

BEARING WITNESS:

UNCOVERING THE LOGIC BEHIND RUSSIAN MILITARY CYBER OPERATIONS

“ As the most technically advanced potential adversary in cyberspace, Russia is a full-scope cyber actor, employing sophisticated cyber operations tactics, techniques, and procedures against U.S. and foreign military, diplomatic, and commercial targets, as well as science and technology sectors. Russia will likely continue to integrate cyber warfare into its military structure to keep pace with U.S. cyber efforts, and conduct cyberspace operations in response to perceived domestic threats. Also, Russian cyber actors have demonstrated the intent and capability to target industrial control systems found in the energy, transportation and industrial sectors. ”

– *Paul Nakasone, then-nominee for Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service (2018)*¹

“ This is what I can say about cyber-attacks or war of words in the press and other issues. Action always causes reaction. Always. ”

– *Vladimir Putin, President of the Russian Federation (2018)*²

Table of Contents

EXECUTIVE SUMMARY.....	1
INTRODUCTION.....	3
ANALYTIC FRAMEWORK.....	5
CASE STUDIES	11
WHAT'S NEXT	37
CONCLUSION	39
PROTECT YOUR ORGANIZATION	40
APPENDIX A: METHODOLOGY	42
APPENDIX B: INDUSTRY NAMES FOR GRU-LINKED ACTIVITY GROUPS	43
APPENDIX C: RELEVANT TOOLS USED BY GRU OPERATORS	46
APPENDIX D: RELEVANT GRU PERSONAS	49
ENDNOTES	51

This report is based solely on open-source research and analysis and was completed for research purposes. The opinions outlined within do not represent the official positions of Booz Allen Hamilton, its officers, directors, or shareholders.



ДОМ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

The House of the Government of the Russian Federation

Executive Summary



For more than a decade, cyber operations linked to Russia's military intelligence agency (GRU^a) have disrupted elections, damaged economies, and endangered people in dozens of countries. Among much else, they have twice turned off the lights in Ukraine, unleashed a globally destructive wiper, and leaked information to smear athletic associations, journalists, and politicians. The methods and tools used in these operations are well documented, but a systematic explanation for why these operations occur is lacking.

This report demonstrates a consistent reusable framework to explain the GRU's thought process based on Russia's military doctrine, a public policy document. Specifically, this report shows the fundamental connection between GRU-attributed cyber activity and the GRU's mission to monitor, neutralize, and counter certain publicly enumerated circumstances and actions that endanger Russian military security. The GRU executes its mission using methods consistent with declared strategic concepts.

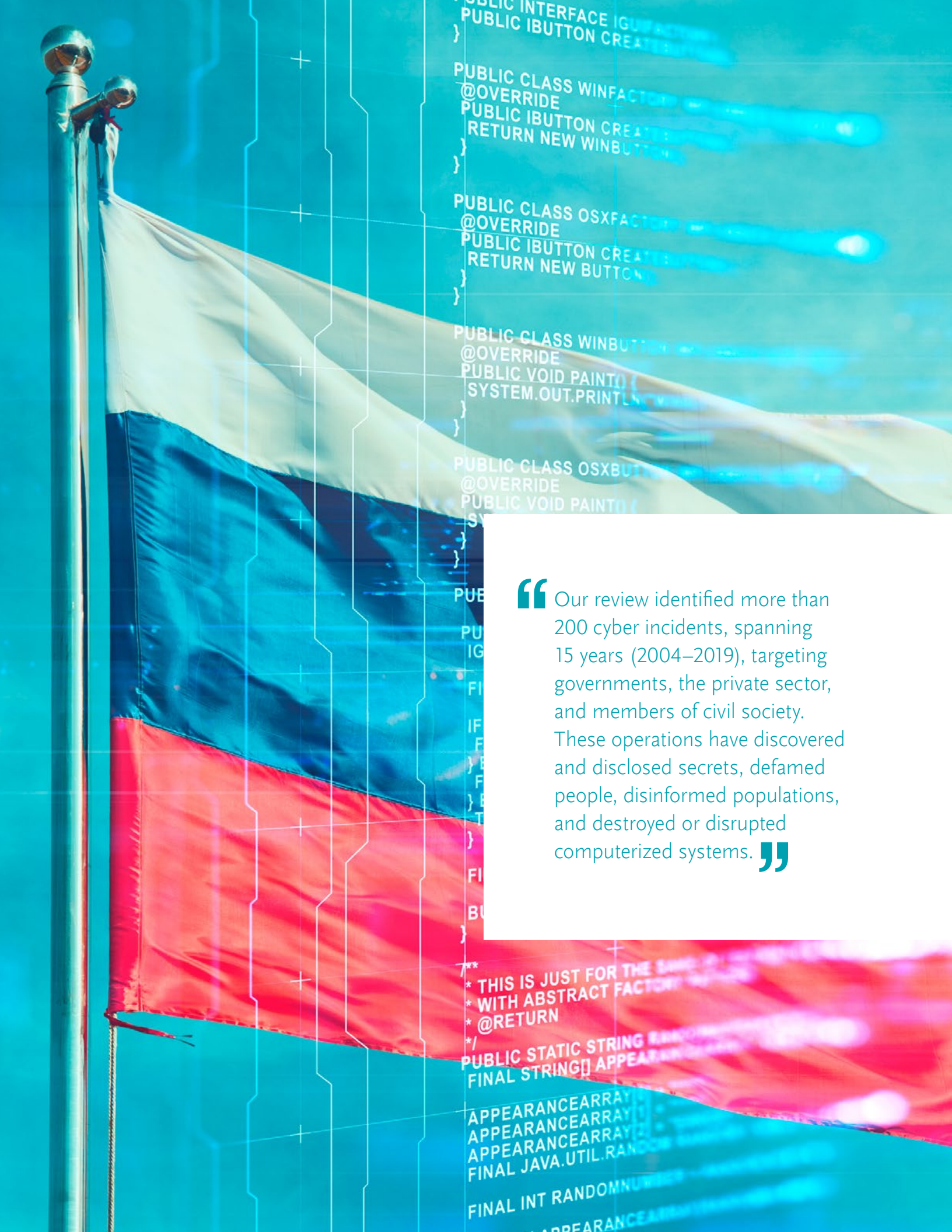
Defending against cyber operations—like those of the GRU—demands understanding not just how these operations occur but, more importantly, why. Fundamentally, state-aligned adversaries are organizations tasked with responding to national mission requirements in a manner consistent with strategic doctrine.^b By understanding why adversaries act, defenders can better anticipate when, where, and in what form those actions may occur and take deliberate action to mitigate their risk based on that insight.

CHALLENGE

Compliance and recovery efforts alone fail to prepare for or respond to such determined, targeted threats. By understanding what we are up against, we can lift the haze and afford ourselves the ability to make pointed, deliberate, and informed risk management decisions throughout the security lifecycle—from the hands-on-keyboards network defenders to the C-suite.

^a The **Main Directorate of the General Staff of the Armed Forces** is widely known within Russia and abroad by its former acronym, the GRU, derived from its historic name Glávnoye Razvedyvatel'noje Upravléniye (Main Intelligence Directorate or GRU). The acronym GU is technically more accurate for its present name Glávnoye Upravléniye (Main Directorate), but it is infrequently used.

^b In this report, the term **state** is used in the political science sense of the totality of permanent power structures representing and governing people in a territory (e.g., in the sense of "state secrets" or "head of state"), not in the sense of subordinate territorial units unless being explicitly discussed in the context of the United States.



“ Our review identified more than 200 cyber incidents, spanning 15 years (2004–2019), targeting governments, the private sector, and members of civil society. These operations have discovered and disclosed secrets, defamed people, disinformed populations, and destroyed or disrupted computerized systems. ”

```
** THIS IS JUST FOR THE SAKE OF COMPLETION  
* WITH ABSTRACT FACTORY  
* @RETURN  
*/  
PUBLIC STATIC STRING RANDOMNUMBER  
FINAL STRING[] APPEARANCEARRAY  
APPEARANCEARRAY  
APPEARANCEARRAY  
FINAL JAVA.UTIL.RANDOMNUMBER  
FINAL INT RANDOMNUMBER  
APPEARANCEARRAY
```

Introduction



The Main Directorate of the General Staff of the Armed Forces (GRU) is an agency within the Russian military responsible for intelligence production and special forces operations.³ It produces insights and recommendations for senior Russian government members about circumstances that may impact Russian military security. The GRU also conducts covert espionage, influence, and sabotage operations, using kinetic and digital means.

The GRU is not the only Russian government agency that conducts cyber operations, but it is Russia's most thoroughly documented and consistently publicly implicated cyber operations organization. In recent years, the United States, its allies, and its partners have repeatedly, explicitly, and unequivocally attributed numerous cyber events, cover personas, and security industry group names to the GRU.^c These governments' assessments are often supported by substantial declassified evidence and closely aligned with other published private sector threat reporting.

With this common understanding in mind, we have taken a comprehensive look at previously disclosed activity that can now be attributed to the GRU. Numerous governments, security firms, researchers, reporters, academics, and victims have released reports detailing different facets of the GRU's activities. Our review identified more than 200 cyber incidents, spanning 15 years (2004–2019), targeting governments, the private sector, and members of civil society. These operations have discovered and disclosed secrets, defamed people, disinformed populations, and destroyed or disrupted computerized systems.

In reviewing these reports, it became clear that while the GRU's tools and methods are well known, a more fundamental understanding of the GRU's decision-making process is elusive. As defenders, we must understand the decision-making process in order to explain why these operations occurred, predict what may be next, and prepare accordingly.

UNDERSTANDING RUSSIA'S CYBER OPERATIONS

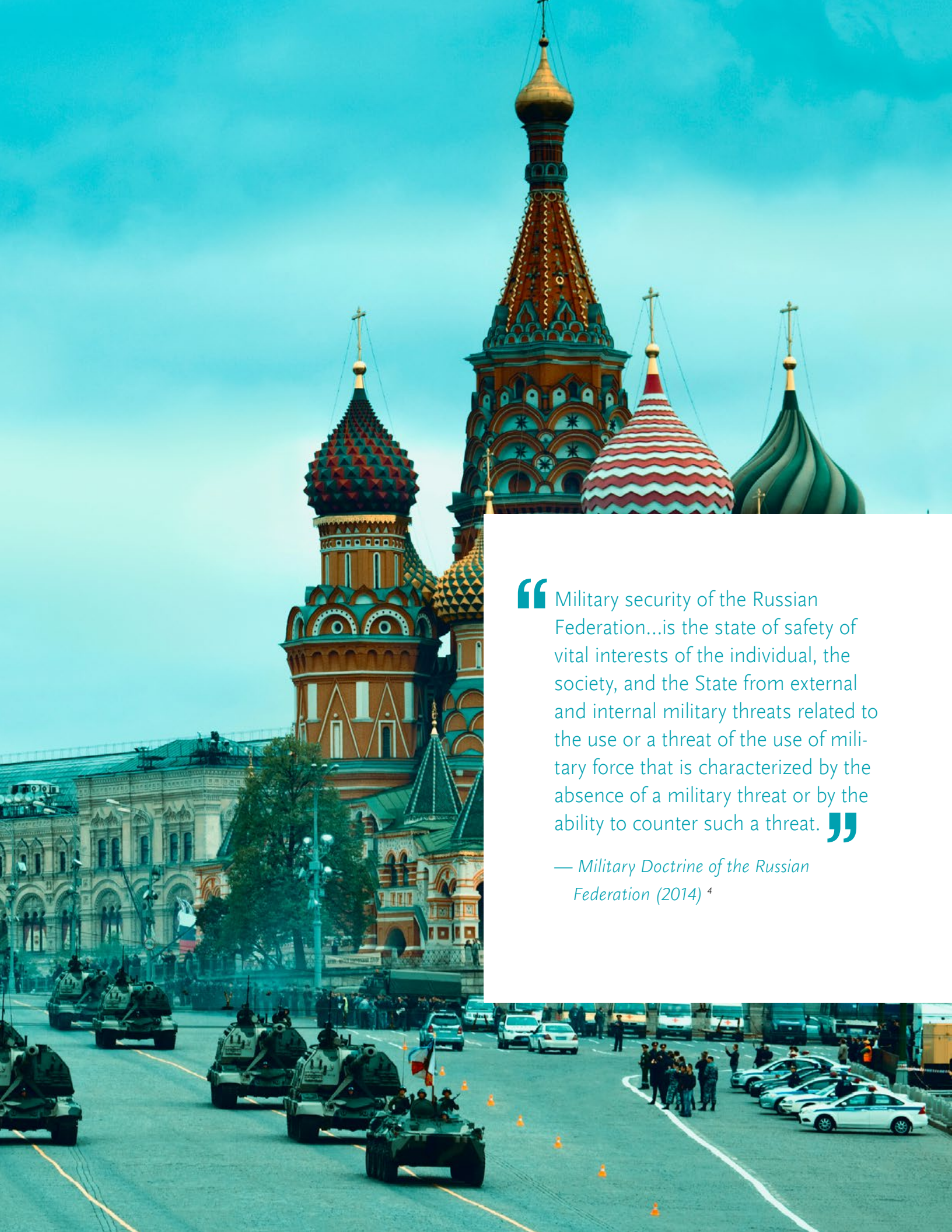
We must analyze the GRU's cyber operations as the work of a government agency, responding to mission requirements and acting in ways consistent with relevant doctrine. This report serves the following purposes:

Establish a framework for understanding the Russian military's cyber operations: Using published Russian military doctrine, we identified the specific circumstances that, by policy, demand a Russian military response. Then, we outlined the spectrum of the military's responses also described in doctrine and the strategic objectives of those responses.

Recontextualize historical cyber activity: We evaluated the alignment of historical GRU-linked cyber operations' timing, target selection, and tactical characteristics with Russian military doctrine.

Predict future activity: We assessed how the GRU may engage its cyber capabilities to respond to Russia's evolving strategic military challenges.

^c Many governments have issued statements attributing cyber activity, personas, and industry threat activity cluster names directly to the GRU. In this report, we rely on attributions made by the United States, the United Kingdom, Australia, New Zealand, Canada, the Netherlands, Estonia, Lithuania, Macedonia, Germany, Georgia, Bulgaria, and Ukraine, among others.



“ Military security of the Russian Federation...is the state of safety of vital interests of the individual, the society, and the State from external and internal military threats related to the use or a threat of the use of military force that is characterized by the absence of a military threat or by the ability to counter such a threat. ”

— *Military Doctrine of the Russian Federation (2014)* ⁴

Analytic Framework



The following section establishes a framework for understanding how the Russian military decides to conduct cyber operations, the forms they may employ, and the objectives of these operations. Specifically, this section covers the following topics:

- The specific circumstances posing a risk or threat to Russia's security requiring a military response
- The Russian military's stated responses to military risks and threats
- How Russia perceives the strategic importance of its cyber operations

RUSSIAN MILITARY DOCTRINE AND VIEWS ON MODERN MILITARY CONFLICT

Russia periodically publishes a key strategic planning document titled "The Military Doctrine of the Russian Federation" (hereafter, the "Military Doctrine"). It publicly affirms the military security concepts, concerns, and focuses expected to guide all Russian Armed Forces^d activities in the coming years. The current version, published in December 2014, notes that its authors took into consideration the contents of several other long-term Russian planning documents for periods "up to 2020," making it highly likely that a new Military Doctrine will be published in 2020 or soon thereafter.⁴

The 2014 doctrine contains two sections that are critical to assessing GRU cyber operations. These sections respectively identify the specific circumstances to which Russian Armed Forces must respond and the manners in which modern armed forces act. Then by extension, these sections identify the circumstances where the Russian military is highly likely to conduct cyber operations and a spectrum of characteristics expected to be present in these operations. Understanding this framework can serve as a model for contextualizing historical or ongoing GRU cyber activity and predicting future activity.

AGGREGATION OF OPEN-SOURCE FINDINGS

Previously published reports and analysis of GRU-linked operations have been critical to developing this report's findings. These sources are fully cited inline, giving specific credit to their authors. Each of these accounts provided different crucial components of the strategic context that this report assesses.

^d The **Armed Forces of the Russian Federation**, or colloquially the "Russian military," are Russia's national uniformed armed services. Per Russian law, their responsibility is "to repel aggression directed against the Russian Federation, to armedly protect the integrity and inviolability of the territory of the Russian Federation, as well as to carry out tasks in accordance with international treaties of the Russian Federation." (Source: Russian Federal Law of May 31, 1996, No. 61-FZ "On Defense").

CONDITIONS DEMANDING A RUSSIAN MILITARY RESPONSE

The Military Doctrine identifies specific activities or circumstances that *generally* create conditions for armed conflict (“military risks”)^e or actions that may *directly* lead to armed conflict (“military threats”). It is the Russian military’s explicit mission to respond to these specific risks and threats. In the Case Studies portion of this report, we will explain what each condition is in greater detail, assess why Russia is wary of each condition, and show how assessed GRU-linked cyber operations likely demonstrated Russian Armed Forces’ efforts to neutralize or balance these risks and threats.

MILITARY RISKS

The Military Doctrine enumerates 18 military risks. Most of these risks are consistent with previous Military Doctrines, indicating that core Russian security concerns are stable and remain useful for long-term prediction of future threat activities. The doctrine does not claim that these activities or conditions are presented in a prioritized order, and we assess no prioritized pattern in their order.

EXTERNAL MILITARY RISKS

(Our assessment of the Russian Military Doctrine §11.12[a]–[n])

INTERNAL MILITARY RISKS

(Our assessment of the Russian Military Doctrine §11.13[a]–[d])

MILITARY THREATS

The Military Doctrine identifies five military threats. These threats constitute other states’ diplomatic or military actions deemed deliberately hostile to Russian interests, that Russia views as direct precursors to an armed conflict. It is critical that the Russian Armed Forces take steps to neutralize or counter these actions or circumstances to prevent such a conflict.

(Our assessment of the Russian Military Doctrine §11.14[a]–[e])

EXTERNAL MILITARY RISKS

- Expansion and strengthening of North Atlantic Treaty Organization (NATO)
 - Global or regional destabilization
- Deployment of military forces adjacent to Russia or its allies
 - Undermining of Russian strategic deterrence capabilities
- Violation of Russia’s or allies’ territorial integrity or sovereignty
 - Proliferation of weapons of mass destruction and missile technology
- Failure to comply with international agreements and treaties
 - Armed conflict adjacent to Russia or its allies
- Unauthorized use of foreign military force adjacent to Russia or its allies
 - Growth of transnational non-state threats like terrorism or organized crime
- Growth of ethnic, religious, or cultural disagreements over territorial borders
 - Illicit use of cyber or information operations against Russia or its allies
- Establishment of hostile states adjacent to Russia
 - State-sponsored subversive activities targeting Russia

INTERNAL MILITARY RISKS

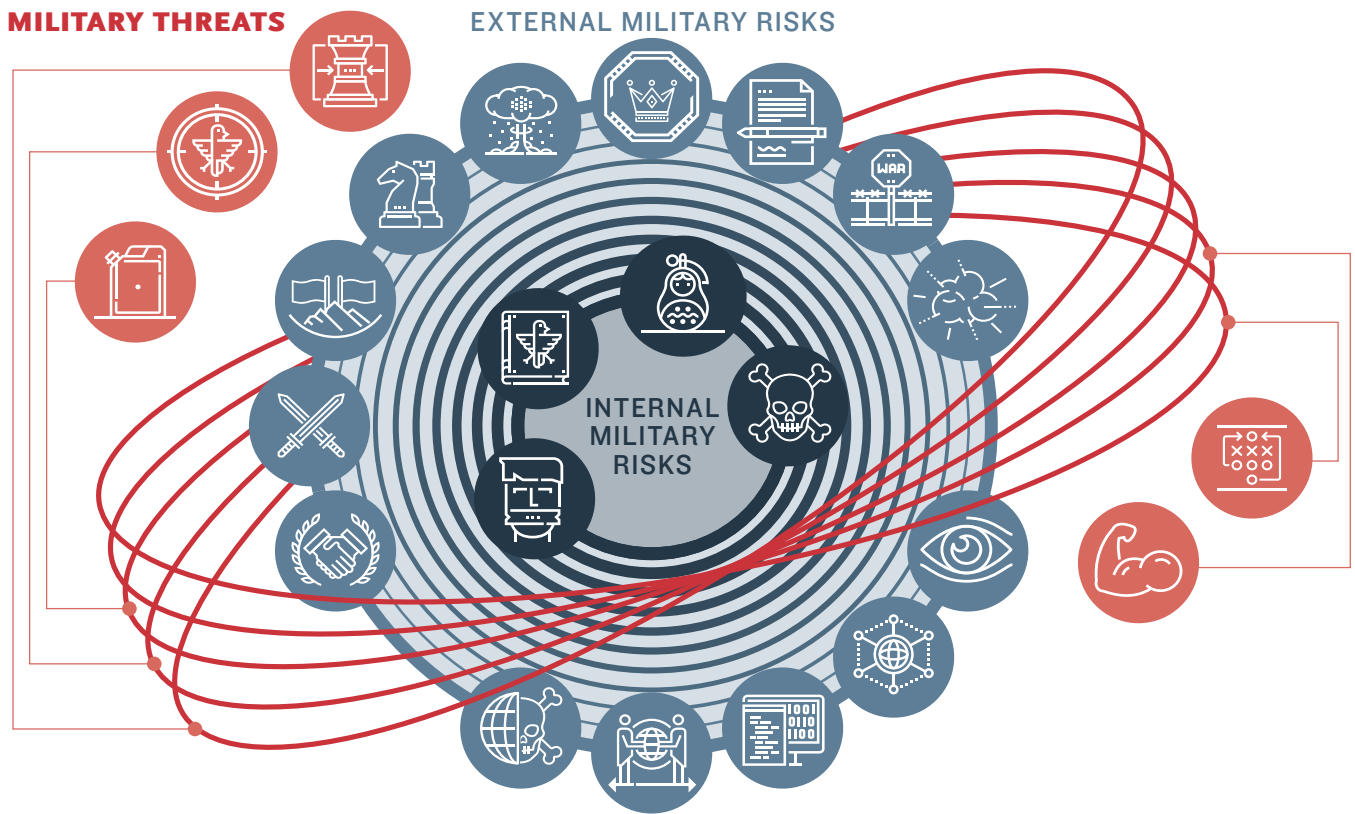
- Provocation of Russian political strife
 - Separatist and ethno-religious terrorism
- Undermining of Russian historical, spiritual, and patriotic traditions
 - Provocation of Russian cultural strife

MILITARY THREATS

- Sharp deterioration of interstate relations
 - Disruption of key Russian military capabilities or critical sectors
- Support of armed insurrection in Russia or its allies
 - Use of military force during exercises adjacent to Russia or its allies
- Heightened combat readiness

^e The Russian government’s official English-language translation of the Military Doctrine translates the term “опасности” (opasnosti) as “risks.” Unofficial translations, such as in much English-language academic discourse on the doctrine, tend to translate the term as “dangers.”

RUSSIA'S 23 PRINCIPAL ACTIONS AND CONDITIONS THAT MAY PRECEDE AN ARMED CONFLICT



Based on assessment of the Russian Military Doctrine



MILITARY RESPONSES TO RISKS AND THREATS

The Russian Military Doctrine describes key ways in which states currently avoid or resolve conflicts using military force. We assess that, in articulating these elements of modern military conflict, Russia has authorized its military to engage in any of these activities to identify and respond to potential and concrete military risks and threats.

IDENTIFY AND ASSESS POTENTIAL RISKS AND THREATS


The Military Doctrine requires continuous evaluation of the global political, diplomatic, and military environment to identify emerging military risks or threats. This mission primarily manifests as espionage, including through the use of modern technical means and information technologies.

RESPOND TO CONCRETE RISKS AND THREATS

Once a risk or threat is identified, the military must respond. Nuclear weapons and conventional military power remain the foundation of Russian national security. That backstop enables the military to support a whole-of-government fusion of hard and soft power to implement national security policy and secure strategic interests. These types of activities provide operational flexibility with a reduced risk for large-scale military confrontation or other unacceptable costs.⁵

Military engagement beneath the level of armed conflict is therefore a constant multidimensional struggle between states, with reduced emphasis on direct battlefield engagement and greater emphasis on nonkinetic measures to achieve military security goals. The Military Doctrine and other supporting documents supply an operational concept characterized as hybrid-warfare. These activities typically integrate special operations forces and nonkinetic political, economic, or informational measures to shape an adversary's social and political environment.

IDENTIFY AND ASSESS POTENTIAL RISKS AND THREATS

CHARACTERISTICS OF MILITARY ENGAGEMENT	CONCEPT	CYBER OPERATION SIGNIFICANCE
 AWARENESS OF POTENTIAL MILITARY RISKS AND THREATS	The ongoing use of technical means to collect information to identify emerging military risks and threats at the regional and global level.	Cyber operations are used to conduct espionage against political and military targets.

(Our assessment of the Russian Military Doctrine §III, 21[a])

RESPOND TO CONCRETE RISKS AND THREATS

CHARACTERISTICS OF MILITARY ENGAGEMENT	CONCEPT	CYBER OPERATION SIGNIFICANCE
 WIDESPREAD USE OF ADVANCED WEAPONS AND TECHNOLOGIES	The use of a broad range of weapons that employ advanced technologies such as computerization, directed energy, robotics, and unmanned flight.	Cyber operations' tools may be advanced military technologies that provide an advantage over other states that lack the technical or financial capacity to develop, acquire, or defend against them.
 WARFARE IMPACTING THE ENTIRE DEPTH OF AN ENEMY'S TERRITORY SIMULTANEOUSLY	The ability to cause widespread harm to an adversary across its physical or digital battlefield.	Cyber operations should be able to cause widespread harm to a targeted country's computerized devices.
 PRECISE DESTRUCTIVE ATTACKS	The ability to selectively destroy targets rather than cause indiscriminate damage.	Cyber operations should be able to cause highly targeted destruction with precise outcomes.
 REDUCED TIME TO LAUNCH MILITARY OPERATIONS WITH PREEMPTIVE ACTIVITIES	The time between the appearance of a cause for action and acting must be minimized.	Precise destructive cyber attacks normally have protracted timelines. Preemptive establishment of persistent access to high-value digital and computerized targets ("prepping the battlefield") is thus necessary.
 GLOBAL COMPUTERIZED COMMAND AND CONTROL	The use of computer systems to provide unified situational awareness, enabling unified decision among dispersed military forces. Subordinate forces can take initiative with surprise, decisiveness, and aggressiveness.	Cyber operators are empowered to take rapid, decisive action.
 CREATION OF PERMANENT WAR ZONES	Modern warfare creates a state of constant conflict, denying the adversary an opportunity to regroup and reassess, increasing the adversary's stress and confusion.	Cyber operations can maintain a state of constant conflict with limited risk of escalation.
 IRREGULAR AND PRIVATIZED WARFARE	The involvement of irregular or nonstate combatants in warfare, encompassing militias, terrorists, and private military companies.	Cyber operations can use hired contractors, mercenaries, or other nonstate actors to achieve military outcomes. This characteristic also includes regular military operators' use of fake nonstate personas to accomplish military objectives.
 INDIRECT AND ASYMMETRIC WARFARE	The ability to neutralize threats without deploying a parity of forces.	Cyber operations typically need fewer forces and less materiel than kinetic warfare.
 MANIPULATION OF SOCIAL OR POLITICAL ENVIRONMENT	The attempt to influence, control, or instigate political and social movements, with the objective of either weakening the opponent socially or installing friendlier politicians.	Cyber operations can bolster political and social manipulation efforts, such as harming the reputation of political and social targets with provocative data leaks and disinformation.

(Our assessment of the Russian Military Doctrine §II, 15[a]–[j])



HYBRID WARFARE AS INFORMATION CONFRONTATION

The military's use of hybrid warfare reflects a popular Russian strategic paradigm known as "information confrontation."^{6, 7, 8} Within this paradigm, international relations is a constant struggle for dominance of what is known, perceived, believed, or emotionally felt. More granularly, states conflict over information itself (known as informational-psychological effects) or the means by which it is held, transmitted, or processed (known as informational-technical effects).

This context of this information confrontation concept illuminates our understanding of the GRU and its cyber operations:

Mission and Objectives: Beyond traditional espionage, GRU operations should be considered as part of Russia's vision of a long-term confrontation over beliefs, understanding, and emotions that impact Russia's ability to advance its policy vision and secure its strategic interests. GRU operations' short-term effects, such as how long an attack disrupts power distribution, are of secondary importance to their ability to signal, penalize, and emotionally influence target populations.

Organization: Public sources generally track most GRU cyber activities as two mission-focused activity clusters that mirror the dual aspects of informational confrontation, with the division covering informational-psychological effects most commonly referred to as APT28 and the division covering informational-technical effects most commonly referred to as Sandworm. Though their infrastructure and toolsets are usually separate and distinct, their occasional overlaps serve as one publicly observable indicator of their bureaucratic interconnection. In this report we treat all GRU-linked activity groups collectively as the "GRU operators" because this report's framework analyzes the GRU as a singular entity using multiple capabilities to advance its mission. A list of relevant industry threat group names appears in Appendix B.

Case Studies

We assess that GRU cyber activity consistently reflects the agency's explicit purpose to monitor, neutralize, and counter the 23 risks and threats to Russian military security outlined in its Military Doctrine. This section evaluates, within the context of the Military Doctrine, 33 case studies about cyber activity that public sources link to GRU operators. Furthermore, for each risk and threat, we assess the reasons why Russia likely considers these initiating circumstances or actions to be core military security concerns.

