/mcmaster-accuses-russia-of-subversion-kremlin-reacts

Global Threat Intelligence Center. (2014, March 7). Behind the Curtains of New War: Bringing Cyber War to the Crimean Peninsula. Retrieved from Optiv: https://www.optiv.com/blog/behind-the-curtains-of-new-war-bringing-cyber-war-to-the-crimean-peninsula

Greenberg, A. (2017, June 20). How an entire nation became Russia's test lab for cyberwar. Retrieved from Wired: https://www.wired.com/story/russian-hackers-attack-ukraine/

Hacquebord, F. (2018, January 14). Update on Pawn Storm: New Targets and Politically Motivated Campaigns. Retrieved from Trend Micro: https://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns/

Hannam, K. (2017, November 10). Russia 'Pushed Fake News' in Catalonian Independence Fight. Retrieved from Fortune: http://fortune.com/2017/11/10/russian-role-catalonia-independence/

Harding, L. (2016). A Very Expensive Poison: The Definitive Story of the Murder of Litvinenko and Russia's War with the West. Guardian Faber Publishing.

Harris, S. (2018, January 12). Russian hackers who compromised DNC are targeting the Senate, company says. Retrieved from Washington Post: https://www.washingtonpost.com/world/national-security/russian-hackers-who-compromised-the-dnc-are-targeting-the-us-senate/2018/01/12/7e9169ce-f7a9-11e7-91af-31ac729add94_story.html?utm_term=.acd26c8bacbb

Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. New York: Penguin Press.

Krebs, B. (2014). Spam Nation: The Inside Story of Organized Cybercrime - from Global Epidemic to Your Front Door. Sourcebooks.

McKirdy, E. (2017, June 2). Putin: 'Patriotic' Russian hackers may have targeted US election. Retrieved from CNN: http://www.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html

Nakashima, E. (2017, October 10). Israel hacked Kaspersky, the NSA that its tools had been breached. Retrieved from The Washington Post: https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.7cd2803b7602

Popov, M., & Rotenberg, O. (2017, December 18). Kremlin's new cyber weapons spark fears and fantasies. Retrieved from Digital Journal: http://www.digitaljournal.com/news/world/kremlin-s-new-cyber-weapons-spark-fears-and-fantasies/article/510264

Project Grey Goose. (2008, October 17). Russia/Georgia Cyber War - Findings and Analysis. Retrieved from Scribd: https://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report

Reuter, O. J., & Remington, T. F. (2009). Dominant Party Regimes and the Commitment Problem: The Case of United Russia. Comparative Political Studies, 501-526.

Thomas, T. L. (2011). Recasting the Red Star: Russia Forges Tradition and Technology through Toughness. Fort Leavenworth, KS: Foreign Military Studies Office.

Thornton, R. (2011). Military Modernization and the Russia Armed Forces. Carlisle, PA: Strategic Studies Institute.

APPENDIX A: EXPANDED THREAT ACTOR SCORES

The Optiv Global Threat Intelligence Center (gTIC) tracks several different threat actors and has created a proprietary metric for scoring and comparing these threat actors. These scores are meant to serve as a quick reference for decision makers.

Each threat actor is evaluated according to six (6) dimensions that measure three (3) areas of capabilities: Technical, Operations, and Preparation. These dimensions were selected to represent observable patterns and behaviors on the part of the threat actor. Once the threat actor is scored according to these six dimensions, a total score is computed. This final, cumulative score is useful as a quick glance to evaluate and compare threat actors.

Want to learn more?

Insight on Cyber Threat Intelligence is an ongoing series of thought leadership at Optiv. Click the links below to download other corresponding materials on the subject.

2018 Cyber Threat Intelligence Estimate

Cyber Threat Intelligence- as-a-Services At-a-Glance Brief

1144 15th Street, Suite 2900
Denver, CO 80202
800.574.0896 | www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

6.18 | F1