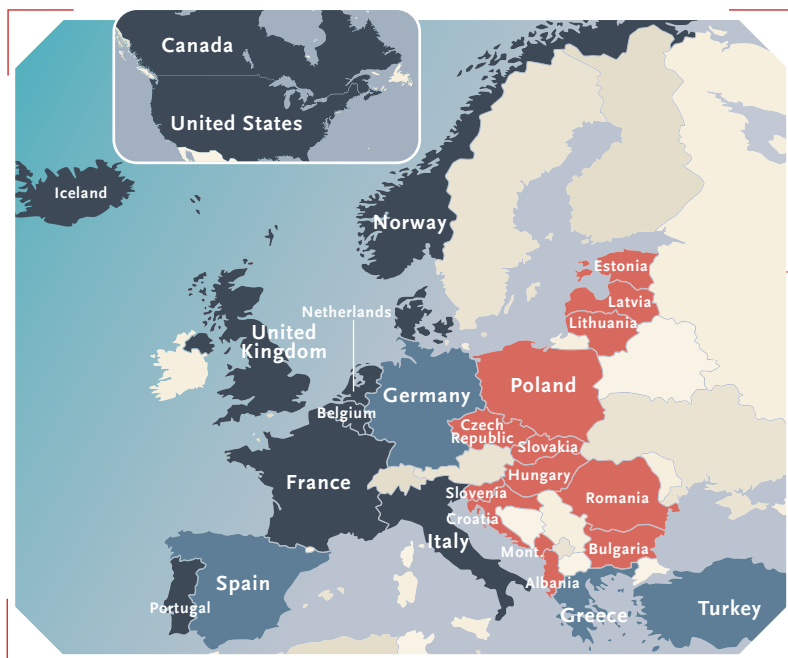
EXTERNAL MILITARY RISKS



EXPANSION AND STRENGTHENING OF NATO

Russia has long firmly opposed NATO's expansion into Eastern Europe and Central Asia. Since the end of the Cold War, Russian leaders and core strategic documents have consistently stated that Europe's security must be shaped by a principle of "equal and indivisible security."^{9, 10, 11} Essentially, Russia argues that all sovereign states have an equal right to security, and changes to their security postures should be considered collectively to prevent a destabilizing security imbalance.¹² For this reason, Russia considered joining NATO in the mid-1990s, but noted that its potential membership must preclude NATO from expanding toward Russian borders.¹³

NATO's continued expansion into Eastern Europe despite this ultimatum has driven a wedge into Russia's relations with the West. Many former Soviet states joined the alliance between 1999 and 2004. In 2007, the U.S. unsuccessfully asked its NATO allies to offer major Russian neighbors Ukraine and Georgia NATO membership, prompting Russian President Vladimir Putin to declare that NATO was now Russia's "enemy."¹⁴ Russia has continued to stridently oppose NATO's continued expansion into remaining unaligned parts of Eastern Europe, like the Balkans.



NATO MEMBERSHIP 1945–POST COLD WAR

COLD WAR ERA (1945–1991)

JOIN DATE	COUNTRY
8/24/1949	Belgium
8/24/1949	Canada
8/24/1949	Denmark
8/24/1949	France
8/24/1949	Iceland
8/24/1949	Italy
8/24/1949	Luxembourg
8/24/1949	Netherlands
8/24/1949	Norway
8/24/1949	Portugal
8/24/1949	United Kingdom
8/24/1949	United States
JOIN DATE	COUNTRY
2/18/1952	Greece
2/18/1952	Turkey
5/08/1955	Germany
5/30/1982	Spain

POST COLD WAR ERA (1991→)

JOIN DATE	COUNTRY
3/12/1999	Czech Republic
3/12/1999	Hungary
3/12/1999	Poland
3/29/2004	Bulgaria
3/29/2004	Estonia
3/29/2004	Latvia
3/29/2004	Lithuania
3/29/2004	Romania
3/29/2004	Slovakia
3/29/2004	Slovenia
4/01/2009	Albania
4/01/2009	Croatia
6/05/2017	Montenegro



Case Studies: Montenegro Joins NATO (2016 –2017)

ATTEMPTS TO PREVENT THE RE-ELECTION OF NATO-FRIENDLY POLITICIANS (OCTOBER 2016)

Montenegro has steadily veered toward NATO and the West since breaking away from Russia’s partner¹⁵ Serbia in 2006. Russia unsuccessfully used its soft power to bolster ties with the newly independent country—promoting their shared Orthodox heritage, investing heavily in many sectors, and sending tourists who account for a quarter of Montenegro’s visitors.¹⁶

In October 2016, Montenegro held parliamentary elections that would determine whether its pro-West government would remain in power and complete the NATO membership process or the Russia-friendly opposition would ascend, scuttling the process. Montenegro and the United Kingdom (UK) allege that Russia, acting via GRU agents, attempted to disrupt this pivotal election using hybrid-warfare tactics, consistent with the Military Doctrine’s concept of modern military conflict.^{17, 18, 19}

Manipulation of social or political environment:

Throughout the three days leading up to the election, Russian operators allegedly²⁰ orchestrated distributed denial-of-service (DDoS) attacks²⁰ that disrupted media websites, the country’s largest telecom (Montenegrin Telekom), a democracy-promoting nongovernmental organization (NGO) monitoring the election (Centre for Democratic Transition), and the Democratic Socialists Party of Montenegro.²¹ Additional unattributed DDoS attacks targeted the Montenegrin government’s web portal for two days following the election.²² In addition to using cyber means to manipulate Montenegro’s political and social environment, Russia allegedly funneled money into opposition political groups and sought to coordinate with politicians, clergy, NGOs, and media outlets.²³

Irregular and privatized warfare: Montenegrin law enforcement arrested GRU officers and agents who were allegedly planning to attack parliament, assassinate the prime minister, and provoke civil unrest with false-flag attacks on civilians.²³

SURVEILLANCE OF A NEW NATO MEMBER (JANUARY–JUNE 2017)

Following the October election, the Montenegrin legislature completed the final steps in its NATO membership process,

accepting NATO’s offer in April 2017 and joining on June 5, 2017, as the first new NATO member in eight years. Amid these developments, from January to June 2017, GRU operators persistently spearphished Montenegrin government members with military and NATO-themed lures.²⁴

Awareness of potential military risks and threats:

This targeting is consistent with a need to gain insight into the military inner workings of a new NATO member and, potentially, to seek controversial information about the concluding membership process that could be used to discredit or tarnish it.



GLOBAL OR REGIONAL DESTABILIZATION

Russia claims to have a historic role as “a guarantor of [international] stability and security.”²⁵ Per its foreign policy doctrine, Russia seeks stability in myriad forms, including military, economic, financial, political, strategic,^f social, global, and regional security.²⁶ The primary threats to global and regional stability, Russia argues, are the U.S. and its allies, whose actions “run counter to the growing need for cooperation and addressing transnational challenges and threats in today’s world.”²⁶ In short, Russia strongly objects to any attempts by other countries to alter the status quo without seeking Russia’s buy-in, authorizing the Armed Forces to maintain or restore the status quo through force.



Case Study: U.S. Begins Airstrikes Against ISIL (2014–2015)

INTIMIDATION OF U.S. MILITARY COMMUNITIES (2014–2015)

In September 2014, the U.S. began airstrikes against the Islamic State of Iraq and the Levant (ISIL or Islamic State) forces in Syria.²⁷ The operation outraged Russia, because it was allegedly fundamentally destabilizing to the world order. The Russian Foreign Minister told the United Nations (UN) General Assembly that the U.S. was using force unilaterally, acting without

^f **Strategic Stability** is an explicitly defined concept in Russian and U.S. policy (e.g., the START I agreement) wherein nuclear powers lack incentives to conduct a nuclear first strike. Russia therefore seeks to reduce these incentives. (Source: <https://carnegie.ru/2019/02/08/preserving-strategic-stability-amid-u.s.-russian-confrontation-pub-78319>).

regard for Syrian sovereignty, and attempting to impose U.S. values on the rest of the world.²⁸ From Russia's perspective, allowing the U.S. to override Syrian sovereignty to impose its values risked normalizing future U.S. actions to shape the political, economic, and cultural character of Russia and its neighbors. Furthermore, by freely acting without Russia's consent as a permanent member of the UN Security Council (UNSC), Russia's ability to prevent future U.S. operations via a UNSC veto might be diminished.

Russia argued that U.S. actions constituted a major threat to Russia's ability to maintain global stability, a key military risk per the Military Doctrine. The GRU likely responded to these circumstances by using an ISIL hacktivist identity to harass and intimidate U.S. military and law enforcement communities from December 2014 through February 2015.

⊕ **Manipulation of social or political environment:**

This fakelist campaign likely attempted to manipulate the American public's emotions about U.S. involvement in Syria, creating the appearance of ISIL retaliating against U.S. communities directly or tangentially associated with counterterrorism operations. On January 6, GRU operators leveraged access to New Mexico and Maryland media outlets' websites and social media accounts to deface them with pro-ISIL imagery. They also published locals' personally identifiable information (e.g., driver's licenses, jail records), photos of service members at a base in Texas,^{29,30} and federal, state, and local law enforcement records.³¹ On January 12, the operators compromised and used the U.S. Military Central Command's (CENTCOM) social media accounts to publish military PowerPoint decks and retired service members' personal data.³² Finally, on February 10, the operators used access to a Maryland television outlet's text message alert system to send threatening messages to subscribers.³³

⊕ **Indirect and asymmetric warfare:** A decrease in public support for the conflict would have likely amounted to partial neutralization of the threat posed by the unauthorized U.S. intervention without directly confronting the United States.



DEPLOYMENT OF MILITARY FORCES ADJACENT TO RUSSIA OR ITS ALLIES

Since Russia's annexation of Crimea in the spring of 2014, NATO has prioritized increasing its presence in Eastern Europe. The alliance's post-Cold War focus on improving cooperation with Russia shifted overnight toward containment, deterrence, and balancing of force.³⁴ In September 2014, for example, NATO announced that it would build five new bases, all in Eastern Europe, with the explicit goal of containing the Russian "threat" and protecting NATO's newest members in the former Eastern Bloc.³⁵

Moscow has reacted to this redoubling of forces in Eastern Europe with dismay and frustration. From Russia's perspective, NATO's presence in Eastern Europe constitutes an improper attempt to "contain alternative centres [sic] of power," restricting Russia's ability to influence global and regional affairs.²⁶ Speaking to Russian exasperation about Western attempts to counter Russia with force deployments, Russia's Defense Minister has quipped that he would like to show the U.S. a globe and "ask them to explain why [the] 'enemies of America,' are located in the Middle East and the Far East and all their military bases and forces are snuggled up to Russian borders."³⁶



Case Studies: Poland Seeks Local Construction of New Foreign-led Military Bases (2014–2018)

Poland is Russia's largest rival in Eastern Europe, with a sizable population, economy, and military shaped by a hawkish anti-Russia worldview.³⁷ Russia feels especially threatened by Poland's focus on strengthening NATO's eastern front in the wake of Crimea's annexation.³⁸ Deploying new missiles and attempting to base more U.S. troops in Poland would serve as counterweights to the Russian exclave Kaliningrad.

SURVEILLANCE OF NATO BASE EXPANSION PLANNING (2014)

Discussions about expanding NATO bases within Polish territory in the summer of 2014 may have motivated GRU monitoring of the Polish government and defense sectors. On July 25, NATO's Supreme Allied Commander in Europe proposed expanding the alliance's base in Szczecin, Poland, to counter Russian threats and planned to discuss his strategy at NATO's September 2014 summit in Wales.³⁹

Concurrently, GRU-linked operators likely conducted espionage operations against the Polish government and defense sectors.⁴⁰ Also that July, GRU-linked hackers compromised websites belonging to a Polish government public records website⁸ and a Polish defense firm⁴¹ to distribute a backdoor primarily associated with GRU informational-psychological effects operations.⁴²

⊕ **Awareness of potential military risks and threats:**

This targeting is consistent with a heightened need to surveil Poland's military security amid discussions of expanding

⁸ The **Bulletin of Public Information** (BIP) is a Polish government website that acts a centralized location for accessing public records.

NATO's permanent military presence in Eastern Europe. The use of a watering hole, as opposed to spearphishing, suggests a desire to infect many targets, potentially reflecting a need for maximum visibility around many Polish elements of this critical military threat (i.e., policymakers, suppliers).

SURVEILLANCE OF PROCESS TO INSTALL A U.S. BASE IN POLAND (2018)

In June 2018, Poland engaged in activities and policy changes intended to more tightly bind Poland to the U.S. and its other NATO allies. On June 1, the Polish Ministry of Defense unveiled its proposal that the U.S. build a permanent military base in Poland⁴² and, on June 4, the NATO exercise Saber Strike 18 kicked off in Poland, Latvia, and Lithuania. Moscow denounced the proposed base, saying, "When NATO infrastructure directly approaches our borders, this certainly does not contribute to security and stability on the continent in any way" and warned that NATO exercises encourage "mutual distrust."⁴³

These events closely aligned with Military Doctrine-defined threats and risks concerning deployment of forces adjacent to Russia and conducting military exercises near Russia. The sudden announcement of the base proposal—unlike the well-publicized NATO exercise—likely created an urgent need for the GRU to surveil the Polish government. On or around June 4, GRU-linked operators spearphished Polish government entities, including the Ministry of Foreign Affairs, distributing malware hosted on Poland's Ministry of Finance website.⁴⁴

⊕ Awareness of potential military risks and threats:

This targeting is consistent with a heightened need to surveil Poland's military security amid discussions of expanding NATO's permanent military presence in Eastern Europe. The operators' willingness to risk their access to a high-profile government ministry's website, whose traffic would likely be trusted by Polish government defenders, may have reflected a mission urgency to gain access to many potentially relevant government targets.

COUNTERBALANCING OF NATO IN POLAND WITH TROOP PLACEMENTS IN BELARUS (2018)

Russia identified Belarus as a possible location to deploy forces to counter the proposed U.S.-led NATO base in Poland. On October 21, 2018,⁴⁵ Russia issued a security guarantee, indicating that Russia would defend Belarus against any invasion, and insisted that additional troop placement was necessary to be able to uphold that commitment.⁴⁶ Belarus, however, was wary of the proposal. Since Russia annexed Crimea in 2014, Belarus had drifted from its historical ally by rejecting further stationing of Russian soldiers in Belarus⁴⁷ and making diplomatic overtures to the European Union (EU)⁴⁸ and the U.S.⁴⁹ Consequently, in October 2018, Belarus strongly resisted any surge in Russian troops, fearing occupation by Russian forces and exposure to eventual annexation.⁵⁰

Belarus's resistance likely prompted Russia to launch surveillance operations against the Belarusian Ministry of Defense. On October 25, 2018, GRU-linked operators spearphished the Belarusian Ministry of Defense's Department of International Military Cooperation.⁵¹ The email claimed to be a

communication from a U.S. Department of Homeland Security multinational counter-narcotics program, suggesting that the intended Belarusian target was expected to be involved in U.S. government security relations.⁵²

⊕ Awareness of potential military risks and threats:

The GRU plausibly sought to increase its awareness of Belarus's internal debates about allowing Russian force deployments and to understand any U.S. overtures or pressure to reject Russia's proposal.



Case Studies: Romanian Military Expansion and Strengthening (2018)

MONITORING OF ROMANIA'S GROWING MILITARY PARTNERSHIP WITH MOLDOVA (FEBRUARY 2018)

Since the end of the Cold War, strongly pro-Western⁵³ Romania's core geopolitical conflict with Russia has been over the trajectory of neighboring neutral Moldova's development as a pro-West or pro-Russian state.⁵⁴ In early February 2018, Romania and Moldova's Defense Ministers prepared to hold a February 4 meeting to discuss new military partnerships, including a joint military battalion.⁵⁵

The possibility that Moldova could establish strong military ties with Romania, reorienting its foreign policy more toward the West, may have prompted GRU activity. In possible response, on February 1, 2018, GRU operators attempted to spearphish Romania's embassy in Russia⁵⁶ by imitating a defense and security consultancy.⁵⁷ Based on these factors, the operators likely sought to surveil Romanian diplomats working on Russian military issues.

⊕ Awareness of potential military risks and threats:

The GRU likely sought to closely monitor the tenor of the firmly anti-Russia Romania's growing military partnership with Moldova.

MONITORING OF ROMANIA'S NAVAL MODERNIZATION (MARCH 2018)

In response to Russia's annexation of Crimea, Romania has prioritized military modernization in recent years.⁵⁸ In 2018, Romania's military procurements primarily focused on naval modernization and expansion.⁵⁹ In February that year, Romania announced that it would purchase three submarines and four surface vessels to expand its deterrence capabilities in the Black Sea.⁶⁰

These proposed improvements conflicted with Russia's stated military objective of expanding its control of the contested Black Sea and likely prompted a responding cyber operation.⁶⁰ In mid-March,⁶¹ GRU-linked operators repeatedly spear-phished an undisclosed European government agency with lures that contained information about a then-upcoming naval-focused defense conference in the UK.⁶¹ Based on the expected naval audience for this lure and the fact that the lures' initial submissions on VirusTotal consistently came from Romania,⁶² the target was plausibly a Romanian navy entity.

⚠️ Awareness of potential military risks and threats:

The GRU likely sought to closely monitor Romanian naval efforts that might eventually contest Russian control of the Black Sea.



Case Study: Denmark Prepares to Join NATO's Missile Defense System (2015–2016)

SURVEILLANCE OF DANISH MINISTRIES OF DEFENSE AND FOREIGN AFFAIRS (2015–16)

In March 2015, Russia was increasingly concerned about Denmark's solidifying plans to participate in NATO's missile defense system.⁶⁴ On March 15, Russia's ambassador to Denmark candidly warned in a newspaper interview that Denmark joining the "American-controlled missile defense [makes] Danish warships...targets for Russian nuclear missiles."⁶⁵ Denmark's Foreign Minister called these threatening remarks "unacceptable."⁶⁵

The GRU likely sought to monitor key Danish parties involved in missile shield expansion planning because its rollout threatened to degrade Russia's deterrence capability against NATO. The GRU likely used cyber operations to closely monitor Denmark's integration into NATO's missile defense system.

⚠️ Awareness of potential military risks and threats:

According to the Danish government, likely starting around March 25, 2015, GRU operators⁶⁶ launched a nearly two-year effort to compromise the email accounts of Danish Foreign and Defense Ministry employees and their secure remote access to unspecified military information technology systems.⁶⁶ The timing of the operation's initiation, immediately following the observable increase in Russian animosity related to the missile system, suggests that the operation may have been in response to the missile system plan.



UNDERMINING OF RUSSIAN STRATEGIC DETERRENCE CAPABILITIES

Since the 1970s, the Union of Soviet Socialist Republics (USSR) and its successor state, the Russian Federation, have supported the concept of strategic stability—the agreed-upon balancing of strategic offensive and defensive arms to remove incentives for a nuclear first strike—to manage its relationship with its primary geopolitical opponent, the U.S.⁶³ The concept of strategic stability has been conceptualized in several nuclear arms control agreements, including the 1972 Anti-Ballistic Missile (ABM) Treaty and several iterations of agreements on strategic offensive arms reductions (Strategic Arms Reduction Treaty [START] agreements).

Since the early 2000s, Russia has increasingly accused the U.S. of destabilizing their relationship by developing new weapons systems and abandoning strategic agreements like the Intermediate-Range Nuclear Forces (INF) Treaty.⁶³ Russia's Military Doctrine specifically notes several technologies it believes increase incentives for the U.S. to launch a strategic first strike by diminishing Russia's own ability to defend itself or retaliate. These technologies include strategic non-nuclear high-precision weapons, space-based weapons, and missile defense systems. Russia considers several actions of other members of the NATO alliance to be threats to strategic stability. Examples include hosting U.S. or NATO troops and military exercises or deploying NATO missile defense or strategic weapons within allied countries proximate to Russia.



VIOLATION OF RUSSIA'S OR ALLIES' TERRITORIAL INTEGRITY OR SOVEREIGNTY

The preservation and strengthening of territorial integrity and sovereignty have been key pillars of Russian foreign policy since the start of Putin's first administration in 2000.⁶⁷ By "territorial integrity," Russia refers to the idea that countries' borders extend to wherever the local people recognize a government as "legitimate," meaning representative of their will and interests, and territorial change should not occur because of invasion. By "sovereignty," Russia refers to the

international relations concept that a legitimate state has an absolute right to manage its internal affairs without outside influence. By compelling other states to respect territorial integrity and sovereignty, Russia seeks to better manage the stability of its own vast territory, multiethnic population, and political environment.

In the past decade, Russia has drawn substantial Western ire for its annexation of Crimea, which, from the Western perspective, disregarded Ukraine's sovereignty. In response to these objections, Putin has responded, "Respecting the sovereignty [of a state] means preventing coups, unconstitutional actions and illegitimate overthrowing of the legitimate government [of a state]. All these things should be totally prevented."⁶⁸ Russia argues that the post-revolution Ukrainian state was illegitimate, because a small group of Ukrainian nationalists had allegedly overthrown an elected government and installed a new government that allegedly did not protect the interests of ethnic Russians in Crimea and eastern Ukraine.

Demanding international respect for the sovereignty of Russia, its allies, and ethnic Russians is therefore a critical component of Russia's foreign policy. In Russia's view, its sovereignty extends over ethnic Russians living in former Soviet states. It sees these groups as a large cultural Russian civilization that was torn apart by the collapse of the USSR. Therefore, Russia views foreign attempts to shape the politics of post-Soviet successor states like Ukraine, (e.g., support for regime change or dissident groups with pro-Western or anti-Russian views) as a threat to Russian sovereignty. Russia's belief in the inviolability of territory or matters of internal affairs from foreign interference is applied broadly and serves as the root of Russian criticism of foreign states for military activities undertaken without UNSC authorization.



Case Study: Ukraine Excludes Russia-aligned Separatist Territories from Elections (2015)

DISRUPTION OF BROADCASTERS DURING UKRAINIAN LOCAL ELECTIONS (2015)

In 2015, Russia and the West wrangled over the legal status of the pro-Russian separatist territories in eastern Ukraine. That spring, as part of a new, tenuous de-escalation protocol ("Minsk II"), Ukraine conceded to decentralization measures to give greater authority to local governments, including those of the breakaway separatists. As a result, the separatists would have been able to conduct internationally recognized elections

and establish a degree of local sovereignty⁶⁹ and, in Russia's eyes, legitimacy.⁷⁰ Mounting violence later in the summer and fall prompted Ukraine's president to block the separatists from participating in nationwide local elections scheduled for October 25, which Minsk II stipulated must be free, safe, and open to be internationally recognized.⁷¹

From Russia's perspective, the Ukrainian government's delegitimization of separatists' elections may have amounted to a violation of Russian allies' sovereignty, prompting a military response. Starting on the evening before election day, GRU operators conducted numerous destructive and disruptive attacks against several Ukrainian broadcasters.⁷²

➤ Reduced time to launch military operations with preemptive activities: The GRU prepared beachheads at media companies likely for the possibility that the tenuous Minsk II protocol might collapse without achieving key Russian policy objectives, such as holding internationally recognized elections in separatist territories. Initial intrusions began around March 6, shortly after the finalization of Minsk II.^{73, 74} Intrusion attempts continued through the summer, perhaps in an attempt to increase the number of breached broadcasters or establish additional access to new resources at the same broadcasters.⁷⁵

➤ Precise destructive attacks: The operators used their multimonth dwell time to establish access to diverse resources and nearly total control over victim networks, allowing for numerous destructive elements in the operation's actions phase. The attackers used domain controller access to distribute KillDisk data-wiping malware through the networks,⁷² corrupting servers and workstations.⁷⁵ They overwrote video files with another video supporting an undisclosed political party, likely a far-right nationalist group.⁷⁶ The operators redirected one broadcaster's website to an extreme-nationalist political party's website and claimed elsewhere to be associated with another nationalist political party's paramilitary wing.⁷⁷

➤ Manipulation of social or political environment: The operation disrupted Ukrainian media, which plays a key role in the democratic process. By repeatedly referencing hardcore nationalist political groups, the operation created the appearance of extremist Ukrainian nationalists running rampant in Ukraine, likely serving to increase Ukrainian domestic strife.



PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AND MISSILE TECHNOLOGY

Russian military doctrine for the past two decades has consistently opposed the proliferation of WMDs (especially nuclear weapons) and associated long-range delivery vehicles (i.e., missiles).⁷⁸ In a 2006 strategic document on antiproliferation policy, Russia argued that political will, rather than

scientific and engineering hurdles, will be the most important barrier to limiting WMD and missile proliferation;⁷⁹ states must comply with export control regimes and protect weapons' designs and stockpiles from leaks to other states or substate actors (e.g., terrorists).

A failure to limit WMD and missile technology proliferation would create several military security challenges for Russia, as noted in the 2006 document. It might lead to geopolitical destabilization as nuclear breakout by one regional power might prompt its rivals to seek similar capabilities. Proliferation might facilitate mass-causality terrorist attacks because more and diffuse WMDs would be harder to secure. Finally, a disparity in nuclear forces (either in terms of size or delivery method) between Russia and its NATO geopolitical challengers might fundamentally undermine Russia's strategic deterrence capability⁸⁰ necessary for continued geopolitical stability.⁸¹ Furthermore, to fill this capability gap, Russia might feel compelled to participate in an expensive arms race that it may be unable to afford.^{82, 83}

In our review of publicly attributed GRU-linked operations, we could not confidently link any examples to this key military threat specifically. That said, in the past decade, several circumstances or events likely triggered a necessary Russian military response to monitor, neutralize, or counter this threat. For example, in February 2019, the United States announced its intent to withdraw from the Intermediate-Range Nuclear Forces (INF) Treaty on the grounds that it found Russia to be noncompliant.⁸⁴ In theory, withdrawing would allow the U.S. to deploy intermediate-range missiles throughout Asia and Europe. The U.S. ultimately withdrew in August, prompting Russia to warn that the deal's collapse would spark a new arms race.⁸⁵ This series of events likely demanded close surveillance of parties involved in the policy's creation and implementation process, both inside the U.S. and among its NATO and East Asian partners.



FAILURE TO COMPLY WITH INTERNATIONAL AGREEMENTS AND TREATIES

Russia argues that multilateral laws, treaties, and agreements play a critical role in global security. Russia's constitution notes that international laws, treaties, and agreements to which Russia is a signatory shall supersede existing Russian law.⁸⁶ Its foreign policy doctrine further notes that Russia seeks the "uniform interpretation and application" of international agreements.⁸⁷ By supporting the inviolability of international organizations like the UN and International Monetary Fund (IMF), Russia "bolsters its position as a great power," pushing back on what it perceives as the U.S.' illegitimate and unsustainable unilateral claims to hegemony.⁸⁸ Furthermore, following these agreements arguably increases predictability and thus stability and security in international relations, which

is a key Russian foreign policy aim (as noted on page 12). When others accuse Russia of breaking laws and agreements, it tends to dismiss such criticism as Western hypocrisy and asks that Russia be treated equally by the West's standards. For example, when the West condemned Russia's 2014 annexation of Crimea, Putin asked why Russia "defending" Crimea's ethnic Russians' self-determination should be considered legally different from NATO backing Kosovo's secession from Yugoslavia in 1999.⁸⁹



Case Studies: Ukraine Intentionally Defaults on a Russian Energy Loan (2015–2017)

SIGNALING OF RUSSIAN DISPLEASURE WITH CONTINUED FOREIGN LOANS TO UKRAINE (2015)

On December 17, 2013, Ukraine's soon-to-be-oust pro-Russia president secured a loan from Russia worth \$3 billion in a deal that also included Russia cutting the price of natural gas it supplied to Ukraine.⁹⁰ If Ukraine had been forced to fulfill its end of the bargain, this deal would have strengthened Russia's already substantial economic and energy leverage over Ukraine. Even after Ukraine's revolution, Russia likely expected that Kyiv would eventually be forced to pay down the loan to maintain eligibility for loans from the IMF, which Ukraine was also seeking. The new Ukrainian government, however, indicated that it did not intend to repay the loan under existing terms,⁹¹ despite the traditional IMF policy that a member should not receive IMF loans while deliberately defaulting on loans to other countries.^{92, 93, 94}

The possibility that Ukraine might intentionally default on the energy loan constituted a military risk for Russia. It risked reducing the ability of Russia to apply economic pressure on Ukraine, giving Ukraine access to funds that might prolong the conflict, and decreasing Russia's ability to use international legal mechanisms to constrain its geopolitical opponents. The GRU likely used cyber operations to apply pressure to key foreign and domestic parties in the IMF loan process to reinforce the narrative that new loans would be improper.

7.01.2015 CyberBerkut has blocked German Chancellor and the Bundestag's websites.

www.bundestag.de
www.bundestag.de

The Ukrainian government wants to review national budget by the 15 of February, 2015. The Prime Minister Arseniy Yatsenyuk hopes to obtain multi-billion credits from the EU and the IMF. It is obvious how this money will be wasted. Yatsenyuk needs money to extend the war and not to restore collapsed infrastructure of our country. This war has already taken thousands of lives, and Yatsenyuk will kill more for your money!

That's why we appeal all people and government of Germany to stop financial and political support of criminal regime in Kiev, which unleashed a bloody civil war.

We are CyberBerkut! We will not forget! We will not forgive!

Figure 1. CyberBerkut's statement of grievances regarding the DDoS of German government websites (Source: <https://cyber-berkut.org/en/olden/index1.php>)

Irregular and privatized warfare: The GRU used a fake hacktivist group to signal Russia's concerns about loans to Ukraine. On January 7, 2015, the GRU, in the guise of CyberBerkut, launched DDoS attacks on the German Chancellery,^h the Bundestag,ⁱ and the Foreign Office.⁹⁵ CyberBerkut stated that its attack was in opposition to Germany's financial and political support of the Ukrainian government and Ukraine's alleged plans to request German support for future EU and IMF loans. CyberBerkut claimed that these funds were being redirected from infrastructure spending to pay for the war in Eastern Ukraine.⁹⁶

SABOTAGE OF POWER DISTRIBUTORS IN RESPONSE TO UKRAINE'S FAILURE TO REPAY THE ENERGY LOAN (2015)

Despite Russian objections, the IMF changed its policy to accommodate Ukraine on December 8, 2015, allowing it to receive new IMF loans without first repaying Russia.⁹⁷ On December 20, Ukraine intentionally defaulted on its gas-related loans, undermining a key Russian tool for building economic influence and energy dependence on Russia. Perhaps even more important than the money itself, the default and the IMF waiver represented to the Russian government the unfairness of international dealings with Russia, which referred to the rule change as "hasty and biased" and made "exclusively to the detriment of Russia."⁹⁸

We assess that Ukraine's intentional default on this symbolically and strategically important energy loan was likely the primary precipitating factor that led to the GRU conducting the first publicly documented cyber-enabled power outage only three days later, on December 23, immediately following Ukraine's professional holiday for energy workers. GRU⁹⁹ operators caused power outages in large portions of Ukraine for several hours by leveraging their multimonth access to three power distribution companies.

Reduced time to launch military operations with preemptive activities: Intrusion activity began no later than March 2015, giving operators enough time to prepare for a multifaceted, precise attack against three power distribution companies simultaneously. GRU operators attempted to breach power companies via varied means, including spear-phishing to deliver remote access tools and breaching insecure web servers to pivot onto corporate IT networks.¹⁰⁰

Precise destructive attacks: The operators took multiple carefully orchestrated actions to disrupt power distribution and hamper recovery efforts. They remotely opened breakers to stop the power flow, as well as conducted telephonic denial of service attacks to hamper the companies' communications, disrupted workstations, and corrupted field devices.¹⁰¹

SABOTAGE OF MULTIPLE SECTORS ON SYMBOLIC DATES (2016–2017)

In 2016, the IMF expressed concerns about corruption in Ukraine,¹⁰² and Russia issued protests and threats of legal retaliation¹⁰³ if the IMF followed through with issuing new funds to Ukraine. Despite these issues, the IMF ultimately dispersed another \$1 billion loan to Ukraine in September 2016.¹⁰⁴

The IMF's decision to release new funds to Ukraine, over Russia's insistence that Ukraine needed to pay down the energy loan, constituted a growing military risk. Starting in December 2016, the GRU initiated a 10-month campaign of sabotage operations against Ukraine, likely in continued retaliation for the failure to repay the energy loan.

Consistent with these strategic concerns, the GRU selected dates for these operations on or around days related to Ukrainian identity and independence generally and, occasionally, the loan specifically. On certain occasions, the target choice also strongly aligned with the operation's symbolic significance. A full list of identified operations and the assessed significance of their timing appears on page 19.

The most prominent examples include the following:

Sabotage of Ukraine's Financial Sector (December 8, 2016):

The campaign began with GRU operators—in the guise of F Society, the fictional debt-wiping hackers from the HBO TV drama *Mr. Robot*—sabotaging numerous financial-sector organizations in Ukraine on December 8, 2016.¹⁰⁵ The attack occurred almost exactly one year after the IMF changed its lending rules, enabling Ukraine to default on its debt to Russia.¹⁰³ From Russia's perspective the IMF, like F Society, had wiped away Ukraine's debt. This attack also occurred on Ukrainian Armed Forces Day, an annual celebration of the formation of Ukraine's armed forces in 1991, a major signifier of the new Ukrainian state's independent identity from the Soviet Union and Russia.



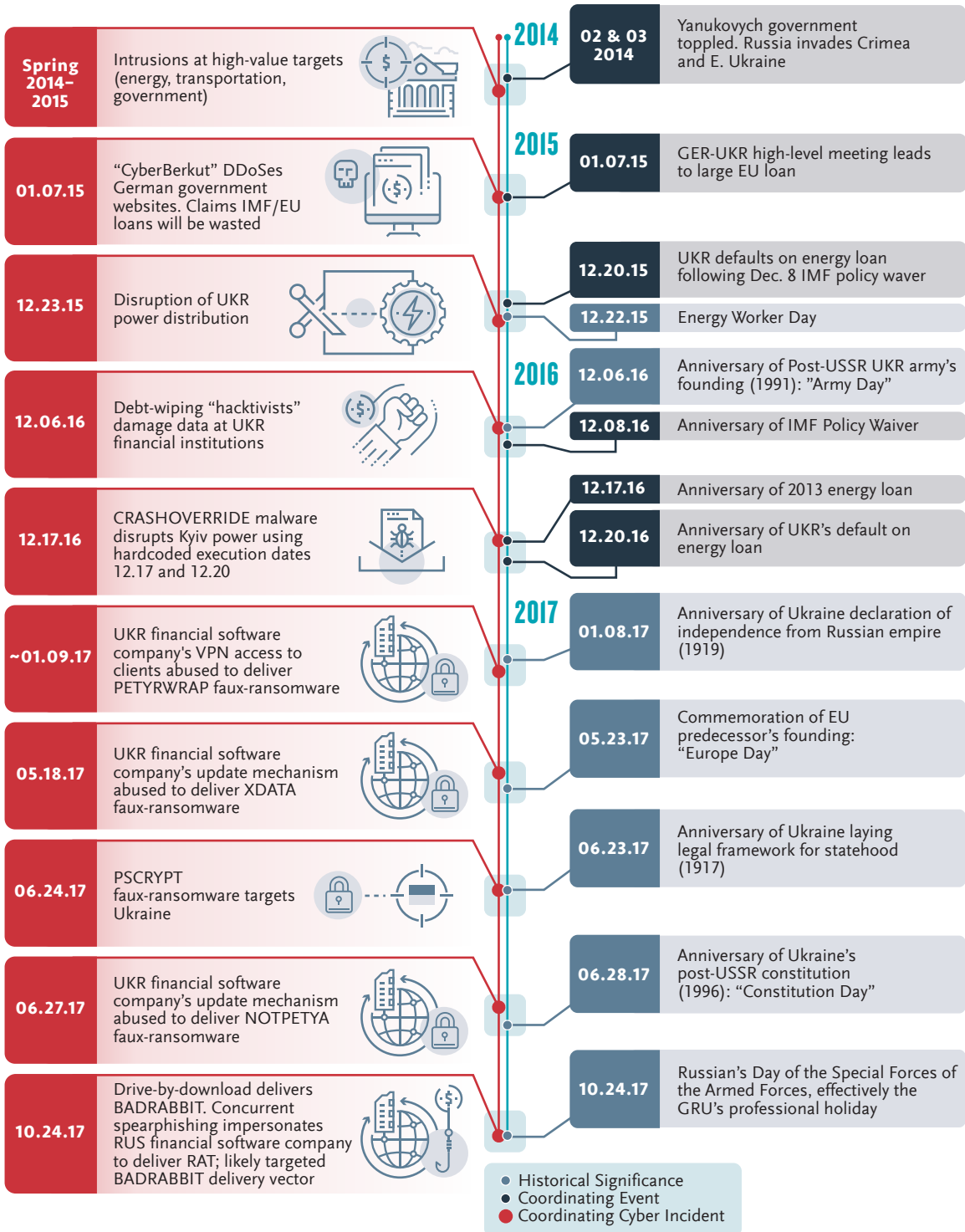
TO READ BOOZ ALLEN'S REPORT ON THIS INCIDENT, "WHEN THE LIGHTS WENT OUT," VISIT: BOOZALLEN.COM/UKRAINE

^h The German **Federal Chancellery** is the agency responsible for direct support of the German head of state, the Chancellor. Its functions include policy support and management of the intelligence community.

ⁱ The **Bundestag** is Germany's federal legislative assembly or parliament.

CONTEXTUALIZING OPERATIONS IN UKRAINE

PLACING OPERATIONS IN THEIR STRATEGIC CONTENT REVEALS LIKELY MOTIVATION AND INTENT



Sabotage of Kyiv's Power Distribution (December 17, 2016):

GRU operators used autonomous, self-destructing malware (CrashOverride) to disrupt power in Ukraine's capital. The malware contained two hardcoded activation dates^{106, 107} corresponding to the three-year anniversary of the loan's signing (December 17) and the one-year anniversary of Ukraine officially defaulting on its debt payment (December 20). Targeting Kyiv's power grid further stressed the attack's likely political significance.

Sabotage of Ukraine's Economy Broadly (June 27, 2017):

GRU operators¹⁰⁸ used worming wiper malware (NotPetya) to disable computers worldwide at organizations with Ukrainian tax liabilities.¹⁰⁹ The operation was executed on the eve of Constitution Day, which commemorates Ukraine's approval of its post-Soviet constitution in 1995 that formally established Ukraine's modern government, territory, and sovereignty.

This series of disruptive operations reflected many of the recurrent aspects of modern warfare identified in the Military Doctrine.

Warfare impacting the entire depth of an enemy's territory simultaneously: In several incidents, the GRU simultaneously conducted destructive attacks with a high degree of precision (i.e., highly targeted against Ukraine), impacting targets on a countrywide scale, harming huge portions of Ukraine's critical sectors. Repeatedly, GRU operators abused update processes for financial software used mainly in Ukraine or by entities touching Ukraine's economy, thereby enabling targeted sabotage at scale, causing billions of dollars of damages globally.¹¹¹ The NotPetya attack impacted Ukraine's government, banks, transportation (e.g., airports, subways), trading firms, telecommunications companies, and gas filling stations,¹¹² reportedly crippling 10 percent of all computers in Ukraine.¹¹³ It also disrupted foreign pharmaceutical, shipping, consumer goods, parcel delivery, and health-care companies with business ties to Ukraine.¹¹¹

Precise destructive attacks: Several operations targeting specific organizations involved multiple disruptive aspects with likely intent to demoralize, confuse, and, in at least one case, create hazardous recovery conditions. On December 17, 2016, GRU operators¹¹⁴ disrupted power distribution in parts of Kyiv; they opened breakers (cutting the power flow), wiped operators' monitoring systems (reducing insight into impacted systems), and unsuccessfully¹ attempted¹¹⁵ to disrupt safety devices that protect equipment from electrical abnormality (a dangerous environment for manually closing breakers during decreased visibility).¹¹⁶ Similarly, on December 15, GRU operators disrupted numerous systems at a railway company, wiping servers and systems used for empty freight car distribution, online ticketing, and traffic safety management.¹¹⁷ This last aspect of the attack appears to coincide with the Ukrainian railway company's plan to run its first tests of a new empty train dispatching system on December 28, 2016 as a railway modernization project.¹¹⁸

Creation of permanent war zones: The GRU's close timing of numerous sabotage operations established a state of constant, relentless, unstoppable conflict in Ukraine. For example, within one week in December 2016, the GRU disrupted Ukraine's railways (December 14–15), power distribution (December 17),¹¹⁹ and shipping (December 19).¹²⁰ The GRU's barrage of near monthly attacks on the Ukrainian financial sector and corporate finance departments in early- and mid-2017 continued this trend.

Manipulation of the social or political environment:

The operators may have had several secondary strategic objectives consistent with the GRU's mission, in addition to retaliation against a perceived unfair application of international rules by the IMF. By repeatedly disrupting Ukrainian critical sectors, especially Ukraine's financial sector, the GRU may have sought to dissuade foreign companies from doing business in Ukraine (disrupting the Ukrainian economy), demoralize Ukrainians, and reduce their confidence in the anti-Russia Ukrainian government's competence. Furthermore, as a show of force, the attacks may have further served to deter other post-Soviet countries from turning Westward and signal to NATO Russia's cyber capabilities, establishing a new form of strategic deterrence.

MITIGATION OF RETALIATION AND REPROBATION FOR THE NOTPETYA INCIDENT (2017)

Despite the GRU's attempts to make the NotPetya incident look like a cybercriminal ransomware operation, public assessments quickly shifted to blame to the GRU. Within a week, Ukrainian security services and several foreign cybersecurity firms concluded that GRU-linked operators were responsible for NotPetya—likely the costliest cyber attack in history—as well as the two previous power disruption attacks.¹²¹ The next year, first in February 2017,¹²² the U.S. publicly endorsed this attribution and, then in April, several other countries also reaffirmed it.¹²³

The growing likelihood of a global backlash against Russia in the months after NotPetya might have constituted a sharp deterioration in Russia's interstate relations, a military threat listed in the Military Doctrine. Unlike the GRU's other sabotage operations whose damage was contained within Ukraine's borders, NotPetya had caused billions of dollars of damage to civilian companies in many NATO countries including the U.S. Against this backdrop, the GRU conducted a final major disruptive operation, again deploying wiper malware (BadRabbit) on October 24, 2017.¹²⁴

We assess that the BadRabbit operation was likely designed to appear like a Ukrainian government or aligned group retaliating against Russia and the GRU. Such an operation might serve to create seeming moral equivalence between Russian and Ukrainian government hackers, this time painting Russia as the victim of a similar large-scale wiper attack by a Western-aligned state. The operation borrowed elements of the NotPetya attack, such as deploying wiper malware disguised

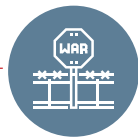
¹ It is unclear whether the coding error that prevented the safety device disruption from occurring was intentional or unintended. If it was intentional, the attack may have served in part to have a deterrent effect by revealing a new destructive GRU capability to Russia's adversaries.

as ransomware, and attacking on a symbolic date; October 24 is a Russian professional holiday that commemorates the creation of Russian military's special forces (Day of Special Forces of the Armed Forces), essentially the GRU's professional holiday. Most victims were in Russia,¹²⁵ infected via fake Flash update alerts on mostly low-traffic Russian websites,¹²⁶ but incongruously most high-profile victims were in Ukraine.^{127, 128}

◆ **Warfare impacting the entire depth of an enemy's territory simultaneously:** The operation struck many high-profile victims in Ukraine across varied sectors.¹²⁶ These victims paralleled victims of other GRU sabotage attacks in Ukraine over the previous few years, including the Ministries of Finance and Infrastructure, the Odesa airport, and companies in rail transport and media.^{128, 129}

◆ **Precise destructive attacks:** The concurrent, disproportionate disruption of numerous high-profile targets in Ukraine suggests that the GRU likely used a second, more-targeted malware distribution method than just social engineering via exploit-less fake Flash update alerts.¹³⁰ Ukrainian security services note that an associated spearphishing campaign occurred concurrently, which we assess may have been used to deploy BadRabbit to targeted Ukrainian victim networks.¹³¹

- We have discovered that these messages,¹³² purporting to be from Russian financial software developer 1C, encouraged targets to install a free security update from GitHub for their flagship 1C Enterprise^k accounting software.¹³² The update, which we recovered, was an obfuscated copy of remote administration tool (RAT) Ammy Admin disguised as various component update files (e.g., PDFs, images).¹³³ This tactic matches a June 2018 Ukrainian government claim that Russian government operators had been spearphishing Ukrainian "companies, including banks and energy firms" with malware "[broken] into separate files, which are put onto targeted networks before activating them."¹³⁴ The operators could have used the RAT to direct computers to the websites delivering fake Flash updates to download and install the BadRabbit malware.



ARMED CONFLICT ADJACENT TO RUSSIA OR ITS ALLIES

Armed conflict along Russia's borders or those of its allies presents numerous threats for Russian military security. In the context of Europe's challenges with Syrian refugees, Russia has warned that a failure to offer refugees jobs or integrate them into local society risks heightened social tensions (a key

internal military threat).¹³⁵ Violence in these areas may spill over into Russia or its allies' territories (a key military risk), leading to armed conflict involving the Russian military. Finally, armed conflict may lead to failed states, leading to safe havens for terrorists that could strike at Russian civilians.

This military threat of terrorism stemming from nearby failed states has been a contributing factor to Russia's involvement in the Syrian Civil War. Among other objectives, Russia explicitly sought to defeat ISIL and prevent terrorism's proliferation elsewhere, including in Europe.¹³⁶ As Russian state-owned broadcaster Channel One noted, "Let's not wait until the fire comes home to us."¹³⁷



Case Study: Middle East Opposition to Russia's Involvement in the Syrian Civil War (2015)

MONITORING OF MIDDLE EAST FOREIGN POLICY PLAYERS (2015)

On September 22, 2015, the Gulf Cooperation Council (GCC)^l issued a statement that its members had condemned Russia's just-announced plan to become directly involved in the Syrian Civil War.¹³⁸ The statement argued that Russia's involvement would prolong the bloody conflict and strengthen Syrian ties with the GCC's primary regional rival, Iran.

Likely in response to this diplomatic pushback, the GRU plausibly sought to gain insight into GCC foreign policy players' internal discussions pertaining to Russia's involvement in Syria. Such information could have informed Russian strategies to manage its increasingly important relationship with the GCC while balancing its desire to intervene in Syria.

◆ Awareness of potential military risks and threats:

Concurrent with the announcement of Russia's involvement in the Syrian Civil War, the GRU attempted to surveil GCC members' diplomatic and military apparatuses. Principally in September and October 2015, GRU-linked operators spearphished¹³⁹ militaries and the ministries of defense and foreign affairs in Saudi Arabia, Kuwait, United Arab Emirates, and Qatar¹⁴⁰ with messages directing them to fake webmail portals.

^k In May 2017, Ukraine declared that 1C was effectively spy software and placed sanctions on its developer. Regardless, Ukrainian companies were reportedly slow to transition from this software. (Sources: <https://www.kyivpost.com/business/sbu-says-dealers-1c-software-ukraine-placed-sanction-list.html>; <https://informnapalm.org/en/one-year-of-ukrainian-sanctions-against-russian-social-networks-and-yandex-interim-results/>).

^l The **Gulf Cooperation Council** is a multistate trading bloc consisting of the six Persian Gulf countries, other than Iraq. The countries share common political systems (monarchies), religion (Sunni Islam), and economies reliant on natural resources, especially oil and natural gas. The GCC organization serves to promote common economic, security, and cultural goals. Russia shares many pragmatic interests with the GCC, such as countering Islamic terrorism, sustaining oil prices, and developing mutually beneficial economic and military relations. (Source: <https://trendsinstitution.org/wp-content/uploads/2016/05/Russian-Foreign-Policy-and-the-GCC-Final.pdf>).



UNAUTHORIZED USE OF FOREIGN MILITARY FORCE ADJACENT TO RUSSIA OR ITS ALLIES

Consistent with Russia's concerns about the failure to abide by international agreements, Russia strongly objects to the use of force without the UN's approval. Such action creates two key strategic problems for Russia. First, it undermines the supremacy of the UNSC and Russia's veto as a permanent member, thereby diminishing Russia's ability to counter the U.S. in international affairs. Second, it degrades the importance of sovereignty in international relations, a key military threat as noted on pages 15–16.

In the post-Cold War era, Russia has grown increasingly frustrated by Western states repeatedly acting, in its mind, extralegally of the UN. Although Russia strongly supported the U.S.' and NATO's efforts at the start of the War on Terror, it denounced the U.S.-led 2003 invasion of Iraq as acting outside the bounds of agreed-upon UN resolutions, stating, "Not one of [which] authorize[d] the violent overthrow of the leadership of a sovereign state."¹⁴¹ Other notable instances where Russia has objected to the use of force without UN approval include the U.S.-led toppling of the Qaddafi regime in Libya (under the auspices of humanitarian intervention),¹⁴² the NATO-led interventions in the Balkans in the 1990s, and numerous states' involvement in the ongoing Syrian conflict.^{143, 144}



Case Study: UK Considers Military Operations in Syria (2014–2015)

BREACH OF A BRITISH BROADCASTER (2014–2015)

Following a June 2015 ISIL-aligned terrorist attack on British tourists in Tunisia, the UK began to mull over launching air strikes in Syria.¹⁴⁵ Formal Parliamentary debate on the strikes began in November in response to a major terrorist attack in Paris,¹⁴⁶ prompting Russia's ambassador to the UK to ask that the two countries "beat ISIL as we did the Nazis: together."¹⁴⁷ Parliament authorized air strikes on December 2¹⁴⁸ and, two weeks later, the UNSC unanimously approved a resolution calling for a ceasefire against all civilian targets in the conflict while authorizing the continued targeting of UN-recognized terrorist organizations like ISIL.¹⁴⁹

The emerging possibility of the UK unilaterally launching airstrikes within the territory of Syria, a Russian partner, plausibly prompted the GRU to establish preemptive beachheads at a UK television station, in order to launch a destructive attack. According to the UK and Australia, in July 2015, the GRU breached Islam Channel, a small British television outlet.^{150, 151} The operators achieved a stealthy persistence on the Islam Chanel's networks by December 2015, around the time of the UNSC Syria resolution. The operators largely ceased further lateral movement, did not conduct operations to disrupt or otherwise publicly abuse the networks, and retained access until the breach was discovered in late 2016.¹⁵²

➤ **Reduced time to launch military operations with preemptive activities:** The initial intrusion began immediately after the terrorist attack in Tunisia, allowing the operators to establish extensive persistent access to the broadcaster that could be selectively abused on a short timeline as needed.

➤ **Precise destructive attacks:** The operators conducted extensive lateral movement and reconnaissance across the station's corporate and broadcast networks. Their reported areas of focus were the corporate-broadcast network bridge, the station director's workstation, and a production control room.¹⁵²

➤ **Manipulation of social or political environment:** The target's identity as a broadcaster tailored to the Islamic community likely would have shaped any eventual disruptive or destructive attack's character. The GRU conducted several other attacks against broadcasters around this time in the guise of an ISIL-aligned hacktivist group called CyberCaliphate.¹⁵³ These operations may have sought, in part, to foment socially divisive anti-Muslim sentiment in affected countries like France¹⁵⁴ and the United States.¹⁵⁵



GROWTH OF TRANSNATIONAL NON-STATE THREATS SUCH AS TERRORISM OR ORGANIZED CRIME

Combatting transnational terrorism has been a major Russian priority in the post-Cold War era. Through the early 2010s, Russia's top terrorism concern was domestic Islamist terrorism originating in its North Caucasus region in Central Asia, but this focus shifted around 2014 to the Middle East with the rise of ISIL.¹⁵⁶

This shift abroad has likely increased the importance of the Russian military in Russian counterterrorism policy, as the military focuses specifically on foreign-originating military security threats. According to the Russian Armed Forces, its counterterrorism mission has several strategic functions. These functions are to generate intelligence on and policy suggestions for terrorist threats, coordinate with foreign and domestic partner agencies, conduct special operations against

terrorist groups and their supply chains, and prevent the development of domestic pro-terrorist views.¹⁵⁷

Our review of GRU-linked cyber operations from the past decade did not identify any examples that could be confidently assessed as likely counterterrorism or counter-organized-crime activities. The cybersecurity industry's tendency to decline to publicly report suspected counterterrorism activities is likely a major contributing factor for this trend.¹⁵⁸



GROWTH OF ETHNIC, RELIGIOUS, OR CULTURAL DISAGREEMENTS OVER TERRITORIAL BORDERS

Nationalist movements threaten Russia's borders. In nationalism, group identity markers such as ethnicity, religion, or culture define a country's territorial boundaries. Numerous groups of Russian citizens without major identity markers of Russian ethnicity—being Slavic, Eastern Orthodox Christian, and Russian speaking—live along the country's borders. Nationalism by such groups has at times led to secessionist movements and disputes over Russian territorial claims, especially in the post-Soviet Era.¹⁵⁹ Various groups that have fought or petitioned to secede from Russia in the 21st century include Sunni pan-Islamists,¹⁶⁰ Chechens,¹⁶¹ Tatars,¹⁶² the Kaliningrad exclave,¹⁶³ Circassians,¹⁶⁴ Idel-Ural nationalists,¹⁶⁵ and Siberians.¹⁶⁶

Despite its concerns about losing territory to nationalist movements, Russia has been a strong advocate of its nationalist ties to people with Russian identity markers outside Russia.^{167, 168} It routinely touts its linkages to countries like Ukraine that were historically part of Russia proper, as well as to ones like Estonia that were "Russified" during the Cold War.^{167, 168} In some cases, like in Eastern Ukraine and Georgia's South Ossetia region,^{169, 170} Russian military operations have directly supported ethnic Russian separatist movements. Russia therefore seeks to push back against attempts to dispute Russia's nationalistic ties to its neighbors and support people claiming nationalist ties with Russia.



Case Study: The Rise of Ukrainian Nationalism Threatens Russian Claims to Ukrainian Identity (2014–2015)

ESTABLISHMENT OF BEACHHEADS AT ENTITIES POSSESSING RUSSO-UKRAINIAN HISTORICAL RECORDS (2014–2015)

For decades, Russian leaders have rejected Ukraine's claims to independence based on any asserted unique national identity independent from Russia. In recent years, Russia's president, for example, has repeatedly rejected Ukrainian nationalism, saying, "Ukraine is not a country" (2008)¹⁷¹ and "Russians and Ukrainians are one people. We are essentially the same nation" (2019).¹⁷² In 2016, the Russian Foreign Policy Concept identified as a policy goal strengthening the shared cultural, religious, economic, and political ties of the two countries.¹⁰ Asserting a unique Ukrainian identity was a defining element of the 2013–2014 Ukrainian revolution. Ukrainian efforts to reorient the country with the West and break or downplay ties with Russia are therefore diametrically opposed to Russia's own views of Ukrainian identity.

Per the Military Doctrine, the Russian military must therefore neutralize or counter the threat of Ukrainian nationalism. We assess that the GRU may have sought to establish the opportunity to leak data or disrupt systems at Ukrainian heritage-and-identity targets under the guise of nationalist hackers to further the Russian government's narrative of pervasive, dangerous Ukrainian nationalism. In August 2014 and March 2015, GRU operators repeatedly attempted to breach entities in Europe, the U.S., and Russia possessing Russo-Ukrainian historical records, such as archives, heritage associations, regional records authorities, museums, and universities.^{173, 174}

✚ **Precise destructive attacks:** The specific tools used in the campaign are consistent with the GRU's informational-technical effects team, suggesting that achieving the ability to cause disruption or destruction was a likely objective.^{173, 174}

✚ **Reduced time to launch military operations with preemptive activities:** No disruptions were linked to these operations. We assess that the GRU may have attempted to gain beachhead access to a wide range of cultural targets that could be leveraged in response to a specific cultural conflict with Ukraine.

⊕ Manipulation of social or political environment:

The ultimate purpose of these beachheads may have been an operation that stoked ethnic tensions in Ukraine. In other instances, GRU operators conducted attacks in the guise of extremist Ukrainian nationalist hacktivist groups. Such attacks created the appearance of post-revolution Ukraine being overrun with violent Ukrainian nationalists, a threat to the many ethnic minorities in Ukraine. The cultural organization campaigns' spearphishing emails pretended to be from the leader of an extreme far-right¹⁷⁵ Ukrainian nationalist political party, possibly laying the narrative groundwork for a similar attack.^{173, 174}



ILLICIT USE OF CYBER OR INFORMATION OPERATIONS AGAINST RUSSIA OR ITS ALLIES

Russia seeks to limit global state-sponsored informational-conflict operations. Since 1998, Russia has repeatedly proposed at the UN laws, norms, and structures to guide the actions of states in cyberspace.¹⁷⁶ If ever accepted, these proposals would have the effect of limiting states' abilities to shape any other state's "sovereign" information space and establish mechanisms for Russia to legally dispute cyber activities that break those standards.¹⁷⁷

While Russia continues to press for legal restrictions on cyber operations through diplomatic channels, the GRU will likely attempt to deflect criticism about its own operations. The GRU's defense against such allegations might look like an incident in the summer of 2016. At the time, public awareness grew in the U.S. that Russia was likely attempting to covertly influence that year's U.S. presidential election. Concurrently, a still-unattributed threat actor using the identity "The Shadow Brokers" began leaking hacking tools¹⁷⁸ belonging to the U.S. Government, a fact that the White House has since publicly confirmed.^{177, 179} While it remains unclear whether The Shadow Brokers was a GRU-linked entity, the operation followed the tactics of other GRU operations. For example, if it were a GRU operation, it may have sought to neutralize Russia's critics by creating an appearance of moral equivalence (i.e., Russia's critics also conduct cyber operations).



ESTABLISHMENT OF HOSTILE STATES ADJACENT TO RUSSIA

Since the Cold War, Russia has sought to surround itself with states that are either friendly or neutral. Moscow employs a spectrum of soft and hard power means to maintain this state of affairs. It has joined several neighbors in a collective security alliance, bolstered trade and tourism, and promoted

shared cultural identity markers. Meanwhile, Russia has also invaded countries spinning out of its orbit, like Ukraine and Georgia; underwritten overt traditional media and covert social media efforts to destabilize its opponents and damage their publics' opinion of NATO and the EU; and used energy policy to integrate with or strong-arm potential opponents.



Case Study: Ukraine Holds Its First Post-Revolution Election (2014)

DISRUPTION OF UKRAINE'S NATIONAL ELECTION ORGANIZATION (MAY 2014)

In February 2014, a revolution overthrew Ukraine's Russia-friendly president with calls demanding closer ties with the West. This upheaval prompted the scheduling of a presidential election on May 25 to form a new legitimate government.

The pending establishment of a new Ukrainian government, overtly hostile to Russia, generated substantial risk for Russia, prompting a mixed kinetic and cyber military response. Within weeks of the revolution, Russian military special forces, including members of the GRU, rapidly annexed southern Ukraine's Crimean Peninsula and coordinated a separatist movement in eastern Ukraine's Donbass region.¹⁸⁰ Russia justified its actions by claiming that it was protecting the Donbass region's substantial ethnically Russian populations from "fascist" persecution by the new anti-Russia Ukrainian government.¹⁸⁰ On election night, GRU operators¹¹² disrupted key election resources with the likely objective of creating the appearance of a Ukrainian government conspiracy to install an extremist nationalist politician as the new president.

⊕ Manipulation of social or political environment:

The cyber operators took progressive steps on election day to further the Russian narrative that corrupt, dangerous anti-Russian politicians had illegitimately seized control of Ukraine. On election day, in the guise of antirevolutionary hacktivists named CyberBerkut, GRU operators leaked emails that purported to be a regional governor conspiring to bolster certain "correct" candidates for the Ukrainian presidency¹⁸¹ and blocked Central Election Commission (CEC) staffers' cellphones.¹⁹⁰ Then, on election night, GRU operators wiped¹¹² "network nodes and key components of the election system"^{112, 183} at the Ukrainian CEC, disabling software used to display real-time vote counts for 20 hours. Minutes before the polls closed, the operators defaced the CEC website claiming that a far-right nationalist politician had won the election¹⁸³—fictitious information that

Russian news stations immediately broadcast.¹⁸⁴ The operators then launched a DDoS attack on a CEC system that collected vote tallies from election districts, further delaying the publication of an official tally.¹⁸⁵ In addition, the attack propelled a key Russian narrative that Ukraine was overrun with violent and extremist nationalists, which partially served to harm ethnic Russians' perceptions of the new Ukrainian government.

✦ **Precise destructive attacks:** The operators' disruption, destruction, and manipulation of diverse election resources through varied means demonstrated a carefully planned strategy to progressively delay the publication of election results and degrade confidence in the validity of results.



STATE-SPONSORED SUBVERSIVE ACTIVITIES TARGETING RUSSIA

Foreign-backed democracy promotion groups are deeply concerning to the Russian government. From its perspective, sovereignty guarantees that a country's political system is off-limits to state-sponsored foreign influence.¹⁸⁶ Consequently, Russia classifies numerous foreign-funded democracy promotion groups as illegal "foreign agents," (i.e., subversive organizations acting at the behest of foreign states).¹⁸⁷ It also retains the ability to expel any "undesirable" international NGO if it is deemed to be a threat to Russia's national security.¹⁸⁸ Russia has even explicitly accused the U.S. of attempting to invalidate Putin's 2012 presidential election and return to power by stirring up the massive protests that occurred that year.¹⁸⁶



Case Study: Growing Awareness that Russia Attempted to Covertly Influence the 2016 U.S. Presidential Election (2016)

DISINFORMATION CAMPAIGN AGAINST U.S. DEMOCRACY PROMOTION GROUPS (2016)

In June 2016, news broke that an incident response effort at the Democratic National Committee had determined that two teams of "Russian government hackers" (now known to be linked to separate ununiformed security services and military operations¹⁸⁹) had stolen huge quantities of data from this political organization.¹⁹⁰ The news proved to be the

precipitating moment in the public's growing awareness of a covert Russian campaign to influence the 2016 U.S. presidential election.²⁰²

Among other ramifications, the GRU campaign's growing exposure threatened to undercut Russian denunciations of state-sponsored political influence activities (e.g., overt democracy promotion groups) as hypocritical, a risk to core security interests in the Military Doctrine. In possible response to this risk, GRU operators leaked emails and documents from U.S.-based democracy promotion organizations in August and October 2016, with the apparent objective of establishing a moral equivalency narrative. Russia's president has made this very argument: if Russia were conducting social media disinformation campaigns and leaks, it would be no different than the U.S.'s democracy promotion efforts, including those by one of the organizations that the GRU breached, the Open Societies Foundation (OSF).¹⁹¹

✦ **Manipulation of social or political environment:**

According to the GRU operators' proxy¹⁹² identities, like DCLeaks¹⁹³ and CyberBerkut,¹⁹⁴ their leaks allegedly revealed covert U.S. operations to stoke protest movements and influence elections worldwide, with an emphasis on upsetting the Russian political order. For example, they claimed that an email from the National Endowment for Democracy (NED) showed that the "U.S. [was] preparing a color revolution in Russia according to [the] Ukrainian model."¹⁹⁴ They also claimed to have uncovered proof of the OSF interfering in elections throughout Europe and South America.¹⁹³ Other leaks, amplified by Russian media, allegedly showed that the OSF's financial backer had also underwritten disruptive political movements in Ukraine, Bulgaria, and the United States.¹⁹⁵

INTERNAL MILITARY RISKS



PROVOCATION OF RUSSIAN POLITICAL STRIFE

Foreign civil society organizations, such as democracy promotion and anticorruption groups, are deeply concerning to the Russian government. Russia views these groups as hostile actors threatening to sow instability and foment extremism that may spill back into Russia in the form of terrorism or revolution (pointing to the Arab Spring and the 2013–2014 Ukrainian revolution as example scenarios).¹⁹⁶

Since protests riled Russia after Putin's disputed 2012 reelection,²¹¹ Russia has greatly curtailed the ability of foreign civil society organizations to operate. In the following years, it promptly expelled the United States Agency for International Development (USAID) and passed legislation authorizing the removal of any "undesirable" international NGO deemed to be a threat to national security.¹⁸⁸ Organizations targeted under these policies include Transparency International ([TI],

deemed a foreign agent in April 2015),¹⁹⁸ OSF (banned in November 2015),¹⁹⁹ the National Democratic Institute ([NDI], banned in March 2016),²⁰⁰ and the International Republican Institute ([IRI], banned in August 2016).²⁰¹



Case Study: Calls for Fair Elections and Combating Corruption Sweep Russia (2017–2019)

SURVEILLANCE OF DEMOCRACY PROMOTION AND ANTICORRUPTION GROUPS (2018–2019)

Between 2017 and 2019, a series of protests engulfed Russian domestic politics. Intermittent mass demonstrations in major cities called for major structural changes because of popular concerns about corruption and election fairness. Russia blamed foreign governments, traditional and social media outlets, and civil society organizations for inciting or supporting some of these demonstrations.²⁰²

The perceived elevated risk from foreign civil society foundations in 2017–2019 has likely prompted a Russian military response. The GRU has likely surveilled these groups to maintain awareness of their activities in Russia. Plausibly, GRU operations might have also sought to gather information that could be leaked to discredit these groups.

➤ **Awareness of potential military risks and threats:** In 2018 and 2019, GRU operators spearfished numerous foreign civil society organizations either banned from Russia or analyzing Russian civil society issues. Based on domain registration dates, the operators targeted the Hudson Institute²⁰³ (a U.S. think tank that runs an anticorruption initiative that often profiles Russia)²⁰⁴ and the IRI likely in early 2018. In early- and mid-2019, they also targeted the IRI, OSF, the European Endowment for Democracy, and TI.^{205, 206} The impact of these operations is not public; OSF disclosed in July 2019 that there had been an “attack,” but declined to elaborate.²⁰⁶

➤ **Reduced time to launch military operations with preemptive activities:** One objective of these operations may have been to gather information to enable the GRU to defame or discredit foreign civil society organizations. The GRU similarly attempted to stoke controversy about the OSF and NED in 2016 using leaked information, though as we previously assessed

(see page 25) that operation’s goal was likely to establish a moral equivalence narrative in response to public awareness of GRU interference in the 2016 U.S. presidential election.



SEPARATIST AND ETHNO-RELIGIOUS TERRORISM

Islamic terrorism is a persistent threat to Russian national security.²⁰⁷ Chechen separatists in the 1990s and 2000s and Islamic State-aligned terrorists in the 2010s conducted mass casualty attacks inside Russia. Russia has often argued that it should take an active military role in counterterrorism operations to deny terrorists safe havens and, ultimately, prevent terrorism from spilling back to Russia.²⁰⁸



Case Study: International Backlash Threatens Antiterrorism Operations in Chechnya (2013–2014)

SURVEILLANCE OF JOURNALISTS COVERING ANTITERRORISM ACTIONS IN CHECHNYA (LATE 2013)

In the fall of 2013, Russia faced a challenging narrative in international media that it was committing extensive human rights abuses²⁰⁹ in its tumultuous North Caucasus region, home to the Russian Federation republics of Dagestan and Chechnya.^m At the time, Russia was mounting a major counterterrorism effort in the region to manage security risks related to the upcoming 2014 Winter Olympics in nearby Sochi; the world’s spotlight would be on Russia and a terrorist attack would have been a devastating blow to Russia’s prestige.^{210, 211} Russian law enforcement threatened and imprisoned human rights groups, lawyers, and journalists attempting to draw attention to Russia’s actions.²⁰⁹

The possibility of international condemnation constraining Russia’s counterterrorism strategy may have prompted the GRU to conduct cyber operations to surveil foreign journalists covering Chechnya. In late 2013, GRU-linked operators attempted to phish an undisclosed journalist under the

^m Dagestan is a Russian republic (a constituent political entity akin to a province) in the North Caucas region. To its south and west, it borders Georgia, Azerbaijan, and the Russian republic of Chechnya. Since about 2009, there has been a low-intensity conflict throughout this North Caucasus region between the Russian state and Islamic militants, a follow-on conflict to the Second Chechen war of 1999–2000.

pretenses of soliciting an article submission for an American magazine.²¹² Clues in the document and contextual information suggested that the target may have been a Georgian journalist of Chechen descent specializing in Chechen and human rights issues.²¹²

⊕ Awareness of potential military risks and threats:

Russia's desire to reap international goodwill from hosting the Olympics²¹³ may have made the country more vulnerable to foreign pressure on its counterterrorism operations. Consequently, the GRU may have tracked journalists whose coverage might spark a foreign backlash against its urgent counterterror activities.



UNDERMINING OF RUSSIAN HISTORICAL, SPIRITUAL, AND PATRIOTIC TRADITIONS

Russia considers the preservation of its national identity to be a key national security interest. Internally, these elements of heritage and national narrative serve to unify a culturally and ethnically diverse population with common conceptions of national identity and undergird patriotic support for the state.²¹⁴ Abroad, pan-Russo nationalism bolsters Russia's relationships with many of the former Soviet republics through the concept of a common identity. Elements of that identity are varied, including historical, spiritual, and patriotic aspects. Per the Military Doctrine, foreign activities that threaten Russia's preeminence in this pan-nationalist narrative are therefore a threat to Russian national security.



Case Study: Independence Threatens the Preeminence of the Russian Orthodox Church in Ukraine (2012–2018)

SURVEILLANCE OF RELIGIOUS FIGURES RELATED TO UKRAINIAN ECCLESIASTIC INDEPENDENCE (2012–2018)

Eastern Orthodox Christianity is deeply intertwined with Russian identity. Nearly four out of five Russians profess to be Eastern Orthodox, and Eastern Orthodoxy is widely practiced in much of Russia's southern and western peripheries.²¹⁵ For these reasons, the Russian government was alarmed by plans in the 2010s for a schism between the Ukrainian and Russian Orthodox Churches, giving the Ukrainian Church autonomy and removing a third of all parishes from the Russian Orthodox Church's oversight.²¹⁶ Ultimately, in December 2018, Ukrainian religious leaders formally established the new autonomous Ukrainian Eastern Orthodox Church, a move Ukraine's president hailed as "another pillar of Ukrainian independence."²¹⁷

The growing support for Ukrainian ecclesiastic independence in the 2010s constituted a military risk per the Military Doctrine. It risked further diminishing Russian influence in Ukraine and undermining the legitimacy of Russian narratives about entrenched pan-national unity with Ukrainians that had partially justified the Russian annexation of Crimea. In response to these evolving circumstances, Russian security services,ⁿ including the GRU, likely surveilled and harassed individuals involved in the ecclesiastic independence movement.

⊕ Manipulation of social or political environment:

In 2012, an unknown adversary leaked emails belonging to an official Russian Orthodox Church theologian, revealing that he was secretly supportive of Ukrainian efforts to gain ecclesiastic independence. The controversy around this leak ultimately led to him stepping down from his position with the church. Though this operation has not been attributed, GRU operators have reportedly repeatedly targeted this theologian at unspecified times.²¹⁸

⊕ Awareness of potential military risks and threats:

GRU-linked operators have been implicated in multiple efforts since 2015 to surveil Eastern Orthodox Clergy involved in the schism process by targeting their email accounts with spear-phishing. Targets have included the Chancellor of the Orthodox Church in America^{218, 219} (2015) and aides to the Eastern Orthodox Church's spiritual leader, the Archbishop of Constantinople²¹⁸ (2018).

ⁿ The 2012 activity described in this section occurred prior to the Military Doctrine identifying Russian internal affairs as a military priority in 2014. Though that operation's target is a reported GRU target, the 2012 leak-and-defame operation has not been publicly attributed. (Source: <https://www.apnews.com/26815e0d06d348f4b85350e96b78f6a8>).



Case Study: International Sports Organizations Threaten Russian Athletic Achievements (2016–2018)

ATTEMPTS TO DISCREDIT SPORTS ORGANIZATIONS AND DISRUPT THE 2018 OLYMPICS OPENING CEREMONY (2016–2018)

Russian athletic prowess, especially in the Olympics, has for decades bolstered Russo-Soviet and Russian patriotism and shaped perceptions of Russian might, internally and abroad.²²⁰ Because of the perceived strategic importance of athletic success, the Soviet Union^{221, 222} and Russia²²³ have run extensive, secretive doping programs to boost their athletes' performance—especially during major international competitions like the Olympics. In June 2016, less than a month before the 2016 Summer Olympics, the World Anti-Doping Agency (WADA) released the first of a two-part report exposing Russia's modern doping program, which leveraged Russia's intelligence agencies to undermine independent antidoping testing processes.^{223, 224} Following a subsequent investigation, on December 5, 2017, the International Olympic Committee (IOC) banned Russia from competing in the February 2018 Pyeongchang Winter Olympics.²²⁵

These actions taken by WADA and the IOC threatened Russia's patriotic traditions (i.e., its reputation as an athletic powerhouse), a military risk as defined by the Military Doctrine. If the WADA report and subsequent investigations were broadly accepted as truthful and unbiased, Russia's reputation might significantly suffer among international and domestic communities. The IOC ultimate ban was, from Russia's perspective, a hostile act directed at a core strategic interest. In response to these circumstances, the GRU likely conducted a multiphase operation to first discredit WADA and other organizations accusing Russia of athletic perfidy, and second, to disrupt the Pyeongchang Olympics' opening ceremony in an act of retaliation for the ban.



Figure 2. Russian government outlets, like embassies and state-funded media, amplify GRU leaks to further mainstream associated narratives. This Russian Embassy in the UK tweet highlights the “hypocrisy” of UK and U.S. athletes receiving therapeutic use exemptions (Source: <https://twitter.com/RussianEmbassy/status/776343061504860161>)

Manipulation of social or political environment:

Between August 2016 and February 2017, GRU operators breached multiple national antidoping agencies, sports federations,²²⁶ and sports governing authorities.²²⁷ In many cases, the GRU leaked—via fake proxy hacktivist identities—foreign athletes' therapeutic use exemptions (TUE), which are waivers that allow athletes to compete while taking prohibited pharmaceuticals if they have a documented medical reason.²²⁸ The GRU operators likely sought to establish a false moral equivalency, arguing that Russia had received unfair treatment, because athletes in countries that called for Russia's Olympic expulsion like the U.S.^{229, 230} and Canada²²⁶ also used prohibited drugs (albeit drugs that were deemed medically necessary, formally disclosed, and authorized by sports federations). Russian state-funded media²³¹ and diplomatic services²³² republished leaks and pushed the moral equivalence defense, both referring to Western “hypocrisy.”

Precise destructive attacks: Two hours before the 2018 opening ceremony, GRU operators²³³ unleashed a worming and wiping malware dubbed “Olympic Destroyer” at the Olympics' key IT service provider, two South Korean ski resorts, and the games' official website.²³⁴ Just as the ceremony prepared to kick off, televisions in the press center stopped working, the stadium's Wi-Fi crashed, and the official website went offline.^{234, 235}

Widespread use of advanced weapons and technologies:

The Olympics campaigns employed several technically notable tactics. The GRU used a close access operations team to locally breach some antidoping targets, a capability of security services that is rarely publicly documented. Specifically, the GRU deployed two hackers^{236, 237} to locally breach the Wi-Fi networks used by WADA and U.S. antidoping officials at the 2016 Olympics in order to steal the officials' credentials for accessing an antidoping records database.²³⁸ Also, unusually, the GRU incorporated code in Olympic Destroyer from malware linked to numerous states (e.g., China, North Korea, Russia), to obfuscate Russia's role in the attack and deflect attribution by purely technical means.²³⁹



PROVOCATION OF RUSSIAN CULTURAL STRIFE

Russia views social stability as key to ensuring continued popular support for the government's authority; maintaining societal harmony is critical because politicized ethnic identification can become a strong vehicle of separatist organization and resistance.²⁴⁰ The possibility that foreign actors would work to create unrest in Russia by provoking ethnic, social, or religious tensions is therefore viewed as a military risk. Excessive stoking of these types of social divisions that has existed in Russia and the USSR for decades could lead to civil disobedience, expanded support for opposition candidates, or even the rise of separatist movements—a trend already observed in the North Caucasus, Tatarstan, and Bashkortostan regions.²⁴¹

When faced with criticism of its record on issues of human rights, civil and religious liberties, inter-ethnic conflict, and other social issues, Russia is typically quick to either establish a moral equivalency with its critics or seed an opposing narrative that distracts and redirects criticism toward others.²⁴² Taken further, this reaction is consistent with Russia's response to public criticism that Russia undermines and subverts its adversaries by exploiting those very same social tensions in their populations. Therefore, those accusing Russia of certain subversive measures are likely to become targets for GRU intelligence collection and efforts to distract, confuse, or undermine their credibility.



Case Study: Religious Leaders Threaten Russian Security Interests

SURVEILLANCE OF UKRAINIAN RELIGIOUS LEADERS

During Russia's conflict with Ukraine, several Ukrainian religious leaders and groups accused Russia of working to stir up social strife in Ukraine. The GRU likely sought to surveil these leaders to understand and prepare for further action should the narratives gather enough weight to cause reciprocal intercultural, social, ethnic, or religious tensions within Russia.

➤ **Awareness of potential military risks and threats:** The GRU has surveilled numerous religious groups in Ukraine that have alleged Russian attempts to stoke ethnic tension in Ukraine. Examples of this targeting include the following:²¹⁸

- **Ummah**, a Ukrainian Muslim group, has been sympathetic to Ukrainian nationalist concerns and critical of Russia's treatment of ethnic Ukrainians. Ummah publicly called for a more representative government through the 2013–2014 revolution and seeks broader recognition that the 1927–1933 famine was a genocide inflicted by the USSR on the Ukrainian people.²⁴³
- **Josef Zisels**, the chairman of the Association of Jewish Organizations and Communities of Ukraine, accused Russia of pushing an illegitimate narrative that the post-revolution Ukrainian government is deeply anti-Semitic.^{244, 245} For example, he accused Russia of surreptitiously committing hate crimes like vandalizing synagogues with neo-Nazi symbols to create the appearance of widespread Ukrainian antisemitism.²⁴⁵
- **The Ukrainian Greek-Orthodox Church** (a.k.a. the Ukrainian Greek Catholic Church) is an extension of the Western Catholic church that was forcibly absorbed by the Russian Orthodox Church during the Soviet era. The Ukrainian Greek-Orthodox Church has publicly blamed Russia for the conflict in eastern and southern Ukraine.²⁴⁶

MILITARY THREATS



SHARP DETERIORATION OF INTERSTATE RELATIONS

The Russian Armed Forces are attuned to monitoring for the deterioration of interstate relations and attempting to prevent these circumstances from escalating into an armed conflict. Within the broader context of Russia seeking stability in its international relations, Russia likely especially worries about sudden changes in its relationships—particularly relationships that are fundamentally consistent and non-confrontational over those that are contentious.

The 2013–2014 revolution in Ukraine has been a defining moment of Russia's recent international relations. The collapse of the Russia-friendly regime ushered in a pro-Western, anti-Russia Ukrainian nationalist government. Russia responded by launching a multidimensional hybrid war in Ukraine. The course of that conflict has made countering Russia an urgent political issue in many countries, degraded Russia's otherwise productive relationships with several Western powers, prompted a shift Westward among some officially neutral states, and strained Russia's relations with several historically friendly states on its borders.



Case Studies: Relations Deteriorate Due to the Ukraine Conflict (2014–2017)

PREPARATION OF THE BATTLEFIELD IN UKRAINE (2014)

Relations between Ukraine and Russia sharply deteriorated in 2013 and 2014. Ukraine appeared to be spiraling out of Russia's orbit—a massive geopolitical change along Russia's border. After several months of protests starting in late 2013, revolutionaries toppled Ukraine's Russian-friendly president in February 2014. The new Ukrainian government was eager to politically, militarily, and economically distance itself from Russia. It immediately signed a trade deal with the EU²⁴⁷ and a nuclear fuel deal with the U.S.-based Westinghouse Energy Company (WEC). The growing conflict between neighbors threatened to develop into a larger, more violent international conflict as a direct result of Ukraine's efforts to join NATO²⁴⁸ and boost NATO's presence near Russia's border.²⁴⁹

The growing conflict in Ukraine led to a sharp deterioration of relations with Russia—a leading threat to military security enumerated in Russia's Military Doctrine. A key component of the GRU's initial response appears to have been establishing beachheads for possible future destructive operations throughout Ukraine. These operations targeted several sectors that later experienced destructive attacks.

➤ Reduced time to launch military operations with preemptive activities: Starting around late 2013⁷³ or early 2014,²⁵⁰ GRU-linked operators attempted to breach varied Ukrainian targets including state-owned enterprises in the energy sector and railways, as well as federal and municipal government agencies.^{250, 251} Consistently, these sectors and entities were targets of GRU destructive attacks in the following years.

➤ Precise destructive attacks: Sometimes, the operators were caught while conducting internal network reconnaissance consistent with long-term planning for destructive attacks. In one instance, the operators stole virtual private network (VPN) credentials in May or June 2014 from a Ukrainian railway's partner, possibly a French telecommunications firm,^{73, 252} and proceeded to conduct internal reconnaissance at the railway.⁷³ The operators then destroyed the

victim's routers in June in apparent retaliation for remediation efforts by incident responders.⁷³

➤ Awareness of potential military risks and threats:

Ukraine's energy reliance on Russia has historically been a pressure point that Russia targets to resolve conflicts with Ukraine.²⁵³ Ukraine's growing partnership with WEC threatened to increase Ukrainian energy independence. Starting in November 2014, the GRU began a multiyear phishing and network reconnaissance campaign against WEC, repeatedly spearphishing WEC staff working in nuclear energy, reactor development, and reactor technology.^{229, 254} We identified one subdomain^o linked to the campaign referencing WEC's AP1000, a nuclear reactor design for which Ukraine had signed a memorandum with WEC to learn more about.²⁵⁵ The GRU operators' ultimate objective is unclear but may have been related to buttressing Russia's ability to increase pressure on Ukraine via the energy sector.

SURVEILLANCE OF OFFICIAL AND JOURNALIST INVESTIGATIONS INTO THE SHOOTDOWN OF FLIGHT MH17 (2014–2017)

In July 2014, Malaysian Airlines Flight 17 (MH17) exploded mid-flight over eastern Ukraine, killing all 298 people aboard. In October 2015, the Dutch Safety Board concluded that a Buk missile had caused the explosion, and subsequent multinational criminal investigations in 2016 and 2018 unequivocally determined the Russian Armed Forces had supplied the Buk missile system to Russian-backed separatists who shot down the plane.²⁵⁶ In addition to the formal investigation, the UK-based open-source investigation (OSINT) organization Bellingcat published a series of articles using public data to discredit the Russian Armed Forces' explanations for the incident and to support the criminal investigations' conclusion implicating the Russian Armed Forces in supplying the missile system.

These investigations threatened to provoke a large-scale diplomatic, military, and economic backlash against Russia—a key military threat per the Military Doctrine. In response, over several years, the GRU used numerous cyber capabilities to track and discredit parties involved in the investigation.

➤ Awareness of potential military risks and threats:

On August 22, 2015, a Finnish news outlet revealed that the Finnish Defense Forces had secretly detonated a Buk to test the theory that such a missile downed MH17.²⁵⁷ We assess that the GRU's alleged attempts to breach the email accounts of Finnish news outlets likely occurred in direct response to this revelation.²⁵⁸ A GRU-linked domain from this campaign, mimicking the only publicly disclosed news outlet targeted in the operation,²⁵⁸ was registered two days after the missile test news broke.¹⁴⁰ The Finnish government identified a second target of this phishing campaign: a Finnish journalist associated with the independent investigative outlet Bellingcat²⁵⁸ who had previously published research tracking the missile

^o Staff received messages appearing to be generated by their Microsoft Exchange Server, directing them to log-in to a phishing page at `webmail[.]westinghousenuclear[.]com`. Passive DNS databases indicate that the hackers created another subdomain, `apl000[.]westinghousenuclear[.]com`, a likely reference to the AP1000, Westinghouse nuclear reactor redesign. An operator appears to have erroneously created an intended subdomain name "AP1000.westin..." as "APL000.westin..." perhaps misreading the design name's number "1" as a lowercase "l"; typo-squatting a subdomain is superfluous.

launcher that downed MH17 from Russia into the separatist-held area of Ukraine.²⁵⁹

🔍 **Widespread use of advanced weapons and technologies:**

In addition to spearphishing, the GRU also used close access operations to surveil members of the MH17 investigation. In 2018, Dutch security officials revealed that they had captured members of the GRU's close access operations team. The Dutch allege that, among the operators' myriad activities, the team likely targeted Malaysian law enforcement officials connected to the investigation in December 2017 based on Wi-Fi connection logs found on a seized GRU operator's laptop.^{260, 261}

🔍 **Manipulation of social or political environment:**

The GRU has repeatedly threatened Bellingcat and attempted to embroil it in scandals. Bellingcat has extensively investigated Russian military- and GRU-linked incidents, including the downing of MH17,²⁶² the attempted assassination of Segey and Yulia Skirpal, the surveillance of worldwide sports anti-doping agencies,²⁶³ and the attempted coup in Montenegro.²⁶⁴ The GRU has repeatedly used its proxy social media identities like Anonymous Poland and CyberBerkut in attempts to embroil Bellingcat journalists in fictitious scandals (e.g., suggesting Bellingcat had published private information of Ukrainian soldiers, sold stolen credit card data.²⁶⁵) and likely coordinated fake journalist accounts to amplify these faux scandals.²⁶⁶

COUNTERING OF POLISH SUPPORT FOR UKRAINE AND ESCALATING POLISH RHETORIC ABOUT RUSSIA (2014)

Poland has emerged as one of Ukraine's most loyal allies during its conflict with Russia. In 2014–2017, Poland was Ukraine's fourth largest source of direct military assistance.²⁴⁹ It has consistently supported sanctions on Russia over its role in the conflict²⁶⁷ and been a reliable, vocal champion for Ukrainian interests in the EU and NATO.^{268, 269}

The situation grew especially tense in the late summer and fall of 2014. In early August, Poland and Ukraine signaled their expectation of a rapid escalation in the Ukraine conflict. On August 6, Poland's Prime Minister suggested that Russia was planning to launch a much larger invasion of Ukraine under spurious pretenses (e.g., humanitarian efforts, peace-keeping).²⁷⁰ Two days later, Ukrainian security services likely erroneously²⁷¹ claimed that Russia had planned to shoot down an Aeroflot flight filled with Russian vacationers (instead of MH17), blame it on Ukraine, and use it as a *casus belli*^p for a wider invasion of Ukraine.²⁷² Then, in October, Poland's former Minister of Foreign Affairs claimed²⁷³ that, in 2007, Russia had offered to dismantle Ukraine and divide it between Russia and Poland (the minister later retracted the claim²⁷⁴).

Poland's long-term military support for Ukraine and bellicose tone in 2014 threatened to draw other countries into the Ukraine conflict or, at least, prolong the conflict—variously

constituting a military threat and risk as defined by the Military Doctrine.

🔍 **Reduced time to launch military operations with preemptive activities:** The GRU likely sought to establish the ability to disrupt Poland's energy sector as a contingency plan. The campaign that established numerous beachheads in varied Ukrainian sectors in early 2014 reportedly also had an equal number of targets in Poland, but they were limited to the energy sector.^{41, 250, 275} Poland, like Ukraine, was highly susceptible to Russian pressure on its energy supply²⁷⁶ and consequently embarked on an aggressive energy independence strategy in the 2010s.²⁷⁷ Russian concerns about Poland's efforts to diversify its energy supply likely dovetailed closely with the country's increasingly vocal support for Ukraine.

🔍 **Awareness of potential military risks and threats:** The GRU plausibly responded to the escalating Polish and Ukrainian rhetoric about the MH17 shootdown in early August 2014 by attempting to surveil the Polish government. On August 11, GRU-linked operators spearphished senior⁴¹ Polish government members⁴⁰ with a lure containing a recent news article about Malaysia and the Netherlands calling for a cessation of fighting near the MH17 crash site.²⁷⁸

🔍 **Irregular and privatized warfare:** The GRU, in the guise of its hacktivist persona CyberBerkut, launched DDoS attacks on the websites of Poland's president and the Warsaw Stock Exchange (GPW) starting on August 14.²⁷⁹ The GRU persona stated that the attacks were in response to Poland's support for Ukraine's "fascist" government and sending "mercenaries" to the conflict.^{280, 281} CyberBerkut's messaging aligned with alleged Russian disinformation that circulated in Russian social and news media concurrently. This Russian narrative stated that mercenaries^q from a firm founded²⁸² by Poland's Interior Minister were illegally fighting in Ukraine.^{283, 284}

🔍 **Manipulation of social or political environment:** The GRU-purported mercenaries' scandal risked compounding another allegedly Russian-fomented narrative about Poland's Interior Minister. Earlier that summer, Poland accused Russia of bugging a controversial, profanity-laced discussion between Poland's Interior Minister and Central Bank Governor, tapes of which were leaked to the press in June and caused "mayhem" in Polish politics (the "Waitergate" scandal).^{285, 286}

🔍 **Precise destructive attacks:** In possible response to the false Polish claim that Russia had offered to divide Ukraine with Poland, the GRU conducted a multipart attack on the GPW. On October 23, GRU²⁸⁷ operators leaked 52 MB of login data from two educational stock market competition games and simulations run by GPW subsidiaries. The hackers also leaked administrator login credentials for GPW servers and routers, as well as network scans (nmap) of portions of the

^p **Casus belli** (literally, an "occasion of war") is a Latin expression referring to an event or circumstance that directly leads to a war, often used in the context of a state justifying a declaration of war.

^q Russia also alleged then and onward that mercenaries with Academi (formerly known as Blackwater) were also fighting in the Ukrainian conflict. Around October 26, 2014, the GRU spearphished Academi employees. (Sources: <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf>; <https://community.riskiq.com/search/mail.academi.com>).

GPW internal network.²⁸⁸ Finally, the hackers defaced GPW subsidiary websites with “an image of jihadists” and the English statement “To Be Continued....”²⁷⁹ The defacement and internal network leak likely served to signal Russia’s ability and willingness to disrupt the GPW if the tensions between Poland and Russia did not de-escalate.

RETALIATION AGAINST FRANCE’S REFUSAL TO DELIVER PURCHASED-AND-PAID-FOR WARSHIPS TO RUSSIA (2014–2015)

In early 2015, a growing dispute between Russia and France over a contract to build warships for the Russian navy was reaching a breaking point. In 2010, France agreed to a \$1.5 billion contract to build two carriers for Russia—Moscow’s first major arms importation deal since the fall of the Soviet Union.²⁸⁹ In September 2014, France temporarily suspended the vessels’ delivery because of Russia’s role in the Ukraine conflict²⁹⁰ and extended the suspension again in November, citing lack of progress on meeting new criteria (e.g., observing a multilateral ceasefire).²⁹¹ On January 15, 2015, Russia announced its plans to soon initiate legal action against France,²⁹¹ signaling a deterioration in negotiations. Ultimately, on April 16, Russia demanded that France refund the warships, apparently resigned that France might never deliver the vessels.

Russia may have interpreted these circumstances as either a French failure to comply with international agreements (a military risk) or, within the broader Ukraine conflict context, as a sharp deterioration in its relationship with France (a military threat). In a possible response to these rising tensions, on April 8, 2015, the GRU^{292, 293} conducted a destructive attack on a French television station, TV5Monde, in the guise of jihadist hacktivists. This attack followed in the mold of other GRU-linked faux jihadist attacks in the preceding months, such as the GRU’s disruption of a Polish stock exchange (page 31) and U.S. media outlets (page 13).

➤ Reduced time to launch military operations with preemptive activities: GRU operators first breached a TV5Monde resource about a week after Russia announced its plans to litigate the vessels’ delivery.³⁹⁴ They ultimately performed actions on objectives one week before Russia signaled that it was resigned to possibly never receiving the vessels, launching a multipart attack made possible by the operators’ protracted access to TV5Monde.

➤ Precise destructive attacks: The operators conducted varied, precise destructive actions to conclude their operation. They erased the firmware on nearly all of TV5Monde’s routers and switches,²⁹⁵ disrupting broadcasts for three hours.²⁹⁶

➤ Manipulation of social or political environment: Concurrent with the destructive attack, the operators took control of the TV5Monde website and social media accounts to claim credit for the attack as CyberCaliphate and published

personal information belonging to French soldiers involved in anti-ISIL operations.²⁹⁷ The use of an ISIL fakativist group spoke to elevated concerns in France about Islamic terrorism and rising Islamophobic sentiment regarding France’s often poorly integrated Muslim population.^{298, 299, 300} CyberCaliphate explicitly referenced the January 7–9, 2015, île-de-France attacks,[†] riffing on the “Je suis Charlie” slogan as “Je SuIS IS” and referencing the attacks in a Facebook post.²⁹⁷

MONITORING OF AND RESPONSE TO DETERIORATING RELATIONS WITH GERMANY (2014–2017)

Russia’s relationship with its historically important European partner Germany has been strained by the war in Ukraine. Putin’s return to power in 2012 initially propelled this shift, as his antidemocratic, nationalistic policies unsettled the German establishment, and the 2014 annexation of Crimea decisively ended most lingering good feelings.³⁰¹ Germany responded by sanctioning Russians, increasing military spending, and championing European unity and the continued relevance of NATO. In late November 2016, news surfaced that a leading proponent of these measures^{302, 303, 304} would become Germany’s next Ambassador to the UN following a scheduled vote in September 2017.^{305, 306}

The sharp deterioration of Russia’s relations with Germany constituted a military risk, demanding a response from Russia’s Armed Forces. The GRU likely responded by conducting a large-volume intelligence-gathering campaign targeting German parliamentarians and attempting to defame Germany’s sharp Russia critic before he received the UN ambassadorship.

➤ Awareness of potential military risks and threats:

The rapid devolution of Germany-Russia relations in 2014 established a need to closely track evolving political dynamics within the German government. Over six months, December 2014 through May 2015,³⁰⁷ GRU³⁰⁸ operators breached the German parliament’s internal ParlaCom network,³⁰⁷ compromised all 20,000 email accounts,³⁰⁹ and exfiltrated 16 GB of data, mostly from email inboxes.³¹⁰ The GRU likely sought to identify allies amid the growing political turbulence. GRU operators reportedly appeared to primarily target the inboxes of parliamentarians from Germany’s rising,³¹¹ third-largest³¹² political party Die Linke (The Left).³¹³ At the time, Die Linke was tilting toward hardliners supportive of anti-NATO policies³¹⁴ and seeking to form an alliance with Russia.³¹⁵

➤ Manipulation of social or political environment:

The GRU attempted to embroil the incoming UN ambassador in scandal before he could take his new post. In approximately April 2017, the GRU breached UN email accounts and later provided a portion of the stolen emails to Der Spiegel,³¹⁶ which it published in November 2017.³¹⁷ The emails purported to show the ambassador improperly asking the Secretary General’s chief of staff in December 2016 to procure a job for his wife, who was also a diplomat.³¹⁶

[†] The **Île-de-France attacks** were a series of jihadist-linked terrorist attacks in and around Paris that are most famous for the murder of 11 employees of satirical magazine *Charlie Hebdo*. The attacks gave rise to the French unity slogan of popular resistance, “Je suis Charlie!” (I am Charlie!).

PUSHBACK AGAINST THE RISE OF WESTERN POLITICIANS STRONGLY OPPOSED TO RUSSIAN INTERESTS (2015–2017)

Russia's actions in Ukraine were a watershed moment in Western politics. The events likely compelled many NATO-country politicians to come out publicly opposed to Russian foreign policy interests and several officially neutral states to shift Westward. Notable examples of this shift include the following:

The Netherlands: In the 2000s and early 2010s, Russia and the Dutch touted their strong trade and cultural relations.³¹⁸ After several scandals,^{318, 319} the Netherlands fully reoriented in strong opposition to Russia after it annexed Crimea and, according to Dutch investigators, it enabled the shootdown of MH17, which killed 193 Dutch nationals.³²⁰

France: In November 2016, Emanuel Macron joined a crowded field of candidates for the 2017 French presidential election. The leading candidate then appeared to be Marine Le Pen, an overtly pro-Russia, anti-EU candidate, followed by other Russian accommodationists and mostly Eurosceptics.^{321, 322, 323} Macron quickly gained support³²⁴ as a fervent supporter of the EU (e.g., proposing an EU defense force)³²⁵ and internationalism.³²⁶

United States: In the 2016 U.S. presidential election, early front runner Hillary Clinton positioned herself as a strong proponent of NATO and a Russia-hawk.³²⁷ The Russian foreign policy establishment openly worried that her tendency to “stubbornly adhere to moral postures regardless of their consequences” could spark a war with Russia.³²⁸

Malta: Though officially military neutral, Malta took positions strongly opposed to Russian interests in the mid-2010s. In 2014, Malta condemned the annexation of Crimea,³²⁹ and in 2016, it refused use of its ports and airspace to the Russian military.³³⁰ Russian state-media characterized this trend as “Russophobia” that might draw Malta into wars.³³¹

In response to this broad deterioration of relations with the West, the GRU engaged in myriad activities to neutralize or counter this military threat. Unlike in Ukraine, Russia's interference in other Western elections has almost exclusively focused on causing informational-psychological effects. We observe that the GRU has taken steps to obtain the ability to cause informational-technical effects that might result in the manipulation, disruption, or destruction of election infrastructure, such as websites that host vote totals, companies providing software for voting machines, and agencies retaining voter registration data.

Manipulation of social or political environment: GRU leaks and Russian social media disinformation campaigns served to aggravate political disunity and discord. In 2016, the GRU fomented tensions in the U.S.'s Democratic Party by leaking Clinton associates' emails on the eve of the Democratic National Convention, the conclusion of a divisive nomination process. The GRU's proxies and allies claimed that the emails showed a conspiracy to unfairly buttress candidate Clinton,³³² thereby exacerbating internal party tensions and decreasing confidence in the democratic process.³³²

In France, GRU operators leaked emails from Macron, purporting to show that he had an undisclosed offshore bank account,³³³ Russian state-sponsored social media influence operations promoted candidates with pro-Russia stances,³³⁴ and the Russian government allegedly funneled financial assistance to Macron's competitor.³³⁵

The Netherlands claims that Russian actors spread online rumors with intent so sway popular opinion around the election.³³⁶

Reduced time to launch military operations with preemptive activities: Attempts to steal election-related emails in the U.S. and France began months before they were leaked, enabling the GRU to maximize their impact by releasing them at opportune moments. The Macron leaks occurred variously on the eve of the final candidates' debate, allowing his opponent to highlight them,³³³ and immediately before the media blackout prior to the election, denying the media an opportunity to debunk them.³³⁷ The Clinton leaks, as mentioned, were timed to inflame party tensions about a contentious primary process.³³²

Precise destructive attacks: The GRU targeted election infrastructure in numerous countries. In the U.S., the GRU breached a voting software company, county websites, and state voter registration databases, and conducted network and infrastructure reconnaissance in all 50 states.^{338, 339, 340} Russian operators, likely the GRU, penetrated unspecified infrastructure in France,³³⁷ and Dutch authorities abandoned ballot counting software in favor of manual tabulation because of unspecified concerns about the vote's integrity.³⁴¹ Like the Ukrainian CEC attack (see pages 24–25), the GRU might have wanted to be able to alter unofficial vote tallies on state or local websites. Like the GRU's data destruction attacks, GRU operators might have attempted to corrupt voter registration data or push out malicious updates to voting machine customers. Furthermore, public awareness of the activity prior to elections could have reduced voter confidence in the integrity of the electoral process, throwing elections' outcomes into question.



DISRUPTION OF KEY RUSSIAN MILITARY CAPABILITIES OR CRITICAL SECTORS

For Russia, the state-sponsored obstruction of its core strategic military capabilities or endangerment of its most sensitive sectors constitutes a likely prelude to armed conflict. Attacks on Russia's command and control, nuclear weapons, space control, and missile warning systems might reduce Russia's ability to deter or respond to a nuclear first strike—a leading concern for Russia's national security apparatus in the context of strategic stability (see also page 15). Likewise, the disruption of pharmaceutical, chemical, nuclear, medical, and energy sectors—the sectors named in the Military Doctrine—may pose an immediate threat to life.

In the past decade, Russia has alleged on a few occasions to have been targeted by foreign state-sponsored cyber operations.

Disruption of Russian Military Capabilities: In February 2019, a Kremlin spokesman stated, without further providing detail, that a “huge number of cyber attacks are constantly carried out from U.S. territory against various organizations, legal entities, and individuals.”³⁴² This statement appeared in the context of *Washington Post* reporting that claimed the U.S. had disrupted internet access at a known Russian social media influence operation (the “troll farm”) on the U.S.’s 2018 Election Day.³⁴³

Intrusions in Russia’s Critical Sectors: In June 2019, Russian media reported that security services had “neutralized” U.S. attempts to “attack” Russian industrial control systems,³⁴⁴ a claim made in the context of *The New York Times* alleging U.S.-sponsored intrusions in Russia’s power grid.³⁴⁴ Russian media further claimed that foreign intelligence services have, in recent years, increasingly targeted Russia’s transportation, banking, and energy infrastructure.³⁴⁵

Despite these claims, no reviewed, publicly disclosed GRU-linked cyber operations appear to be in response to these reported activities. Because no disruptions of Russian critical systems were reported, the GRU may have assessed that no relevant activity crossed the line of being a military threat. Alternatively, the GRU may have responded with new attempts to establish similar beachheads in U.S. critical infrastructure that have not been reported. An earlier instance of similar activity is apparent in U.S. Government claims that GRU³⁴⁶ operators attempted to breach U.S. industrial control systems, including energy infrastructure, in a 2011–2014 campaign—^{347, 348} actions consistent with the GRU’s need to reduce time to action with preemptive access.



SUPPORT OF ARMED INSURRECTION IN RUSSIA OR ITS ALLIES

In light of Russia’s steadfast support of the inviolability of state sovereignty and territorial integrity, foreign state-sponsored support of armed insurrection within the territory of Russia or an ally would likely be a sufficient threat to precipitate a military response. Armed insurrection within Russia is a clear threat to Russian security, and eliminating sources of training and support for groups involved in insurrection would be a top priority for the military. In cases where the perceived support of insurrection occurs within the territory of a foreign partner—such as U.S. support of the Kurds during the Syrian civil war—Russia may decide that an even higher level of direct support is necessary before taking military action.

Despite the likelihood that Russia’s military would view the support of armed insurrection as a military threat, there are

no instances available in reviewed open sources that document GRU-linked cyber operations we assessed to be likely conducted to counter support for armed insurrection. The lack of publicly available evidence of such activities may reflect the fact that there have been few instances of Russia alleging foreign state-sponsored armed insurrection within Russia since the Chechen Wars of the 1990s. In 2015, Putin accused the U.S. of providing support to North Caucasus separatist fighters “trying to tear Russia apart” during the mid-2000s.³⁴⁹ Although we did not find any clear examples of cyber activity related to this claim, it is nevertheless consistent with activity that would typically provoke a military response.



USE OF MILITARY FORCE DURING EXERCISES ADJACENT TO RUSSIA OR ITS ALLIES

Russia likely increasingly views U.S. and NATO military exercises as military threats because they increasingly occur close to Russian territory.³⁵⁰ Since Russia’s annexation of Crimea, NATO exercises have expanded in size and scope, drawing nearer to Russian borders and increasingly involving non-NATO forces.³⁵¹ Russia’s military monitors exercises in Europe and Central Asia and likely views NATO’s expanded footprint into areas close to its territory or those of its allies as destabilizing actions that could spark military conflict.

Russia has already adjusted its own military exercises in response to the expansion of NATO exercises in Europe. Russia has in recent years moved its own exercises to closely match those conducted by NATO forces; in 2015, Russia mirrored NATO drills in the Baltics, Romania, and Hungary.³⁵² In 2018, the Russian military took the unusual step of jamming Global Positioning System (GPS) signals in the Kola Peninsula—Russian territory bordering Norway and Finland—during NATO’s exercise Operation Trident Juncture.³⁵³ The jamming was probably because of the proximity of the exercise to Russia, as well as the fact that the operation was the largest NATO exercise since the Cold War and involved non-NATO members Finland and Sweden.³⁵⁴



Case Study: Finland Hosts NATO Exercises (2016)

INCREASED SURVEILLANCE OF FINLAND'S POLITICAL-MILITARY ESTABLISHMENT (2016)

Much to Russia's distress, neighboring Finland has increased its cooperation with NATO. Despite being an EU member, Finland has insisted for decades that it will not join NATO. In the 1990s, for example, Finland indicated that joining NATO would make it untenably responsible for smaller Baltic countries' security from Russian aggression.³⁵⁵ Ironically, Russian aggression in Eastern Europe in the past decade has actually spurred Finland to expand its partnership with NATO.³⁵⁶ According to a senior Finnish diplomat, "Keeping Finland out of NATO is Russia's primary political objective in the region,"³⁵⁷ and Russia has warned that Finland joining NATO could fundamentally sour Finland's relationship with Russia.³⁵⁶ As Finland's cooperation with NATO increases—marked by hosting NATO landing exercises for the first time in June 2016³⁵⁸—Russia's concerns have likewise grown.

The conduct of NATO landing exercises adjacent to Russia and the growing Finland-NATO relationship constitute threats and risks noted in the Military Doctrine. These circumstances have likely prompted the increased GRU intelligence collection focus on Finland.

➤ Awareness of potential military risks and threats:

The Finnish Security Intelligence Service (Supo) observed an overall uptick in cyber espionage activity in 2016, noting that GRU-linked operators were responsible for most of the year's state-sponsored cyber activity.³⁵⁹ This activity principally targeted individuals involved in Finnish national security and foreign policy, rather than in private companies.



Case Study: Kazakhstan Hosts U.S.-led Military Exercises with Several NATO Members (2017)

SURVEILLANCE OF STEPPE EAGLE MILITARY EXERCISE PARTICIPANTS (2017)

Kazakhstan and Russia have generally favorable but uneasy relations, especially under the country's previous president (Nursultan Nazarbayev, in office 1990–2019). Growing Kazakhstani independence in foreign, economic, and military policy in the 2010s under Nazarbayev gave Russia cause for concern.³⁶⁰ Kazakhstan's ongoing involvement in NATO's Partnership for Peace Program by receiving training and participating in U.S.-led military exercises (e.g., Steppe Eagle)³⁶¹ prompted "paranoid"³⁶² reactions among Russian elites in the wake of Ukraine's Westward tilt after its 2014

revolution. In April 2017, Kazakhstan hosted the Steppe Eagle military exercises, which involved a mixture of Central Asian and NATO states. Monitoring military developments related to NATO are a consistent area of interest for the GRU.

A Russian partner and neighbor like Kazakhstan hosting U.S.-led military exercises constituted a risk as described in the Military Doctrine. We assess that an early 2017 GRU-linked phishing campaign may have attempted, in part, to surveil participants in this exercise, based on its timing and targets.

➤ Awareness of potential military risks and threats:

The campaign reportedly targeted government and defense entities operating in Central Asia with possible connections to NATO.³⁶³ Campaign targets were in Kazakhstan, Turkey, Kyrgyzstan, the UK, Uzbekistan, Armenia, and Jordan. These targets significantly overlapped with the April 2017 Steppe Eagle participants: Kazakhstan, Turkey, Kyrgyzstan, the UK, Tajikistan, and the United States.³⁶⁴



HEIGHTENED COMBAT READINESS

Like most countries, Russia considers the enhancement of an adversary's combat readiness, including the intensification of wartime activities, partial or full mobilization of troops, or the enhancement of government or military command and control to wartime status as a major threat to its security. Because enhanced combat readiness could be an indication of impending offensive activities, Russia's military is deeply concerned with the operational status of its adversaries' militaries. Activation of military forces is particularly threatening to Russia when it occurs in countries within Russia's extended cultural periphery or near its borders.³⁶⁵ Mobilization of U.S. or NATO troops in Eastern Europe, post-Soviet states, and the Baltics would likely prompt the Russian military to take action to alleviate or respond to the threat of outright armed conflict.³⁶⁵



Case Study: Ukraine Shifts to a Wartime Footing (2018)

COUNTRYWIDE AND TARGETED DESTRUCTIVE MALWARE INFECTIONS IN UKRAINE (2018)

In February 2018, Ukraine announced that it would adopt a more aggressive strategy to expel Russian forces from its contested Donbas region.³⁶⁶ Up to that point, Ukraine had formally referred to its response as the Anti-Terrorist Operation (ATO), which was led by the Security Service of Ukraine (SBU, a law enforcement agency). Starting on April 30,³⁶⁷ the newly named military-led Joint Forces Operation would make the “reintegration of Donbas[s]” an explicit goal and be led by Ukrainian Armed Forces.³⁶⁸ The change shifted the mission focus from fighting separatists (referred to as “terrorists”) to directly confronting the Russian military.

Ukraine’s policy shift to militarily engage Russian and Russian-backed forces in Ukraine was consistent with the threat posed by heightened combat readiness identified in the Military Doctrine. This military threat may have prompted two major GRU³⁶⁹ operations in Ukraine using the modular, destructive VPNFilter router malware. U.S.³⁷⁰ and Ukrainian^{371, 372} authorities successfully neutralized these operations before the operators could abuse their access.

🔥 Warfare impacting the entire depth of an enemy’s territory simultaneously: On May 8 and May 17, 2018 operators conducted a large-volume infection across Ukraine’s territory.³⁷³ The mass infection occurred immediately before holidays relating to Ukrainian identity and history, celebrating the end of World War II (May 9) and the founding of the EU’s precursor entity (May 20). This timing pattern is consistent with GRU attacks in 2015–2017, like NotPetya, assessed in the IMF Loan case study, on pages 17–21. Based on this pattern, the GRU may have considered conducting another widespread disruptive attack on holidays and anniversaries related to Ukrainian identity.

🔗 Widespread use of advanced weapons and technologies: VPNFilter is a modular malware likely based on the BlackEnergy2 and BlackEnergy3 malware,³⁷⁴ which were mainly associated with the GRU technical-informational effects team. VPNFilter serves a variety of functions like modifying device configurations and redirecting traffic.³⁷⁵ Significantly, VPNFilter sometimes contains modules used to monitor for Modbus supervisory control and data acquisition (SCADA) protocols, which are used in industrial environments to monitor and control physical equipment.³⁷⁶ This capability is a strong indicator of the operators’ likely ability to perform technically challenging targeted disruptive attacks on industrial control systems.

🎯 Precise destructive attacks: On July 11, 2018, Ukraine announced that it had thwarted a GRU operation attempting to disrupt the operations of a liquid chlorine bottling facility in eastern Ukraine (AKhPS^s).³⁷⁷ The hackers had reportedly

targeted the plant’s process control and emergency detection systems.³⁷⁷ Like the 2016 power outage attack (see page 20), this activity is consistent with establishing the ability to create a specific dangerous condition at the plant and reduce the ability of the safety systems to detect or respond to the condition. Since June 19, AKhPS was Ukraine’s only functional liquid chlorine bottler, a lynchpin in the country’s clean water supply.³⁷⁸ The operation’s target and timing suggest an operator intention to specifically target this facility, as opposed to any Ukrainian critical industrial asset.

🚩 Irregular and privatized warfare: Since 2017, the UN warned that Russian-backed forces in eastern Ukraine were kinetically targeting water filtration and purification plants, which stockpile liquid chlorine, and risked causing mass-casualty events.^{379, 380} Russian-linked forces continued to attack Ukrainian water works around the time of the VPNFilter event at AKhPS. The Donetsk Filtration Station, for example, was shut down on multiple occasions in April and May 2018 due to violence.³⁸¹

🗑️ Manipulation of social or political environments: AKhPS may have been the concurrent target of a Russia-linked fear-mongering disinformation campaign. In the month prior to the cyber operation’s disruption, sudden rumors emerged suggesting that AKhPS was unsafe, compelling the plant to host a press conference on June 20 detailing the plant’s numerous safety precautions. Furthermore, the plant accused a controversial journalism group “Stop Corruption”^t of waging an information war against the plant by pushing these rumors.³⁸² We found no evidence linking Stop Corruption to Russia, but the timing and specifics of its complaints about the AKhPS combined with its reported history of pushing debunked news stories³⁸³ make its operations suspect.³⁸⁴ The disruption of Ukraine’s only functioning chlorine bottler might have sparked panic about access to clean water in Ukraine.^{381, 385}

^s The official name of **Auly Chlorine Filling Station** in Ukrainian is “Аульська хлоропереливна станція” or “Aulytska KhloroPerelyvna Stantsiya” (АХПС, AKhPS). No official English translation of this company’s name appeared in reviewed sources.

^t **Stop Corruption** (Стоп Корупції) is an investigative journalism group whose stated objective is reducing corruption in Ukraine. It was the first group ever expelled from the Global Investigative Journalism Network, done so on the grounds that it was excessively political, had shown signs of lacking “journalistic professionalism,” and had conflicts of interest. (Source: <https://imi.org.ua/en/news/stop-corruption-expelled-from-global-investigative-journalism-network-i27635>)

What's Next



Looking at the world through the context of the Russian Military Doctrine, we assess several emerging circumstances that may constitute risks and threats that the GRU must monitor, neutralize, or counter.

NATO CONTINUES TO EXPAND

Several states are either seeking to join NATO or are in the process of completing the process to join the alliance—a listed threat in the Military Doctrine. The GRU will likely attempt to derail ascension processes and increase its surveillance of incoming members.

Ukraine: Russia will likely attempt to dissuade other NATO members from approving Ukraine's membership. NATO's Article 5 demands that all members come to the aid of any member if it is attacked. By approving Ukraine's membership during an active conflict, other NATO members would risk being compelled to become immediately and intimately involved in Ukraine's fight with Russia. Cyber attacks can keep the conflict alive without being so devastating as to draw a major international kinetic intervention. Furthermore, continued cyber attacks in Ukraine send warnings to Russia's adversaries and wavering partners, demonstrating Russian capabilities.

Bosnia: Russian proxies are aggravating ethno-religious strife and buttressing ethno-nationalist candidates in Bosnia, risking delaying the country's NATO ascension.³⁸⁶ Pro-Russia politicians have repeated the Russian narrative that democracy promotion, good governance, and international aid groups, like USAID, are Western (or U.S.-specially) tools for illegitimately interfering in Bosnia's internal affairs.³⁸⁶ These activities could be supported by cyber operations. In other countries the GRU has used

cyber operations in attempts to discredit such democracy promotion groups (see page 25) and foment ethnic tension (see page 22).

Georgia: As of late 2019, Russia has indicated that Georgia's possible NATO ascension may create two separate problems: Georgia joining NATO and Georgia asserting that its Russian-occupied territories would be defended by NATO.³⁸⁷ This position is consistent with the Military Doctrine's concerns about NATO expansion and the violation of Russian allies' territorial integrity. GRU operations have continued to target Georgia when its NATO relations appear to be strengthening.⁵¹² For example, days after Georgia's Defense Minister met with NATO in October 2019,³⁸⁸ a large cyber operation defaced thousands of Georgian websites and disrupted the broadcasts of two major Georgian broadcasters.³⁸⁹ Concurrently, Russia-backed traditional news and "fringe" social media outlets amplified unsubstantiated information about the attack,³⁹² and a disinformation campaign claimed that Georgia's potential NATO membership would hinge on legalizing gay relationships,³⁹⁰ which are overwhelmingly disapproved of in Georgia.³⁹¹

North Macedonia: North Macedonia will likely soon secure the approval of outstanding NATO members to complete its membership process. The GRU has likely already attempted to derail the process in North Macedonia in 2018; the U.S. alleges that Russia attempted to covertly influence a vote to change the country's name, a sticking point in securing critical Greek support for North Macedonia's ascension.³⁹³ As the ascension concludes, the GRU will likely surveil the North Macedonian government, military, and defense sector, much like it did during Montenegro's ascension (see page 12).

COMPETING CENTRAL ASIAN INTERESTS STRAIN RUSSIA'S RELATIONS WITH CHINA

In the 2010s, Russia grew concerned about China's expanding economic and political relationships with Central Asian countries.³⁹⁴ China has broken Russia's energy monopoly in Central Asia with new pipelines, undercutting a key lever for Russian influence.³⁹⁵ The diminution of Russian influence along its Central Asian periphery may be considered regional destabilization, a military risk in the Military Doctrine. Russian soft power initiatives may be indicators of parallel covert activities by the GRU. In response to China's evolving relationships in Central Asia,³⁹⁶ Russia has increased its regional infrastructure investment³⁹⁷ and military cooperation.³⁹⁸ The GRU will likely surveil politicians, diplomats, and militaries in Central Asia to maintain awareness of this shifting geopolitical landscape. The GRU might establish beachheads in energy and financial institutions in Central Asian countries to reduce the time to action as a hedge against their relations with Russia suddenly deteriorating.

RUSSIA PLACES INCREASED SIGNIFICANCE ON EAST ASIA

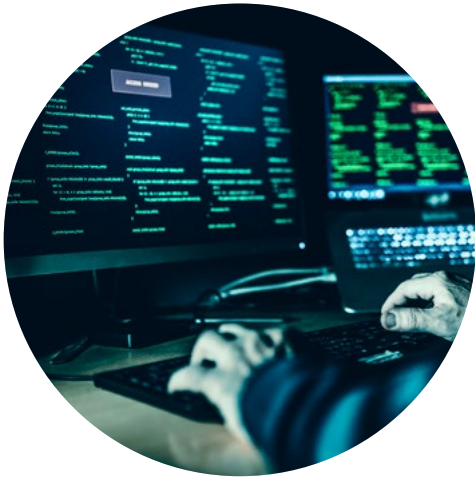
In the past decade, Moscow has declared that it will "pivot to the East" in both political-military and economic senses.³⁹⁹ Russia's strategic reprioritization of East Asia may lead to GRU activities intended to better track and secure its military interests in the region. Key areas of surveillance will likely include U.S.-led military exercises in the Asia-Pacific region and the diplomatic affairs of U.S. partners, like Vietnam,⁴⁰⁰ where Russia has attempted to build military ties.⁴⁰¹ The GRU may also attempt to weaken governments and destabilize societies unfriendly to Russia's growing regional interests; Kremlin-funded media outlets already reportedly engage in such disinformation and propaganda activities in the region.⁴⁰²

COMPETITION IN THE ARCTIC

Global warming has increased the military⁴⁰³ and economic⁴⁰⁴ importance of the Arctic. Russia has rushed to establish its territorial claims to the region by petitioning relevant UN authorities,^t but other states have offered competing claims.⁴⁰⁵ The GRU will likely surveil these authorities and other claimants, much as the GRU surveilled investigators and arbitration bodies in the MH17 downing and Olympic doping incidents, and may attempt to discredit these entities if Russia's claims to the Arctic are not ultimately recognized. Russia also worries that a strengthening NATO presence in the Arctic will endanger Russian's northern border.⁴⁰³ The GRU will likely surveil participants in NATO's Arctic exercises⁴⁰⁶ and conduct disruptive attacks against non-NATO Arctic states forming closer military ties with NATO.

^t The **UN Commission on the Limits of the Continental Shelf** (UNCLOS) is a UN body responsible for recognizing exclusive rights of states to their claimed oceanic territory as determined by the extent of their continental shelf. (Source: https://www.un.org/Depts/los/clcs_new/commission_purpose.htm#Purpose).

Conclusion



The GRU is a prolific, capable, and determined threat actor. Its operations blend technical prowess with strategic vision, taking deliberate steps to target data and systems in ways that advance long-term national military security objectives. Fortunately for defenders, the GRU's process for selecting targets and methods is consistent and therefore predictable. By understanding threat actor motivations, defenders can anticipate when, where, and how attacks will unfold—enabling defenders to take deliberate steps to improve their security posture.

FOR HOW LONG WILL THIS FRAMEWORK BE APPLICABLE?

The next Russian Military Doctrine—expected to be published in 2020—will likely be an iterative evolution of the 2014 doctrine, making this report's framework still broadly applicable, with a need to update specifics. Russian Armed Forces statements from 2019 continue to affirm the 2014 doctrine's core military confrontation concepts, emphasizing hybrid-warfare in modern military conflict, asymmetric capabilities, information confrontation, and sabotage that disrupts social-political stability by creating “an atmosphere of chaos and uncontrollability.”⁴⁰⁷

The Russian military seeks to maintain high-combat readiness and improve nonnuclear deterrence by creating “threats of inflicting unacceptable damage.”⁴⁰⁷ The GRU will therefore likely seek to establish cyber-based deterrence, perhaps signaling that the GRU possesses the access and ability to disrupt critical sectors. To this end, we expect attempted intrusions will likely occur in Western critical sectors such as energy, utilities, and transportation, and attacks are more likely in non-NATO countries, where they are less likely to draw an allied military response.

The Russian military aspires to better coordinate with economic, political, and other nonmilitary elements of state power.⁴⁰⁷ In contrast to trends in the previous decade,⁴⁰⁸ this coordination could plausibly lead to GRU cyber operations occurring in collaboration with Russian civilian security services. Such coordination could undermine attribution efforts going forward.

HOW DOES THIS FRAMEWORK APPLY TO OTHER STATES?

This analytical framework's concepts are broadly applicable to other states and their cyber operators. States' strategic priorities are often public, captured in strategic doctrine, and reaffirmed regularly through statements and overt noncyber policy. By understanding those priorities, we may anticipate the targets and focus areas of state-sponsored operations, as well as contextualize active and completed operations.

Contextualizing Chinese cyber-enabled intellectual property theft, for example, has a fundamentally similar underlying logic to assessing GRU operations. The Chinese government periodically identifies its social and economic goals for the near future. These goals are published in strategic documents, like the Five-Year Plans, much like the Russian government's periodic statement of military priorities in the Military Doctrine. China's cyber economic espionage operations for more than a decade have had a strong alignment with specifically enumerated state priorities; China's declared intent to reduce pollution with green technologies paralleled the theft of wind turbine and solar panel intellectual property by Chinese cyber threat actors.⁴⁰⁹

HOW DOES THIS FRAMEWORK HELP DEFENDERS?

Our framework unveils a notoriously opaque cyber threat actor and lays bare an organization that, although highly effective in its operations is, at its core, a bureaucracy of people working to implement Russia's specific and publicly known security priorities. Understanding the rationale behind the GRU's cyber operations also makes their timing, methods, and targets broadly predictable. Organizational leaders and network defenders alike can use the increased certainty our framework provides in their strategic decision-making, risk modeling, and security postures.

Protect Your Organization



Understanding adversaries' motives is critical to proactive, efficient threat mitigation and risk management. A narrow, inflexible focus on compliance and recovery coupled with a lack of awareness of relevant threats can lead to persistently mounting costs to defend against a vague constant threat of attack. A deep understanding of threat actors can lift this haze, allowing pointed, deliberate, and informed decisions about managing risk from the c-suite to hands-on-keyboards network defenders. This agile, threat-centric security paradigm ultimately aims to drive efficiencies by continuously anticipating, mitigating, detecting, responding, and recovering from rapidly evolving threats.

CYBER RISK MANAGEMENT

Adopt a threat-centric risk management approach to better understand threats, attack vectors, and critical assets, and to prioritize efforts and optimize your investment. Focus on strong asset management and surface area reduction and adopt best practices and settings for configuration management.

Threat Landscape Assessment: Evaluate relevant adversaries' motives, methods, and intentions related to your organization, its sectors, its geographic areas of operation, and its critical assets to increase your awareness of your attack surface and to inform organizational resource optimization and risk management strategies. The results of a threat landscape assessment, paired with the high-value asset identification described in the next recommendation, are central to selecting impactful security controls.

High-Value Asset Identification: Identify the information or resources whose confidentiality, integrity, or availability are most critical to your organization's success. Next, determine if this critical information or resources are similar to assets known threat groups have previously compromised. You will then need



to evaluate whether your top adversaries would consider the abuse of these assets to be useful or unique for advancing their goals. Understanding the vulnerabilities and security control gaps previously leveraged to exploit these assets is a critical step. This allows you to prioritize vulnerability management and security gap mitigations on high-value assets based on impact on mission and business. Applying appropriate mitigation plans will reduce your overall attack surface and ensure your most valuable assets are optimally protected.

Threat, Control, and Risk Modeling and Simulation: Assess the alignment of your security controls and risk management strategy to your top adversaries' capabilities and intentions. This can be accomplished by developing hypothetical scenarios that explore possible future adversary tradecraft to develop a proactive security stance, ahead of adversary capability developments. Then use analytics, modeling, and simulation techniques to run what-if scenarios and gather insights that optimize risk management in the context of your specific threat landscape.

CYBER DEFENSE

Harness insights gained through continuous threat intelligence analysis to predict and defend against evolving attack patterns. Keep your networks secure with a strong vulnerability management program that actively searches for unpatched systems and unauthorized activity. Build, test, and fund incident response plans that can be implemented to thwart data loss or downtime at a moment's notice. Leverage any security incidents to strengthen the program by systematically capturing and integrating lessons learned.

Continuous Risk Management: Adjust your security posture based on anticipated future threat activity. Your adversaries' perspectives on your organization may change due to your business decisions, such as starting new lines of business or entering new markets, or due to broader geopolitical circumstances.

Logging: Maximize network visibility and centralize logs to the greatest extent reasonable. Historic NetFlow traffic and Endpoint Detection and Response (EDR) data can be extremely useful for understanding what happened in incidents. For example, log analysis showed¹¹⁵ that the disruptive attack on a Ukrainian power distribution station in 2016 plausibly had a far smaller impact than attackers may have intended (see page 20). Logging can also provide data to test analytics, train advanced analytics-based detection models, and update organizational threat modeling.

Threat Intelligence: Identify, contextualize, and track campaigns and threats, and integrate these insights into security planning and operations. Actively seek out new sources of threat intelligence that improve situational awareness of political and economic events and interests that trigger adversary response or retaliation. Tracking and analysis of the string of faux-ransomware attacks in Ukraine prior to the NotPetya event (see pages 17-20) might have informed useful defense strategies, such as

global companies reducing connectivity with their Ukraine units around national holidays and anniversaries related to Ukrainian identity and independence.

Advanced Detection: Inform analytic development from threat modeling, prioritizing the most likely attack vectors. Analytics-based detection is key to hunting advanced adversaries that do not use commoditized attack tactics and cannot be detected using commoditized cyber defense. Investing in an analytics platform is the best way to combat these highly capable threats.

Threat Hunting: Optimize hunt efforts by focusing on the resources likely adversaries tend to target or abuse. Organize around purple team capabilities to develop a deep understanding of offensive and defensive capabilities to better inform threat hunting in your environment. Targeted disruptive attacks frequently involve long dwell times, increasing defenders' opportunities to expel or isolate hackers before they act. For example, the faketivist "Mr. Robot"-themed attacks on Ukrainian financial organizations in December 2016 relied on at least nine months of effort, like escalating privileges and lateral movement, before the hackers disrupted their victims (page 18).

Cyber Wargames and Exercises: Evaluate your ability to respond to plausible threat scenarios involving your most likely, dangerous adversaries. A holistic understanding of adversaries—encompassing technical and nontechnical attributes—is necessary to craft realistic, anticipatory scenarios. Most wargames and exercises should simulate a failure to prevent adversaries from acting on their objectives, thereby testing crisis management, business continuity, and service restoration capabilities. Wargamers might have preemptively modeled destructive cyber attacks on Ukrainian chlorine facilities prior to the VPNFilter incident in 2018, leveraging their awareness of trends in kinetic attacks on chlorine and water treatment facilities in the Eastern Ukraine conflict (page 36).

Information Sharing: Share information with peers, governments, and other companies to increase community awareness of current adversary activity and improve visibility of your threat landscape. Greater threat visibility increases the likelihood that early indications and warnings of future threat activity will become apparent.

Appendix A: Methodology



RESEARCH AND ANALYSIS PROCESS

This report is the culmination of a wide-ranging review and analysis of public sources concerning the GRU and its associated cyber threat activity. We applied our technical understanding, international affairs expertise, and threat intelligence tradecraft to this threat data to reconstitute and evaluate threat events. We followed a few guiding principles in the development of the report:

Public Records: Our research identified 15 years of reporting, analysis, and public statements by security firms and researchers, journalists, academics, politicians, national computer emergency readiness teams (CERT), intelligence agencies, militaries, and victims, as well as raw activity data from public malware and phishing repositories, message boards, and social media.

Nomenclature: We consistently refer to previously attributed GRU-aligned activity groups collectively as “GRU operators” without differentiation. This terminology reflects the reality of the GRU being a singular bureaucratic entity able to draw on multiple mission- and function-focused groups to advance the organization’s mission.

Attribution:

- We limited this report’s scope to activity groups that intelligence communities, law enforcement, and senior lawmakers of the U.S., its allies, and its partners have publicly and repeatedly associated with the GRU.
- This report does not attempt to independently verify historical attribution claims that tie offensive activity to industry threat groups. The threat events discussed herein have been attributed to government-recognized GRU-aligned activity groups tracked under various cybersecurity industry names by analytically reputable organizations.
- This report assumes that the referenced, previously published accounts of attribution of threat activity to consistent industry threat activity groups are sufficiently accurate for the purposes of establishing a framework for analysis. For a complete list of referenced industry threat group names, see Appendix B.

SCOPE

Several activity groups, campaigns, and operations have been attributed to the Russian government by public government, industry, or media sources but are largely excluded because of attribution issues.

Inconclusive Attribution:

The U.S. Government and its allies have rarely linked Russian civilian intelligence agencies to specific operations and associated industry activity groups, limiting our ability to confidently describe the constellation of their actions.

Overly General Attribution:

U.S. agencies and lawmakers occasionally publicly attribute links between certain cyber activities and the Russian government broadly, such as the Triton malware incident at a chemical facility in Saudi Arabia⁴¹⁰ in 2017,⁹⁹ but we excluded such events from our analysis because of a lack of specific organizational sponsorship context necessary for our purposes.

Conflicted and Unreliable Attributions:

Cyber activity where attribution is highly conflicted and effectively reliant on second-hand anonymous claims in media sources, like the damaging of a German steel mill in 2014,⁴¹¹⁻⁴¹⁴ was excluded because of the unreliability of claims and evidence.

Appendix B: Industry Names for GRU-Linked Activity Groups

ACTIVITY GROUPS ASSOCIATED WITH BOTH INFORMATIONAL-TECHNICAL EFFECTS OPERATIONS AND INFORMATIONAL-PSYCHOLOGICAL EFFECTS OPERATIONS

ACTIVITY GROUP	CITED ALIGNMENT	JUSTIFICATION FOR INCLUSION
SOFACTY GROUP	U.S. Department of Justice ⁴¹⁵	The U.S. Department of Justice tracks a cluster of operations that broadly includes activities linked to APT28 and Sandworm Team. ⁴¹⁵

ACTIVITY GROUPS ASSOCIATED WITH INFORMATIONAL-PSYCHOLOGICAL EFFECTS OPERATIONS

ACTIVITY GROUP	CITED ALIGNMENT	JUSTIFICATION FOR INCLUSION
APT28	FireEye ⁴¹⁶ Symantec ⁴¹⁷ Cisco Talos ⁴¹⁸ U.S. Department of Justice ⁴¹⁹	<p>APT28 is an umbrella term used by numerous security firms and governments for a cluster of operations targeting government, diplomatic, military, aerospace, defense, energy, media, political organizations, and dissidents around the globe since at least 2004.⁴²⁰ The group conducts traditional espionage as well as psychological effects operations—including the use of fake “personas” to distribute damaging information—designed to further the Russian government’s strategic interests by swaying public opinion, influencing elections, and controlling media narratives. APT28 operations frequently target the U.S., NATO, and European organizations, including special emphasis on Ukraine, although APT28 operations span the globe. Other targets that dovetail with Russian interests, such as international sporting and investigative bodies, are also routinely targeted.⁴¹⁶</p> <p>In October 2018, the U.S. Department of Justice indicted several GRU officers for their role in APT28 operations.⁴¹⁹ The UK’s National Cyber Security Centre (NCSC) declared that the name APT28 refers to GRU activities.¹⁵³</p>
SOFACTY	Kaspersky Lab ⁴²¹ Palo Alto Networks ⁴²² F-Secure ⁴²³	Kaspersky Lab, Palo Alto Networks, and F-Secure consider Sofacy to be synonymous with APT28 and have tracked the group through its use of what they call its Sofacy (a.k.a. SOURFACE) first-stage malware. ⁴²¹
SEDNIT	ESET ⁴²⁰	ESET considers Sednit to be synonymous with APT28. ESET tracks Sednit through its use of a custom backdoor it calls XAGENT. ⁴²⁰
PAWN STORM	Trend Micro ⁴²⁴	Trend Micro considers Pawn Storm to be synonymous with APT28. ⁴²⁵ Trend Micro tracks the activity cluster through its use of a multistage malware it calls SEDNIT (a.k.a. Sofacy). ⁴²⁴
FANCY BEAR	CrowdStrike ⁴²⁶	CrowdStrike considers Fancy Bear to be synonymous with APT28. ⁴²⁷ CrowdStrike tracks this activity cluster through its use of a malware it calls XAgent.
IRON TWILIGHT	SecureWorks ⁴²⁸	SecureWorks considers Iron Twilight to be synonymous with APT28.
THREAT GROUP 4127 A.K.A. TG-4127	SecureWorks ⁴²⁹	SecureWorks considers Threat Group 4127 to be synonymous with APT28, Sofacy, Sednit, and Pawn Storm. ⁴²⁹

ACTIVITY GROUP	CITED ALIGNMENT	JUSTIFICATION FOR INCLUSION
STRONTIUM	Microsoft ⁴³⁰	Microsoft considers Strontium to be synonymous with APT28. ⁴³⁰
SWALLOWTAIL	Symantec ⁴³¹	Symantec considers Swallowtail to be synonymous with APT28, Fancy Bear, Tsar Team, and Sednit. ⁴³¹
GROUP 74	Talos ⁵¹²	Talos considers Group 74 to be synonymous with Tsar Team, Sofacy, APT28, and Fancy Bear. ⁵¹²
SNAKEMACKEREL	Accenture ⁴³²	Accenture considers SNAKEMACKEREL to be synonymous with APT28, Sofacy, Pawn Storm, Sednit, Fancy Bear, Group 74, Tsar Team, and Strontium. ⁴³²
TSAR TEAM	iSight Partners ⁴³³	iSight Partners, now a component of FireEye, considered Tsar Team to be synonymous with APT28, Pawn Storm, Fancy Bear, and Sednit. ⁴³³
ZEBROCY	Kaspersky Lab ⁴³⁴ Palo Alto Networks ⁴³⁵ ESET ⁴³⁶	Multiple security firms track activity using the Zebrocy malware family as a subgroup or activity-subset within the GRU's broader informational-psychological effects operations entity, known principally as APT28.

ACTIVITY GROUPS ASSOCIATED WITH INFORMATIONAL-PSYCHOLOGICAL EFFECTS OPERATIONS

ACTIVITY GROUP	CITED ALIGNMENT	JUSTIFICATION FOR INCLUSION
SANDWORM TEAM	FireEye ⁴³⁷ F-Secure ⁴³⁸ MITRE ⁴³⁹ Trend Micro ^{440, 441} SentinelOne ⁴⁴² U.S. Department of Justice ⁴¹⁵	<p>Sandworm Team is an umbrella name used by numerous security firms and government entities for technical-effects operations and espionage since at least 2009.^{438, 439} The name refers to a tendency in early operations for malware to include references to the book Dune.</p> <p>The group was historically tracked through its use of several versions of BlackEnergy malware (BlackEnergy, BlackEnergy2, and BlackEnergy3 [BlackEnergy Lite]) and continued to be tracked via derivative malware. Notable activities linked to Sandworm Team include destructive attacks against Ukrainian government and industry, like the disruption of electric grid operations in 2015 and 2016,⁴³⁷ the 2017 NotPetya wiper attack,⁴⁸³ and VPNFilter malware operations disrupted in 2018.⁴¹⁵</p> <p>The U.S. Department of Justice attributes Sandworm Team activities to the broader Sofacy Group.⁴¹⁵ The U.S. Department of Homeland Security (DHS) has also noted that the Sandworm industry name refers to Russian intelligence services activity.⁴⁴⁴ The UK's NCSC found that the name Sandworm refers to GRU activities.¹⁵³</p>
BLACKENERGY APT	Kaspersky Lab ⁴⁴⁵	<p>Kaspersky tracked BlackEnergy APT as a cluster of operations that relied on the BlackEnergy malware from 2008 through 2016. The group used BlackEnergy to conduct distributed denial-of-service (DDoS) attacks and to deploy supervisory control and data acquisition (SCADA)-related plugins to victims in several industrial control systems (ICS) and energy sectors, especially in Ukraine.⁴⁴⁶</p> <p>Kaspersky's BlackEnergy APT cluster contains significant overlap with ESET's BlackEnergy Group/Gang and F-Secure's Quedagh.</p>
BLACKENERGY2 APT	Kaspersky Lab ⁴⁴⁷	<p>Kaspersky Lab tracked a cluster of operations against energy and ICS, as well as governmental and technology organizations from 2013 and 2014.⁴⁴⁷</p> <p>Kaspersky Lab considers its BlackEnergy2 APT cluster to be synonymous with Sandworm Team.⁴⁹²</p>

ACTIVITY GROUP	CITED ALIGNMENT	JUSTIFICATION FOR INCLUSION
BLACKENERGY GROUP/GANG	ESET ⁴⁴⁸	<p>ESET tracked a cluster of operations using several iterations of BlackEnergy malware for targeted attacks in Ukraine and Poland from 2010 through 2016.⁴⁴⁹ The campaigns included both espionage- and ICS-related targets with BlackEnergy, BlackEnergy2, and BlackEnergy Lite (a.k.a. BlackEnergy3). ESET also tracked the actors behind the 2015 Ukraine electricity distribution companies as a part of the BlackEnergy Group/Gang.⁴⁴⁸</p> <p>ESET's BlackEnergy Group/Gang cluster contains significant overlap with Kaspersky's BlackEnergy APT and F-Secure's Quedagh.</p>
QUEDAGH	F-Secure ⁴⁵⁰	<p>F-Secure tracked a cluster of operations using BlackEnergy2 and BlackEnergy3 that targeted political organizations and Ukrainian government organizations in 2010–2014.⁴⁵⁰ F-Secure also suspects Quedagh was involved in the 2008 DDoS attacks against Georgia.</p> <p>F-Secure's Quedagh cluster contains significant overlap with Kaspersky's BlackEnergyAPT and ESET's BlackEnergy Group/Gang.⁴⁵⁰</p>
VOODOO BEAR	CrowdStrike ⁴⁵¹	<p>CrowdStrike tracked Voodoo Bear operations using BlackEnergy2 and BlackEnergy3 that targeted energy, ICS, SCADA, government, and media for espionage and destructive purposes since at least 2011.⁴⁵¹ Voodoo Bear's activities have been particularly focused on entities in Ukraine and include the 2015 Ukrainian energy grid outage operation.</p> <p>CrowdStrike considers Voodoo Bear operations to be equivalent to Sandworm Team and BlackEnergy APT.⁴⁵¹</p>
IRON VIKING	SecureWorks ^{452, 453}	SecureWorks considers Iron Viking to be equivalent to Sandworm Team. ^{452, 453}
TELEBOTS	ESET ⁴⁴⁶	<p>ESET tracks TeleBots as a cluster of operations beginning in 2016 against high-value targets in the Ukrainian financial sector. ESET has linked TeleBots to the Industroyer attack against Ukraine's electric grid in December 2016. ESET also attributes the NotPetya faux ransomware and a series of other Discoder.C ransomware outbreaks in 2017 to TeleBots based on a shared backdoor.⁴⁴³ Based on significant overlap with the group ESET tracks as BlackEnergy Group/Gang, TeleBots is likely an evolution or updated campaign.⁴⁴⁶</p>
ELECTRUM	Dragos ⁴⁵⁵	<p>Dragos tracks Electrum as the adversary group responsible for the Crashoverride (a.k.a. Industroyer) malware that de-energized a transmission substation in Ukraine, resulting in power outages on December 17, 2016.</p>
GREYENERGY	ESET ⁵⁵⁶	<p>ESET began tracking another cluster of operations targeting Ukrainian and Polish energy companies and other high-value targets in December 2015 as GreyEnergy. ESET believes GreyEnergy is a subgroup of TeleBots, whose operations focus on espionage and reconnaissance, including against ICS running SCADA software and servers.⁴⁵⁶</p>
HADES	Kaspersky Lab ⁴⁵⁷ Check Point Research ⁴⁵⁸	<p>The activity cluster tracked as Hades first appeared March 2018 when the group conducted a destructive attack against the organizers, suppliers, and partners of the 2018 Pyeongchang Winter Olympic Games. Hades continued to conduct operations against Ukrainian and European biological and chemical threat prevention organizations and Russian financial institutions.⁴⁵⁸</p> <p>The <i>Washington Post</i> reported in February 2019 that U.S. intelligence authorities believe the actors behind NotPetya were responsible for targeting the 2018 Winter Olympics.⁴⁵⁹</p>

Appendix C: Relevant Tools Used by GRU Operators

The following table contains descriptions of tools referenced in this report, intended to provide technical information beyond that which appears in the report's body. It is not an exhaustive list of tools attributed to GRU operators in public reporting.

TOOL	ALIASES	DESCRIPTION
SEDUPLOADER	JHUHUGIT ⁴⁶⁰ JKEYSKW ⁴⁶⁰ SofacyCarberp ⁴⁶¹ Trojan.Sofacy ⁴⁶² Sednit ⁴⁶³ GAMEFISH ⁴⁶³	A first-stage downloader based on the Carberp banking Trojan. It serves as reconnaissance malware and can download a secondary backdoor such as XAgent. ⁴⁶⁰
SOFACY	SOURFACE ⁴⁶⁴	A first-stage downloader that retrieves a second stage backdoor from a command-and-control server. ⁴⁶⁴
DELPHOCY		A malware family used from 2013 to late-2015 consisting of a Delphi-based backdoor and, sometimes, a bootkit. ⁴⁶⁵ Its code overlapped with BlackEnergy and VPNFilter, which are linked to technical effects operations, but its infrastructure overlapped with psychological effects operations Sofacy campaigns.
ZEBROCY	Zekapab ⁴⁶⁶	A multilanguage family of modular downloaders, droppers, and backdoors deriving from Delphocy. ⁴⁶⁷ Zebrocy is used for reconnaissance, maintaining persistence, and exfiltrating information to command-and-control servers. Observed in the wild since October 2015, Zebrocy immediately dropped elements of the Carberp malware seen in Delphocy and eventually dropped elements of BlackEnergy code. ⁴⁶⁵ Like BlackEnergy, it retained the use of victim-identifying build IDs. Zebrocy infrastructure continued to occasionally overlap with infrastructure linked to psychological effects operations Sofacy campaigns.
XAGENT	Xagent ⁴⁶⁸ CHOPSTICK ⁴⁶⁸ Backdoor.SofacyX ⁴⁶² SPLM ⁴²⁰ webhp ⁴⁶³	A family of modular backdoors with Windows, Linux, and iOS variants. ^{463, 470} The malware, which includes espionage functionalities like keystroke logging and file exfiltration, is typically dropped after a reconnaissance phase as second-stage malware. ⁴²⁰
X-TUNNEL	XTunnel ⁴²⁰ Trojan.Shunnael ⁴⁶² XAP ⁴²⁰	A network proxy tool in use since at least 2013. It creates an encrypted tunnel for transmitting data between infected computers and command-and-control servers. ^{471, 472}
SEDKIT		A custom exploit kit used by APT28 from 2014 through October 2016. Victims were redirected to the exploit kit via watering holes and spearphishing emails. The victims' machines are fingerprinted to ensure the delivery of a suitable exploit, usually Seduploader's dropper. ⁴²⁰
CANNON		A first-stage payload written in C# and Delphi that uses an email-based command-and-control channel. The trojan gathers system information and screenshots then executes a second-stage payload. ⁴⁷²

TOOL	ALIASES	DESCRIPTION
SOFACTY	SEDNIT ⁴⁷⁴	Generic names that refer to a family of malware that are primarily backdoors and information stealers, which capture keystrokes and system information, transmitting collected information to command-and-control servers. ⁴⁷⁴
FYSBIS		A persistent modular Linux operating system (OS) trojan and backdoor that can install itself with or without root privileges. ⁴⁷⁵
CORESHHELL		A first-stage downloader that retrieves a second-stage backdoor from a command-and-control server. Coreshell is an updated version of SOURFACE, with additional antianalysis techniques. ⁴⁷⁶
LOJAX		A UEFI rootkit used to maintain persistent remote access on targeted systems. Lojax is a trojanized version of an older Lojack antitheft-software userland agent. ⁴⁷⁷
GOLD DRAGON		A data-gathering implant that acts as a reconnaissance tool and downloader for subsequent payloads. ⁴⁷⁸
BLACKENERGY	BE	A DDoS botnet builder released in 2007 by a criminal using the handle Cr4sh in DDoS-for-hire campaigns. ^{479, 480} The name “BlackEnergy” without version numbering is frequently used interchangeably with the much more diversely capable derivative BlackEnergy2 and BlackEnergy3 malware.
BLACKENERGY2	BE2	A completely rewritten iteration of BlackEnergy that first appeared in the wild in mid-August 2008. ⁴⁸⁰ The new BlackEnergy2 trojan featured rootkit and process-injection techniques, strong encryption, and, critically, a modular architecture. ⁴⁸⁰ Observed modules reflected BlackEnergy’s dual use as a criminal and state-linked espionage or warfare tool. ⁴³⁸ Criminal modules included a DDoS builder, spam distributor, and a banking credential stealer designed for the Russian and Ukrainian markets. ⁴⁸⁰ Other modules showed little for-profit utility such as ones contained in exploits for specific types of human-machine interface (HMI) applications in ICS networks. ⁴⁸¹ The tool was used in both information technical ⁴⁸² and psychological effects campaigns at least as early as January 2012. ⁴³⁸
BLACKENERGY3	BlackEnergy Lite BE3	An updated, 2014 version of BlackEnergy that lacks a driver and includes a simpler installer component, a greater number of plugins, and antianalysis techniques. ⁴³⁸ This version was not linked to for-profit criminal activity.
GREYENERGY		A modular malware family likely based on BlackEnergy that includes a first-stage backdoor that maps networks, collects passwords, and uses escalate privileges. A second-stage backdoor then uses Tor relays and internal nodes as proxy command and control for stealth. GreyEnergy modules vary and enable data exfiltration and execution of remote processes. ⁴⁸³
GREYENERGY MINI	FELIXROOT ⁴⁸⁴	A first-stage backdoor used to evaluate a compromised computer and gain an initial foothold in the network. ⁴⁸³
CRASHOVERRIDE	Industroyer ⁴⁸⁵	A modular malware designed to disrupt ICS processes in electrical substations. Crashoverride consists of an initial backdoor, loader module, and several supporting and payload modules. ⁴⁸¹ The malware also includes a data wiper and a denial of service (DoS) tool targeted at Siemens SIPROTEC protection relays. ⁴⁸⁵
EXARAMEL		A backdoor used to execute shell commands, launch processes, and exfiltrate data to a command-and-control server. ⁴⁸⁶ This malware is an improved version of the Crashoverride (Industroyer) malware. ⁴⁸⁶

TOOL	ALIASES	DESCRIPTION
VPNFILTER		A multistage modular malware targeting networking equipment that allows for theft of website credentials and monitoring of Modbus supervisory control and data acquisition (SCADA) protocols. The malware can exfiltrate data and conduct man-in-the-middle attacks on traffic passing through infected devices. It also has a destructive capability that can be triggered en masse. VPNFilter has significant code overlap with BlackEnergy. ⁴⁸⁷
KILLDISK		A publicly available data wiping tool used to overwrite files with random data, rendering the files inaccessible and the operating system inoperable. ⁴⁸⁸
MOONRAKER PETYA		An early version of the NotPetya ransomware deployed in December 2016. The worm had limited spreading capabilities but contained code that rendered infected computers unbootable by rewriting registry keys and wiping parts of the system drive. It incorporated code from the original Green Petya crimeware. ⁴⁸³
XDATA	Win32/Filecoder. AESNI.C ⁴⁸⁹	A ransomware distributed via a supply-chain attack against the update server of the Ukrainian software M.E.Doc. ⁴⁹⁰ XData attempts spread laterally by using Mimikatz to extract admin credentials and copy itself to all computers on an internal network. ⁴⁹¹
PETRWAP		A family of ransomware used in targeted attacks that contains a sample of the Petya ransomware, modified with entirely new decryption routine. ⁴⁹²
NOTPETYA	GoldenEye ⁴⁹³ ExPetr ⁴⁹⁴ Nyetya ⁴⁹³ Diskcoder.C ⁴⁸⁹ PetrWrap (new version) ⁴⁹³	A wiper disguised as ransomware designed to destroy data and disk structure on compromised systems. Although NotPetya encrypts data and presents a ransom demand on compromised systems, the malware did not have the ability to decrypt data, rendering it permanently unavailable. NotPetya was delivered through a supply-chain attack through an update server for M.E.Doc. NotPetya included a worm-like feature to propagate across a network using EternalBlue and EternalRomance exploits. ⁴⁹⁵ The malware contains substantial code similarities with the Crashoverride (Industroyer) malware. ⁴⁸⁶
BAD RABBIT		A pseudo-ransomware wiper family consisting of a dropper disguised as an Adobe Flash installer. Bad Rabbit used the EternalRomance exploit to spread within networks. Bad Rabbit's encryption uses a hashing process that uses an algorithm similar to NotPetya. Unlike NotPetya, there are technical means to decrypt the key necessary for disk decryption. ⁴⁹⁶

Appendix D: Relevant GRU Personas

The following table contains descriptions of GRU personas referenced in this report, intended to provide additional information to that which appears in the report's body. It is not an exhaustive list of personas that the GRU has used.

PERSONA	DESCRIPTION
CYBERBERKUT	<p>A hacktivist persona named after the Ukrainian special police forces emerged in March 2014 with a blog and Twitter account.⁴⁹⁷ CyberBerkut conducted DDoS attacks (against NATO, Ukraine, and German government websites) and routinely published stolen documents and communications meant to undermine Ukraine and its allies during the period of conflict surrounding the war in Donbass and the Russian annexation of Crimea.⁴⁹⁸ Sample blog posts include the following:⁴⁹⁹</p> <ul style="list-style-type: none"> • The U.S. is testing biological experiments in Ukraine (October 1, 2018) • Ukraine sponsored Hillary Clinton using IMF loans (July 12, 2017) • The U.S. manufactured false evidence of Russian involvement in hacking the 2016 U.S. presidential election (January 13, 2017). • The U.S. is hiding the fact that Kyiv violated the Minsk agreement in Ukraine (June 4, 2015). <p>In 2017, the U.S. Defense Intelligence Agency characterized CyberBerkut as a “front organization for Russian state-sponsored cyber activity, supporting Russia’s strategic objectives in Ukraine.”⁵⁰⁰</p>
ANONYMOUS POLAND (@ANPOLAND)	<p>A Twitter persona created in 2012 modeled after the Anonymous hacktivist collective, likely used to conduct disinformation campaigns in furtherance of Russian interests. The persona was likely used in several separate propaganda campaigns:</p> <ul style="list-style-type: none"> • The group leaked data stolen from the World Anti-Doping Agency (WADA) and Court of Arbitration for Sport following the release of a WADA report recommending a ban on Russian athletes from the 2016 Olympics.⁵⁰¹ • The group leaked dozens of gigabytes of files from a conservative Wisconsin-based think tank, including a fake check for \$156 million to Hillary Clinton, in the lead up to the 2016 U.S. presidential election.⁵⁰² • In 2017, Anonymous Poland released fake information about Bellingcat, an open-source research group investigating the downing of MH17 in Ukraine.⁵⁰³ <p>The account’s tweets were often amplified by bots, possibly purchased on the black market and previously used for illicit marketing campaigns.⁵⁰⁴ The Anonymous Poland account frequently reached out directly to journalists to publicize its activities.⁵⁰⁵</p>
CYBERCALIPHATE	<p>A hacktivist persona purporting to be operated by Islamic extremist hackers from the Islamic State. Social media accounts associated with CyberCaliphate—including Facebook, Twitter, and YouTube accounts—spread disinformation along with jihadist propaganda messages. The persona took credit for the GRU’s destructive attack against TV5Monde and released personal information of individuals allegedly serving in the French military.¹⁵⁴</p> <p>The UK’s National Cyber Security Centre (NCSC) stated that the name CyberCaliphate refers to GRU activities.¹⁵³</p>
GUCCIFER 2.0	<p>A persona used to spread communications and files stolen from the Democratic National Committee in the lead up to the 2016 U.S. presidential election. Purporting to be an independent Romanian hacker, Guccifer 2.0 reached out to journalists, media organizations, and ultimately, WikiLeaks to distribute the stolen files with maximum effect.</p> <p>Guccifer 2.0 was specifically named as a propaganda account in the Justice Department’s 2018 indictment against 12 Russian intelligence agents.⁵⁰⁶</p>

PERSONA	DESCRIPTION
DCLEAKS	<p>A persona used in conjunction with Guccifer 2.0 as a part of the propaganda campaign to influence the 2016 U.S. presidential election.⁵⁰⁶ The persona's Twitter account announced the release of emails stolen from the DNC, the Open Society Foundation, and others, and posted on the DCLeaks website.⁵⁰⁷</p> <p>DCLeaks was specifically named as a propaganda account in the Justice Department's 2018 indictment against 12 Russian intelligence agents.⁵⁰⁶</p>
FANCY BEARS' HACK TEAM	<p>A pro-Russian hacktivist persona created to leak documents, medical records, and communications stolen in a campaign to undermine antidoping organizations, officials, and athletes. The campaign was likely launched after the exposure of Russia's state-sponsored doping campaign in 2015.⁵⁰⁸ The U.S. Department of Justice alleges that the GRU established and maintained the Fancy Bears' Hack Team persona.⁵⁰⁹</p>
PRAVY SEKTOR'S ELECTRONIC RED-AND-BLACK BATTALION	<p>A hacktivist persona purportedly representing the far-right Ukrainian nationalist party Pravy Sektor, part of a disinformation campaign aimed at undermining confidence in Ukrainian elections. The persona claimed responsibility for GRU-attributed disruptive and destructive attacks against media and elections infrastructure in Ukraine.⁵¹⁰</p>

Endnotes

Note: All cited URLs have been changed to hxxp or hxxps as we cannot guarantee the safety of the sites.

1. Paul Nakasone, "Advance Policy Questions for Lieutenant General Paul Nakasone, USA Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service," U.S. Senate Armed Services Committee, March 1, 2018, accessed August 2, 2019, hxxps://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf.
2. "Putin on cyberwarfare: Action causes reaction, you don't like reaction—let's talk rules," RT, last modified May 25, 2018, accessed August 11, 2019, hxxps://www.rt.com/news/427709-putin-cybersecurity-rules-reaction/
3. "What is the GRU? Who gets recruited to be a spy? Why are they exposed so often? Here are the most important things you should know about Russia's intelligence community," Meduza, November 6, 2018, accessed hxxps://meduza.io/en/feature/2018/11/06/what-is-the-gru-who-gets-recruited-to-be-a-spy-why-are-they-exposed-so-often.
4. "The Military Doctrine of the Russian Federation," Approved by the President of the Russian Federation on December 25, 2014, The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, June 29, 2015, accessed November 18, 2019, hxxps://rusemb.org.uk/press/2029.
5. Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action," Carnegie Endowment for International Peace, June 5, 2019, accessed November 14, 2019, hxxps://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.
6. Кирюшин А.Н., "Информационное противоборство: проблема терминологической недостаточности," Вы здесь, March 18, 2013, accessed September 13, 2019, hxxp://www.catu.su/analytics/439-informacionnoe-protivoborstvo-problema-terminologicheskoy-nedostatochnost;
7. "Russia Military Power, Defense Intelligence Agency Report DIA-11-1704-161, 2017, accessed September 13, 2019, hxxps://www.dia.mil/portals/27/documents/news/military%20power%20publications/russia%20military%20power%20report%202017.pdf
8. Ekaterina Kalina, "Narratives of Russia's 'Information Wars,'" DE Gruyter, Politics in Central Europe, Vol. 12, No. 1, 2016, accessed September 13, 2019, hxxps://content.sciendo.com/downloadpdf/journals/pce/12/1/article-p147.xml.
9. Samuel Layton, "Reframing European security: Russia's proposal for a new European security architecture," Sage Journals, January 15, 2014, accessed August 5, 2019, hxxps://journals.sagepub.com/stoken/rbtf/YcxyKBznoiENc/full.
10. The Foreign Policy Concept of the Russian Federation, the Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, November 30, 2016, accessed August 2, 2019, hxxps://www.rusemb.org.uk/rp_insight/.
11. Excerpts From Foreign Minister Sergey Lavrov's Meeting with Students and Faculty at the Azerbaijan Diplomatic Academy, Permanent Mission of the Russian Federation to NATO, November 20, 2017, accessed August 5, 2019, hxxps://missionto-nato.mid.ru/web/nato-en/-/excerpts-from-foreign-minister-sergey-lavrov-s-answers-at-the-meeting-with-students-and-faculty-of-the-azerbaijan-diplomatic-academy-baku-november-20-?inheritRedirect=true.
12. Sergey Lavrov, "The Euro-Atlantic Region: Equal Security for All," Russia in Global Affairs, July 7, 2010, accessed November 18, 2019, hxxps://eng.globalaffairs.ru/number/The_Euro-Atlantic_Region:_Equal_Security_for_All-14888.
13. Benn Steil, "Russia's Clash with the West Is About Geography, Not Ideology," Foreign Policy, February 12, 2018, accessed August 2, 2019, hxxps://foreignpolicy.com/2018/02/12/russias-clash-with-the-west-is-about-geography-not-ideology/.
14. Grzegorz Kuczynski, "NATO-Russia Relations: The Return of the Enemy," Warsaw Institute, April 4, 2019, accessed August 2, 2019, hxxps://warsawinstitute.org/nato-russia-relations-return-enemy/.
15. Vesko Garcevic, "Serbia Is Sealing Its Position as Russia's Best Friend," Balkan Insight, April 3, 2018, accessed August 7, 2019, hxxps://balkaninsight.com/2018/04/03/serbia-is-sealing-its-position-as-russia-s-best-friend-04-02-2018/.

16. Dusica Tomovic, "Montenegro Seeks to Lure More Russian Tourists," *Balkan Insight*, March 16, 2018, accessed August 7, 2019, <https://balkaninsight.com/2018/03/16/montenegro-eyes-more-russian-tourists-in-2018-03-15-2018/>.
17. Podgorica, "Investigation Uncovers Second Russian Montenegro Coup Suspect," *Balkan Insight*, November 22, 2018, accessed August 7, 2019, <https://balkaninsight.com/2018/11/22/media-investigation-identifies-montenegro-coup-suspect-11-22-2018/>
18. Ben Farmer, "Russia plotted to overthrow Montenegro's government by assassinating Prime Minister Milo Djukanovic last year, according to senior Whitehall sources," *The Telegraph*, February 19, 2017, accessed August 7, 2019, <https://www.telegraph.co.uk/news/2017/02/18/russias-deadly-plot-overthrow-montenegros-government-assassinating/>
19. Andrew Higgins, "Finger Pointed at Russians in Alleged Coup Plot in Montenegro," *The New York Times*, November 26, 2016, accessed August 7, 2019, <https://www.nytimes.com/2016/11/26/world/europe/finger-pointed-at-russians-in-alleged-coup-plot-in-montenegro.html>.
20. Dusica Tomovic, "Montenegro on Alert Over Rise in Cyber Attacks," *Balkan Insight*, January 10, 2017, accessed August 7, 2019, <https://balkaninsight.com/2017/01/10/montenegro-on-alert-over-cyber-attacks-01-09-2017/>.
21. Georgi Gotev, "Montenegro hit by cyber-attacks on election day," *Euractiv*, October 17, 2016, accessed August 7, 2019, <https://www.euractiv.com/section/global-europe/news/montenegro-hit-by-cyber-attacks-on-election-day/>.
22. "Government of Montenegro's web portal exposed to DDoS attacks," Government of Montenegro, October 19, 2016, accessed August 7, 2019, <https://web.archive.org/web/20161106103505/http://cherna.gora.me/government/government-of-montenegros-web-portal-exposed-to-ddos-attacks/>.
23. "Kremlin rejects claims Russia had role in Montenegro coup plot," *The Guardian*, February 20, 2017, accessed August 7, 2019, <https://www.theguardian.com/world/2017/feb/20/russian-state-bodies-attempted-a-coup-in-montenegro-says-prosecutor>.
24. Chris Bing, "Russia-linked hackers impersonate NATO in attempt to hack Romanian government," *CyberScoop*, May 11, 2017, accessed August 7, 2019, <https://www.cyberscoop.com/dnc-hackers-impersonated-nato-attempt-hack-romanian-government/>.
25. "Брифинг официального представителя МИД России М.В.Захаровой, Москва, 7 марта 2019 года," Ministry of Foreign Affairs of the Russian Federation, March 7, 2019, accessed November 18, 2019, http://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3562173.
26. "The Foreign Policy Concept of the Russian Federation," The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, November 30, 2016, accessed November 18, 2019, https://www.rusemb.org.uk/rp_insight/.
27. Martha Raddatz et al., "Airstrikes 'Successful' Against ISIS Targets in Syria, U.S. Military Says," *ABC News*, September 23, 2014, accessed August 8, 2019, <https://abcnews.go.com/International/us-airstrikes-syria/story?id=25686031>.
28. Summary of Sergey V. Lavrov's speech to the UN General Assembly, General Assembly of the United Nations, September 27, 2014, accessed August 8, 2019, <https://www.un.org/en/ga/69/meetings/gadebate/27sep/russianfederation.shtml>.
29. Tyler White, "Cyber Caliphate, group claiming ISIS affiliation, hacks U.S. news outlets' Twitter accounts," *My San Antonio*, January 6, 2015, accessed August 7, 2019, <https://www.mysanantonio.com/news/us-world/article/Group-claiming-ISIS-affiliation-hacks-news-5996952.php#photo-7353478>
30. David Mikkelson, "Did Denzel Washington Make a Large Donation to the Fisher House?," *Snopes*, February 10 2005, accessed August 7, 2019, <https://www.snopes.com/fact-check/denzel-washington-2/>.
31. Alba, Alejandro, "FBI investigates ISIS hacker group Cyber Caliphate following series of hacks on news organizations in Maryland, Albuquerque," *New York Daily News*, January 6, 2015, accessed August 7, 2019, <http://www.nydailynews.com/news/national/isis-hacker-group-cyber-caliphate-hacks-article-1.2067634>.
32. Brian Fung & Andrea Peterson, "The Centcom 'hack' that wasn't," *The Washington Post*, January 12, 2015, accessed August 7, 2019, https://www.washingtonpost.com/news/the-switch/wp/2015/01/12/the-centcom-hack-that-wasnt/?utm_term=.b13493e904d6.
33. "WBOC Victim of Another Cyber Attack," *WBOC 16*, February 10, 2015, accessed September 13, 2019, <http://www.wboc.com/story/28070058/wboc-text-alerts-cyberattacked>.

34. Simon Shuster, "Russia is Testing NATO's Resolve in Eastern Europe," *Time*, September 6, 2014, accessed November 18, 2019, <https://time.com/3281844/russia-ukraine-nato/>.
35. Alexey Ermenko, "Sites Named for New NATO Bases in Eastern Europe," *The Moscow Times*, September 1, 2014, accessed November 18, 2019, <https://www.themoscowtimes.com/2014/09/01/sites-named-for-new-nato-bases-in-eastern-europe-a38903>.
36. Reuters, "Russian Defense Minister: NATO Bases Too Close to Our Borders," *The Moscow Times*, July 11, 2018, accessed November 18, 2019, <https://www.themoscowtimes.com/2018/07/11/russian-defense-minister-nato-too-close-to-our-borders-a62205>.
37. Piotr Buras & Adam Balcer, "An unpredictable Russia: the impact on Poland," European Council on Foreign Relations, July 15, 2016, accessed August 5, 2019, https://www.ecfr.eu/article/commentary_an_unpredictable_russia_the_impact_on_poland.
38. Дмитрий Болтенков, "Польские комплексы," *iz*, February 15, 2019, accessed August 5, 2019, <https://iz.ru/845296/dmitrii-boltenkov/polskie-kompleksy>.
39. "NATO to consider the increasing of military personnel and equipment in Poland," *Army Recognition*, July 25, 2014, accessed August 6, 2019, https://www.armyrecognition.com/july_2014_global_defense_security_news_uk/nato_to_consider_the_increasing_of_military_personnel_and_equipment_in_poland_2507146.html.
40. Loucif Kharouni et al., "Operation Pawn Storm," *Trend Micro*, January 16, 2016, accessed August 5, 2019, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf>.
41. Raport 2014, Cert Polska, 2014, accessed August 5, 2019, https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2014.pdf.
42. "Operation Pawn Storm," *Trend Micro*, January 16, 2016, accessed August 5, 2019, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf>.
43. Jane Dalton, "Poland asks Trump to establish military base on Russian border to deter Moscow," *The Independent*, June 1, 2018, accessed August 5, 2019, <https://www.independent.co.uk/news/world/europe/us-russia-trump-military-base-poland-moscow-soldiers-defence-europe-a8378161.html>.
44. Radina Glgova, "Massive NATO exercise starts in Poland and the Baltics," *CNN*, June 4, 2018, accessed August 6, 2019, <https://www.cnn.com/2018/06/03/world/nato-exercise-poland-baltics-russia/index.html>.
45. Mariusz, "GreyEnergy w Polsce," *malware@prevenity*, October 22, 2018, accessed August 6, 2019, <https://malware.prevenity.com/2018/10/greyenergy-w-polsce.html>.
46. "Посол России Михаил Бабич в большом интервью 'Главному эфиру,'" *TVR*, October 21, 2018, accessed August 7, 2019, https://www.tvr.by/news/glavnyy-efir/posol_rossiyskoy_federatsii_mikhail_babich_v_bolshom_intervyu_glavnomu_efiru/.
47. Paul Goble, "Minsk Resisting Moscow's Latest Scheme to Acquire Military Base in Belarus," *Eurasia Daily Monitor*, The Jamestown Foundation, Volume 15 Issue 154, October 30, 2018, accessed August 7, 2019, <https://jamestown.org/program/minsk-resisting-moscows-latest-scheme-to-acquire-military-base-in-belarus/>.
48. "Belarus says Russia made oil threat, calls border plan a political attack," *Reuters*, February 3, 2017, accessed August 6, 2019, <https://www.reuters.com/article/us-russia-belarus-border-idUSKBN1511K8>.
49. Gabriella Gricius, "Belarus: The State in the Middle," *Global Security Review*, March 15, 2019, accessed August 6, 2019, <https://globalsecurityreview.com/belarus-state-in-the-middle/>.
50. Robbie Gramer & Amy Mackinnon, "A Diplomatic Breakthrough for Washington in Europe's Last Dictatorship," *Foreign Policy*, January 10, 2019, accessed August 6, 2019, <https://foreignpolicy.com/2019/01/10/diplomatic-breakthrough-for-washington-in-europes-last-dictatorship-belarus-warming-relations-with-west-united-states-lukashenko-putin-russia-dispute-diplomacy-state-department-eastern-europe/>.
51. Paul Goble, "Moscow's 'Article Five' Guarantee to Belarus; First Step Toward Permanent Russian Base?" *Eurasia Daily Monitor*, The Jamestown Foundation, Volume 15, Issue 150, October 23, 2018, accessed August 7, 2019, <https://jamestown.org/program/moscows-article-five-guarantee-to-belarus-first-step-toward-permanent-russian-base/>.

52. "297819bf06e4f7dda0de1b3c52bb59ede282aba04fe68935d8c3d065dcadab8a," VirusTotal, last updated November 28, 2018, accessed August 6, 2019, <https://www.virustotal.com/gui/file/297819bf06e4f7dda0de1b3c52bb59ede282aba04fe68935d8c3d065dcadab8a/content/strings>.
53. Vladimir Socor, "Pillar of NATO: Romania's Ambition in the Black Sea Region," *Eurasia Daily Monitor*, The Jamestown Foundation, August 7, 2018, accessed August 7, 2019, <https://jamestown.org/program/pillar-of-nato-romanas-ambition-in-the-black-sea-region/>
54. Kremlin Watch Team, "Kremlin Influence in Visegrad Countries and Romania: Overview of the Threat, Existing Countermeasures, and Recommended Next Steps," Kremlin Watch Memo, European Values, October 23, 2017, accessed August 7, 2019, <https://www.europeanvalues.net/wp-content/uploads/2017/12/Kremlin-Influence-in-Visegrad-Countries-and-Romania.pdf>.
55. "In Moldova, voters choose between Russia and Europe," Euractiv, February 22, 2019, accessed August 7, 2019, <https://www.euractiv.com/section/europe-s-east/news/in-moldova-voters-choose-between-russia-and-europe/>.
56. Mihai Popsoi, "Moldova Hopes to Boost Military Ties with Romania Amid Tensions with Russia," *Eurasia Daily Monitor*, the Jamestown Foundation, February 21, 2018, accessed August 7, 2019, <https://jamestown.org/program/moldova-hopes-boost-military-ties-romania-amid-tensions-russia/>.
57. ClearSky CyberSecurity (@clearskysec), Twitter, February 6, 2018, accessed August 7, 2019, <https://twitter.com/ClearskySec/status/960924755355369472>.
58. Kremlin Watch Team, "Kremlin Influence in Visegrad Countries and Romania: Overview of the Threat, Existing Countermeasures, and Recommended Next Steps," Kremlin Watch Memo, European Values, October 23, 2017, accessed August 7, 2019, <https://www.europeanvalues.net/wp-content/uploads/2017/12/Kremlin-Influence-in-Visegrad-Countries-and-Romania.pdf>.
59. Jaroslaw Adamowski, "Romania to buy 3 sub, 4 ships to bolster Black Sea ops," Defense News, February 9, 2018, accessed August 7, 2019, <https://www.defensenews.com/naval/2018/02/09/romania-to-buy-3-sub-4-ships-to-bolster-black-sea-ops/>.
60. Micahael Petersen, "The Naval Power Shift in the Black Sea," War on the Rocks, January 9, 2019, accessed August 7, 2019, <https://warontherocks.com/2019/01/the-naval-power-shift-in-the-black-sea/>.
61. Robert Falcone, "Sofacy Uses DealersChoice to Target European Government Agency," PaloAlto Networks, March 15, 2018, accessed September 27, 2019, <https://unit42.paloaltonetworks.com/unit42-sofacy-uses-dealerschoice-target-european-government-agency/>
62. "e5511b22245e26a003923ba476d7c36029939b2d1936e17a9b35b396467179ae%250Aefb235776851502672dba5ef45d96cc65cb9ebba1b49949393a6a85b9c822f52%250Ac4be15f9ccfecf7a463f3b1d4a17e7b4f95de939e057662c3f97b52f7fa3c52f," VirusTotal, last updated May 15, 2018, accessed August 7, 2019, <https://www.virustotal.com/gui/search/e5511b22245e26a003923ba476d7c36029939b2d1936e17a9b35b396467179ae%250Aefb235776851502672dba5ef45d96cc65cb9ebba1b49949393a6a85b9c822f52%250Ac4be15f9ccfecf7a463f3b1d4a17e7b4f95de939e057662c3f97b52f7fa3c52f/files>.
63. Vladimir Dvorkin, "Preserving Strategic Stability Amid U.S.-Russian Confrontation," Carnegie Moscow Center, February 8, 2019, accessed November 11, 2019, <https://carnegie.ru/2019/02/08/preserving-strategic-stability-amid-u.s.-russian-confrontation-pub-78319>.
64. "Russia threatens to aim nuclear missiles at Denmark ships if it joins NATO shield," Reuters, March 22, 2015, accessed August 6, 2019, <https://www.reuters.com/article/us-denmark-russia/russia-threatens-to-aim-nuclear-missiles-at-denmark-ships-if-it-joins-nato-shield-idUSKBN0MI0ML20150322>.
65. Lars From, "Ruslands ambassadør: Danske skibe kan blive mål for russisk atomangreb," *Indland*, March 20, 2015, accessed August 6, 2019, <https://jyllands-posten.dk/indland/ECE7573125/Ruslands-ambassad%C3%B8r-Danske-skibe-kan-blive-m%C3%A5l-for-russisk-atomangreb/>.
66. Undersøgelsesrapport, Center for Cybersikkerhed, April 2017, accessed August 6, 2019, <https://fe-ddis.dk/cfcs/CFCSDocuments/Unders%C3%B8gelsesrapport%20-%20En%20akt%C3%B8r%20mange%20angreb.pdf>.
67. Gordon B. Smith, "Russian Exceptionalism? Putin's Assertion of Sovereignty at Home and Abroad," (paper presented at the Conference on Sovereignty and the New Executive Authority at the Center for Ethics and the Rule of Law at the University of Pennsylvania Law School, April 20, 2013), accessed November 11, 2019, available at <https://www.law.upenn.edu/live/files/1882-gordon-smith-russian-exceptionalism.pdf>.

68. "Interview to American TV channel CBS and PBS," President of Russia, September 29, 2015, accessed November 17, 2019, [hxxp://en.kremlin.ru/events/president/news/50380](http://en.kremlin.ru/events/president/news/50380).
69. Efrem Lukatsky & Yuras Karmanau, "Right-wing Radical Party to leave Ukrainian parliamentary coalition," Associated Press, September 1, 2015, accessed September 13, 2019, [hxxps://www.theglobeandmail.com/news/world/over-140-still-hospitalized-after-nationalist-protests-turn-violent-in-ukraine/article26172500/](https://www.theglobeandmail.com/news/world/over-140-still-hospitalized-after-nationalist-protests-turn-violent-in-ukraine/article26172500/).
70. "Russia Calling! Investment Forum," President of Russia, October 13, 2015, accessed November 18, 2019, [hxxp://en.kremlin.ru/events/president/news/50498](http://en.kremlin.ru/events/president/news/50498).
71. "Местные выборы на оккупированных территориях можно будет проводить только после создания соответствующих условий - Порошенко," Interfax, September 13, 2015, accessed September 13, 2019, [hxxps://interfax.com.ua/news/general/289853.html](http://interfax.com.ua/news/general/289853.html).
72. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017, accessed August 2, 2019, [hxxps://www.wired.com/story/russian-hackers-attack-ukraine/](https://www.wired.com/story/russian-hackers-attack-ukraine/).
73. Kurt Baumbgartner & Maria Garnaeva, "BE2 custom plugins, router abuse, and target profiles," Kaspersky SecureList, November 3, 2014, accessed August 2, 2019, [hxxps://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/](https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/).
74. Andrey Nikishin, "ICS Threats. A Kaspersky Lab view, predictions, and reality," RSA Conference 2016, accessed August 2, 2019, [hxxps://www.rsaconference.com/writable/presentations/file_upload/sbx1-w09-industrial-cyberthreats-the-kaspersky-lab-view.pdf](https://www.rsaconference.com/writable/presentations/file_upload/sbx1-w09-industrial-cyberthreats-the-kaspersky-lab-view.pdf).
75. "Українські ЗМІ атакують за допомогою Black Energy," CERT-UA, September 11, 2015, accessed August 2, 2019, [hxxps://web.archive.org/web/20160326061731/hxxps://cert.gov.ua/?p=2370](https://web.archive.org/web/20160326061731/hxxps://cert.gov.ua/?p=2370).
76. "ICTV удалил видеоархив за три месяца из-за взлома сервера," LB, October 25, 2015, accessed August 2, 2019, [hxxps://lb.ua/news/2015/10/25/319227_ictv_udalil_videoarhiv_tri_mesyatsa.html](https://lb.ua/news/2015/10/25/319227_ictv_udalil_videoarhiv_tri_mesyatsa.html).
77. "Хакеры взломали все сайты медиagruppy «Интер»," Golos Pravdy, October 25, 2015, accessed August 2, 2019, [hxxps://golospravdy.eu/xakery-vzlomali-vse-sajty-mediagruppy-inter/](https://golospravdy.eu/xakery-vzlomali-vse-sajty-mediagruppy-inter/).
78. "Russian Nuclear Doctrine," Global Security, accessed November 18, 2019, [hxxps://www.globalsecurity.org/wmd/world/russia/doctrine.htm](https://www.globalsecurity.org/wmd/world/russia/doctrine.htm).
79. Nikolai Sokov, "Russian's White Paper on WMD Nonproliferation," Middlebury Institute of International Studies at Monterey, July 25, 2006, accessed November 18, 2019, [hxxps://www.nonproliferation.org/russians-white-paper-on-weapons-of-mass-destruction-nonproliferation/](https://www.nonproliferation.org/russians-white-paper-on-weapons-of-mass-destruction-nonproliferation/).
80. Anya Loukianova Fink, "The Evolving Russian Concept of Strategic Deterrence: Risks and Responses," The Arms Control Association, July/August 2017, accessed November 18, 2019, [hxxps://www.armscontrol.org/act/2017-07/features/evolving-russian-concept-strategic-deterrence-risks-responses#endnote31](https://www.armscontrol.org/act/2017-07/features/evolving-russian-concept-strategic-deterrence-risks-responses#endnote31).
81. Keith Darden, "Keeping the 'New Cold War' Cold: Nuclear Deterrence with U.S. and Russian Nuclear Force Modernization," Policy Memo 530, PONARS Eurasia, May 2018, [hxxp://www.ponarseurasia.org/memo/keeping-new-cold-war-cold-nuclear-deterrence-us-and-russian-force-modernization](http://www.ponarseurasia.org/memo/keeping-new-cold-war-cold-nuclear-deterrence-us-and-russian-force-modernization).
82. "Andrew Osborn, "For Putin, economic and political reality dampen appetite for arms race," Reuters, February 7, 2019, accessed November 18, 2019, [hxxps://www.reuters.com/article/us-usa-nuclear-russia-armsrace-analysis/for-putin-economic-and-political-reality-dampen-any-appetite-for-arms-race-idUSKCN1PW1U8](https://www.reuters.com/article/us-usa-nuclear-russia-armsrace-analysis/for-putin-economic-and-political-reality-dampen-any-appetite-for-arms-race-idUSKCN1PW1U8).
83. Heather Williams, "Russia Still Needs Arms Control," Arms Control Association, January/February 2016, accessed November 18, 2019, [hxxps://www.armscontrol.org/act/2016-01/features/russia-still-needs-arms-control](https://www.armscontrol.org/act/2016-01/features/russia-still-needs-arms-control).
84. Anne Gearan et al., "U.S. to withdraw from nuclear arms control treaty with Russia, raising fears of a new arms race," *The Washington Post*, February 1, 2019, accessed November 18, 2019, [hxxps://www.washingtonpost.com/world/national-security/us-to-withdraw-from-nuclear-arms-control-treaty-with-russia-says-russian-violations-render-the-cold-war-agreement-moot/2019/02/01/84dc0db6-261f-11e9-ad53-824486280311_story.html](https://www.washingtonpost.com/world/national-security/us-to-withdraw-from-nuclear-arms-control-treaty-with-russia-says-russian-violations-render-the-cold-war-agreement-moot/2019/02/01/84dc0db6-261f-11e9-ad53-824486280311_story.html).

85. Ilya Arkhipov, "Putin Warns U.S. of New Arms Race After Nuclear Deal's Collapse," Bloomberg, August 5, 2019, accessed November 18, 2019, <https://www.bloomberg.com/news/articles/2019-08-05/putin-warns-u-s-of-new-arms-race-after-nuclear-deal-collapses>.
86. The Constitution of the Russian Federation, accessed November 18, 2019, <http://www.constitution.ru/en/10003000-02.htm>.
87. "Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016)," The Ministry of Foreign Affairs of the Russian Federation, December 1, 2016, accessed November 18, 2019, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptlCk6BZ29/content/id/2542248.
88. Andrew Radin & Clint Reach, "Russian Views of the International Order," RAND, 2017, accessed November 18, 2019, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1826/RAND_RR1826.pdf.
89. Shaun Walker, "Putin condemns western hypocrisy as he confirms annexation of Crimea," *The Guardian*, March 18, 2014, accessed November 18, 2019, <https://www.theguardian.com/world/2014/mar/18/crimea-putin-condemns-western-hypocrisy-annexation>.
90. Nataliya Vasilyeva, "Ukraine won't repay \$3 billion Russian debt due this weekend," AP, December 18, 2015, accessed August 2, 2019, <https://web.archive.org/web/20160311162705/http://bigstory.ap.org/article/3266e1c4ee134eebacb-860fb07b1ad06/ukraine-says-it-wont-repay-russian-debt-due-weekend>.
91. Reuters, "Ukraine is on Track to Default on its Russian Debt," Fortune, December 18, 2015, accessed November 8, 2019, <https://fortune.com/2015/12/18/ukraine-default-russian-debt/>.
92. "IMF Approves \$1 Billion Loan for Ukraine After One-Year Delay," RadioFreeEurope Radio Liberty, September 15, 2016, accessed November 18, 2019, <https://www.rferl.org/a/imf-approves-1-billion-dollar-loan-ukraine-after-one-year-delay-corruption-concerns/27989129.html>
93. "Ukraine to issue Eurobonds; Russia will purchase \$15 bln, says Russian finance minister," Interfax, December 17, 2013, accessed November 18, 2019, <https://en.interfax.com.ua/news/economic/182491.html>.
94. Natalia Valisyeva, "Ukraine won't repay \$3 billion Russian debt due this weekend," AP News, December 18, 2015, accessed November 18, 2019, <https://web.archive.org/web/20160311162705/http://bigstory.ap.org/article/3266e1c4ee134eebacb-860fb07b1ad06/ukraine-says-it-wont-repay-russian-debt-due-weekend>.
95. "Hacktivist Group CyberBerkut Behind Attacks on German Official Websites," Trend Micro Security Intelligence Blog, January 20, 2015, accessed August 6, 2019, <https://blog.trendmicro.com/trendlabs-security-intelligence/hacktivist-group-cyberberkut-behind-attacks-on-german-official-websites/>.
96. CyberBerkut, "Ukrainian Ministry of Information Policy consists of ordinary fascists," March 19, 2015, accessed November 18, 2019, <https://cyber-berkut.org/en/olden/index1.php>.
97. Anders Aslund, "The IMF Outfoxes Putin: Policy Change Means Ukraine Can Receive More Loans," Atlantic Council, December 8, 2015, accessed August 7, 2019, <https://www.atlanticcouncil.org/blogs/ukrainealert/the-imf-outfoxes-putin-policy-change-means-ukraine-can-receive-more-loans>.
98. "IMF Changes Rule on Debt for Ukraine, as Russia Complains," Radio Free Europe, December 9, 2015, accessed November 18, 2019, <https://www.rferl.org/a/imf-changes-rule-debt-for-ukraine-russia-complains/27415398.html>
99. Chairman Lisa Murkowski, "Opening Statement for the Full Committee Hearing on Cybersecurity Efforts in the Energy Industry," United States Senate Committee on Energy and Natural Resources, February 14, 2019, accessed August 2, 2019, https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=F4C51F03-BC7B-4076-A214-8908F7EA8195.
100. "Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины," Centrum, January 6, 2016, accessed August 2, 2019, https://cys-centrum.com/ru/news/black_energy_2_3.
101. Jake Styczynski & Nate Beach-Westmoreland, "When the Lights Went Out," Booz Allen Hamilton, November 3, 2016, <http://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>.
102. Larry Elliott, "IMF warns Ukraine it will halt \$40bn bailout unless corruption stops," *The Guardian*, February 10, 2016, accessed November 18, 2019, <https://www.theguardian.com/world/2016/feb/10/imf-warns-ukraine-halt-40bn-bailout-corruption-christine-lagarde>.

103. Darya Korsunskaya, "Russia says to oppose new IMF aid tranche to Ukraine," Reuters, September 12, 2016, accessed August 2, 2019, <https://www.reuters.com/article/us-ukraine-crisis-russia-eurobond/russia-says-to-oppose-new-imf-aid-tranche-to-ukraine-idUSKCN111A1>.
104. "IMF Approves \$1 Billion Loan for Ukraine After One-Year Delay," RadioFreeEurope Radio Liberty, September 15, 2016, accessed November 18, 2019, <https://www.rferl.org/a/imf-approves-1-billion-dollar-loan-ukraine-after-one-year-delay-corruption-concerns/27989129.html>.
105. "Декабрь. Атаки на финансовую систему страны. fS0cie7y.," Cys-Centrum, December 12, 2016, accessed August 2, 2019, https://cys-centrum.com/ru/news/december_financial_system_of_ukraine_was_attacked.
106. Joe Slowik, "VB2018 paper; Anatomy of an attack: detecting and defeating CRASHOVERRIDE," Virus Bulletin, March 2019, accessed November 18, 2019, <https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/>
107. Anton Cherepanov, "WIN32/INDUSTROYER," ESET We Live Security, June 12, 2017, accessed November 18, 2019, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
108. Stillgherrian, "Blaming Russia for NotPetya was coordinated diplomatic action," ZDNet, April 12, 2018, accessed August 2, 2019, <https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/>.
109. Alert (TA17-181A): Petya Ransomware, U.S. Department of Homeland Security, July 1, 2017, accessed August 2, 2019, <https://www.us-cert.gov/ncas/alerts/TA17-181A>
110. John Miller et al., "Petya Destructive Malware Variant Spreading via Stolen Credentials and EternalBlue Exploit," FireEye, June 27, 2017, accessed August 2, 2019, <https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html>.
111. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, accessed August 2, 2019, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
112. "КІБЕРАТАКИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ. ХРОНОЛОГІЯ," Ministry of Defense of Ukraine, May 7, 2018, accessed August 2, 2019, <https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html>.
113. Сергей Кулеш, "Дмитрий Шимкив: «От кибератаки вируса-шифровальщика Petya.A пострадало приблизительно 10% компьютеров в Украине»,," ITC UA, July 7, 2017, accessed November 18, 2019, <https://itc.ua/news/dmitriy-shimkiv-ot-kiberataki-virusa-shifrovalshhika-petya-a-postradalo-priblizitelno-10-vseh-kompyuterov-v-ukraine/>.
114. Thomas Brewster, "NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid,'" *Forbes*, July 3, 2017, accessed November 18, 2019, <https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#3587eebd6b89>.
115. Joe Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack," Dragos, August 15, 2019, accessed September 17, 2019, <https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>
116. Anton Cherepanov, "WIN32/INDUSTROYER," ESET, June 12, 2017, accessed August 2, 2019, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
117. Максим Яцков, "Хакеры атакуют: Государство пока не готово к кибервойне," 112.UA, December 29, 2016, accessed August 2, 2019, <https://112.ua/statji/hakery-atakuyut-gosudarstvo-poka-ne-gotovo-k-kiberbvojne-362294.html>.
118. "Ukrzaliznytsia Begins Testing Automated System for Distributing Empty Grain Cars," CFTS, August 4, 2017, accessed September 13, 2019, https://webcache.googleusercontent.com/search?q=cache:9AVUo5NZo4cj:hxxps://en.cfts.org.ua/news/ukrzaliznytsia_begins_testing_automated_system_for_distributing_empty_grain_cars+&cd=1&hl=en&ct=clnk&gl=us
119. "CrashOverride: Analysis of the Threat to Electric Grid Operators," Dragos Inc., June 13, 2017, accessed August 2, 2019, <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf>.
120. "Tkachuk: SBU has evidence that calls for "Maidan-3" are inspired by Russian secret services (video)," Security Service of Ukraine, February 15, 2017, accessed August 2, 2019, <https://ssu.gov.ua/en/news/1/category/2/view/2753#.wVZixfCP.dpbs>.
121. Richard Chirgwin, "SBU claims Russia was behind NotPetya," *The Register*, July 4, 2017, accessed November 18, 2019, https://www.theregister.co.uk/2017/07/04/sbu_claims_russia_was_behind_notpetya/.

122. Andy Greenberg, "The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack in History,'" *Wired*, February 15, 2018, accessed November 18, 2019, <https://www.wired.com/story/white-house-russia-notpetya-attribution/>.
123. Stillgherrian, "Blaming Russia for NotPetya was coordinated diplomatic action," ZDNet, April 12, 2018, accessed August 2, 2019, <https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/>.
124. "Bad Rabbit: The Full Research Investigation," CheckPoint, October 25, 2017, accessed August 2, 2019, <https://research.checkpoint.com/bad-rabbit-full-research-investigation/>; Orkhan Mamedov et al., "Bad Rabbit ransomware," Kaspersky SecureList, October 24, 2017, accessed August 2, 2019, <https://securelist.com/bad-rabbit-ransomware/82851/>.
125. BBC Staff, "'Bad Rabbit' ransomware strikes Ukraine and Russia," BBC, October 24, 2017, accessed August 2, 2019, <https://www.bbc.com/news/technology-41740768>.
126. Marc-Etienne M. Léveillé, "Bad Rabbit: Not-Petya is back with improved ransomware," ESET We Live Security, October 24, 2017, accessed August 2, 2019, <https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/>.
127. "Кібератака 24.10.2017," CERT-UA, October 24, 2017, accessed August 2, 2019, <https://web.archive.org/web/20171201184031/https://cert.gov.ua/?p=2945>
128. "Bad Rabbit: The Full Research Investigation," CheckPoint, October 25, 2017, accessed August 2, 2019, <https://research.checkpoint.com/bad-rabbit-full-research-investigation/>.
129. "Кібератака 24.10.2017," CERT-UA, October 24, 2017, accessed August 2, 2019, <https://web.archive.org/web/20171201184031/https://cert.gov.ua/?p=2945>
130. Orkhan Mamedov et al., "Bad Rabbit ransomware," Kaspersky SecureList, October 24, 2017, accessed August 2, 2019, <https://securelist.com/bad-rabbit-ransomware/82851/>.
131. Pavel Polityuk & Alessandra Prentice, "Exclusive: Ukraine hit by stealthier phishing attacks during Bad Rabbit strike," Reuters, November 2, 2017, accessed August 2, 2019, <https://www.reuters.com/article/us-cyber-summit-ukraine-police-exclusive/exclusive-ukraine-hit-by-stealthier-phishing-attacks-during-badrabbit-strike-idUSKBN1D2263>.
132. "ВАЖЛИВО!!! Розсилання вірусу під виглядом пропозиції завантаження оновлень для платформи 1С:Підприємство," ПП Інтек-Інформ, October 26, 2017, accessed August 7, 2019, https://web.archive.org/web/20180901153453/https://intec.in.ua/news/40-vazhливо!!!_rozsilannya_novogo_virusu.
133. "bdd273bab6c1ba7757b9c932fc7d7fd488126f50095676deae4262c71ab2fdb7," VirusTotal, accessed November 18, 2019, <https://www.virustotal.com/gui/file/bdd273bab6c1ba7757b9c932fc7d7fd488126f50095676deae4262c71ab2fdb7/details>.
134. Pavel Polityuk, "Exclusive: Ukraine says Russian hackers preparing massive strike," Reuters, June 26, 2018, accessed August 2, 2019, <https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-russian-hackers-preparing-massive-strike-idUSKBN1JM225> .
135. "'You can't let refugees do nothing': Russia's immigration tsar on EU migrant policies," RT, March 9, 2016, accessed November 18, 2019, <https://www.rt.com/russia/official-word/334949-romodanovsky-migration-europe-ukraine/>.
136. Vladimir Putin, Statement at the 70th session of the UN General Assembly, September 28, 2015, accessed August 8, 2019, https://web.archive.org/web/20180724062552/gadebate.un.org/sites/default/files/gastatements/70/70_RU_EN.pdf.
137. Masha Kirasirova, "What Vladimir Putin Really Wants in the Middle East," Foreign Policy, December 15, 2017, accessed August 8, 2019, <https://foreignpolicy.com/2017/12/15/what-vladimir-putin-wants-in-the-middle-east/>.
138. William Maclean, "Gulf Arabs oppose Russia role in Syria, still bent on Assad's ouster," Reuters, September 22, 2015, accessed August 8, 2019, <https://www.reuters.com/article/us-mideast-crisis-gulf-russia-idUSKCN0RM1JX20150922>.
139. Feike Hacquabord, "Pawn Storm Targets MH17 Investigation Team," TrendMicro, October 22, 2016, accessed October 13, 2016, <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/>.
140. Feike Hacquabord, "Two Years of Pawn Storm," Trend Micro, April 25, 2017, accessed August 6, 2019, <https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf>.
141. "Russia, Germany, France Criticize United States on Iraq," DW, March 19, 2003, accessed November 18, 2019, <https://www.dw.com/en/russia-germany-france-criticize-united-states-on-iraq/a-812501-0>.
142. Ted Galen Carpenter, "The Duplicitous Superpower," CATO Institute, November 28, 2017, accessed November 18, 2019, <https://www.cato.org/publications/commentary/duplicitous-superpower>.

143. "Statement by Ambassador Vitaly I. Churkin, Permanent Representative of the Russian Federation to the United Nations, at the Security Council meeting on the Report of the Secretary-General on the situation in Afghanistan and its implications for international peace and security," Permanent Mission of the Russian Federation to the United States, June 8, 2016, accessed November 18, 2019, https://russiaun.ru/en/news/sc_rpsgis
144. Dmitri Trenin, "The Mythical Alliance: Russia's Syria Policy," Carnegie Moscow Center, February 12, 2013, accessed November 18, 2019, <https://carnegie.ru/2013/02/12/mythical-alliance-russia-s-syria-policy-pub-50909>.
145. Former Staff, "Cameron asks lawmakers to mull UK air strikes on IS in Syria," Cyprus-Mail, July 2, 2015, accessed August 7, 2019, <https://cyprus-mail.com/2015/07/02/cameron-asks-lawmakers-to-mull-uk-air-strikes-on-is-in-syria/>.
146. BBC Staff, "David Cameron says bombing IS in Syria will make UK 'safer,'" BBC News, November 26, 2015, accessed August 7, 2019, <https://www.bbc.com/news/uk-politics-34927939>.
147. Alexander Yakovenko, "Russia and Britain should beat Isil as we did the Nazis: together," *The Telegraph*, November 27, 2018, accessed August 7, 2019, <https://www.telegraph.co.uk/news/worldnews/islamic-state/12019616/Russia-and-Britain-should-beat-Isil-as-we-did-the-Nazis-together.html>.
148. BBC Staff, " Syria air strikes: MPs authorise UK action against Islamic State," BBC News, December 3, 2015, accessed August 8, 2019, <https://www.bbc.com/news/uk-politics-34989302>.
149. "UN Security Council unanimously adopts Syrian roadmap resolution," RT, December 18, 2015, accessed September 27, 2019, <https://www.rt.com/news/326466-un-syria-resolution-terror/>
150. "GRU took 'complete control' of U.K.-based TV station in 2015," FT, October 5, 2018, accessed November 18, 2019, <https://www.ft.com/content/c35aaea2-c8b5-11e8-ba8f-ee390057b8c9>
151. Prime Minister and Minister of Foreign Affairs, "ATTRIBUTION OF A PATTERN OF MALICIOUS CYBER ACTIVITY TO RUSSIA," October 4, 2018, accessed August 7, 2019, <https://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia>.
152. SecureWorks Counter Threat Unit Threat Intelligence, "Iron Twilight Supports 'Active Measures,'" SecureWorks, March 30, 2017, accessed August 7, 2019, <https://www.secureworks.com/research/iron-twilight-supports-active-measures>.
153. "Reckless campaign of cyber attacks by Russian military intelligence service exposed," National Cyber Security Centre, October 3, 2018, accessed September 9, 2019, <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>.
154. Rik Ferguson, "TV5 Monde, Russia and the CyberCaliphate," Trend Micro, June 10, 2015, accessed August 26, 2019, <https://blog.trendmicro.com/tv5-monde-russia-and-the-cybercaliphate/>.
155. Alba, Alejandro, "FBI investigates ISIS hacker group Cyber Caliphate following series of hacks on news organizations in Maryland, Albuquerque," *New York Daily News*, January 6, 2015, accessed August 7, 2019, <https://www.nydailynews.com/news/national/isis-hacker-group-cyber-caliphate-hacks-article-1.2067634>.
156. Joshua Sinai, "The Terrorist Threats Against Russia and its Counterterrorism Response," Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Vo. 14, No. 4 (Fall 2015), accessed November 18, 2019, https://www.jstor.org/stable/26326421?seq=4#metadata_info_tab_contents.
157. "Combating terrorism," MOD Mission, Ministry of Defence of the Russian Federation, accessed November 18, 2019, https://eng.mil.ru/en/mission/fight_against_terrorism.htm.
158. Collin Anderson, "When Indicators of Compromise Become Indicators of Counterterrorism," CDA.IO, February 8, 2018, accessed November 18, 2019, <https://cda.io/notes/indicators-of-compromise-counterterrorism/>.
159. Moshe Gammer, "Separatism in the Northern Caucasus," Routledge Taylor & Francis Group, ISSN:2376-1199, April 13, 2015, accessed November 18, 2019, <https://www.tandfonline.com/doi/pdf/10.1080/23761199.2014.11417292>.
160. "Caucasus Emirate," Center for International Security and Cooperation, accessed November 18, 2019, <https://cisac.fsi.stanford.edu/mappingmilitants/profiles/caucasus-emirate/>.
161. "Chechnya and Secession in the Caucasus," Stratfor, May 23, 2011, accessed November 18, 2019, <https://worldview.stratfor.com/article/chechnya-and-secession-caucasus>.

162. Valery Dzutsati, "Tartar Nationalism Remains Vibrant Force in Volga Region," *Eurasia Daily Monitor*, Volume 9, Issue 2, The Jamestown Foundation, January 4, 2012, accessed November 18, 2019, <https://jamestown.org/program/tatar-nationalism-remains-vibrant-force-in-volga-region-2/>.
163. Remi Piet, "Kaliningrad: The last wall in Europe," Al Jazeera, November 18, 2014, accessed November 18, 2019, <https://www.aljazeera.com/indepth/opinion/2014/11/kaliningrad-last-wall-europe-20141116114613645536.html>.
164. "A Caucasus Ethnic Group Raises Concerns in Moscow," Stratfor, July 20, 2015, accessed November 18, 2019, <https://worldview.stratfor.com/article/caucasus-ethnic-group-raises-concerns-moscow>.
165. "Free Idel-Ural demands from Russia to stop the oppression of freedom of speech on the internet," UA Post, March 2, 2019, accessed November 18, 2019, <http://www.uapost.us/en/blog/ruh-viljnny-ideljural-vymagae-vid-rosiyi-prypnyty-utysky-svobody-slova-v-interneti/>.
166. Alec Luhn, "Russia bans Siberia independence march," *The Guardian*, August 5, 2014, accessed November 18, 2019, <https://www.theguardian.com/world/2014/aug/05/russia-bans-siberia-independence-march-extremism-law>.
167. Stefano Pozzebon, "All the other places Russia would be able to trigger a crisis," Business Insider, February 19, 2015, accessed August 2, 2019, <https://www.businessinsider.com/russia-foreign-influence-2015-2>
168. Mikhail Suslov, "'Russian World': Russia's Policy towards its Diaspora," Notes de l'Ifri, Russie.Nei.Visions 103, July 2017, accessed August 2, 2019 https://www.ifri.org/sites/default/files/atoms/files/suslov_russian_world_2017.pdf.
169. "Russia continues to support the separatist regimes," *International Herald Tribune*, April 3, 2008, accessed September 13, 2019, <https://web.archive.org/web/20080821043838/http://www.ihf.com/articles/ap/2008/04/03/europe/EU-GEN-Russia-Putin-Georgia.php>
170. Mansur Mirovalev, "What's Behind Russian Support for the World's Separatist Movements?" NBC News, July 23, 2016, accessed November 18, 2019, <https://www.nbcnews.com/news/world/what-s-behind-russian-support-world-s-separatist-movements-n614196>.
171. The New York Review of Books, "The Victory of Ukraine," Anne Applebaum, April 7, 2016, accessed August 2, 2019, <https://www.annapplebaum.com/2016/04/07/3326/>.
172. "'Russians and Ukrainians are one people,' Putin tells Oliver Stone," Russia Today, July 9, 2019, accessed August 4, 2019, <https://www.rt.com/news/463775-putin-russia-ukraine-one-nation/>
173. "Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины," Centrum, January 6, 2016, accessed August 2, 2019, https://cys-centrum.com/ru/news/black_energy_2_3;
174. Robert Lipovsky, "Black Energy 2014," ESET, November 19, 2014, accessed August 2, 2019, http://static5.esetstatic.com/fileadmin/Images/SK/Kampane/2014/ESET-Security-Days/ESET_ESD_Lipovsky_19_11_2014.pdf.
175. Vyacheslav Likhachev, "Far-Right Extremism as a Threat to Ukrainian Democracy," Freedom House, May 2018, accessed August 2, 2019, <https://freedomhouse.org/report/special-reports/far-right-extremism-threat-ukrainian-democracy>.
176. Alex Grigsby, "Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations," Council on Foreign Relations, October 29, 2018, accessed November 18, 2019, <https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations>.
177. David Ignatius, "Russia is pushing to control cyberspace. We should all be worried." *The Washington Post*, October 24, 2017, accessed November 18, 2019, https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014bcc6-b8f1-11e7-be94-fabb0f1e9ffb_story.html.
178. David E. Sanger, "'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?" *The New York Times*, August 16, 2016, accessed November 18, 2019, <https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html>.
179. "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," White House, December 19, 2017, accessed December 11, 2019, [https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/;](https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/)
180. Tor Bukkvoll, "Russian Special Operations Forces in Crimea and Donbass," Russian Military Power, 2016, accessed August 2, 2019, https://ssi.armywarcollege.edu/pubs/Parameters/issues/Summer_2016/5_Bukkvoll.pdf.

181. Robert Morgus, "WHODUNNIT? RUSSIA AND COERCION THROUGH CYBERSPACE," War on the Rocks, October 19, 2016, accessed September 23, 2019, <https://warontherocks.com/2016/10/whodunnit-russia-and-coercion-through-cyberspace/>
182. Katya Gorchinskaya, Olga Rudenko, William Schreiber, "Authorities: Hackers foiled in bid to rig Ukraine presidential election results," Kyiv Post, May 25, 2014, accessed September 23, 2019, <https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html>
183. Nikolay Koval, "Revolution Hacking," Chapter 6, Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO Cooperative Cyber Defense Center of Excellence Publications, Tallinn 2015, https://web.archive.org/web/20160319120248/https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Koval_06.pdf.
184. Kenneth Geers, *Cyber War in Perspective*, NATO CCD COE, 2015, accessed August 2, 2019, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf.
185. "Ukraine election narrowly avoided 'wanton destruction' from hackers," Christian Science Monitor, June 17, 2014, accessed September 23, 2019, <https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers>.
186. Steve Gutterman & Gleb Bryanski, "Putin says U.S. stoked Russian protests," Reuters, December 8, 2011, accessed August 8, 2019, <https://www.reuters.com/article/us-russia/putin-says-u-s-stoked-russian-protests-idUSTRE7B610S20111208>.
187. Susan Cornwell, "U.S. pro-democracy groups pulling out of Russia," Reuters, December 14, 2012, accessed August 8, 2019, <https://www.reuters.com/article/russia-usa-democracy-idUSL1E8NE7FF20121214>.
188. Alec Luhn, "Russia bans 'undesirable' international organisations ahead of 2016 elections," *The Guardian*, May 19, 2015, accessed August 8, 2019, <https://www.theguardian.com/world/2015/may/19/russia-bans-undesirable-international-organisations-2016-elections>.
189. Special Counsel Robert S. Mueller, III, "Report on the Investigation Into Russian Interference in the 2016 Presidential Election," Volume I of II, U.S. Department of Justice, March 2019, accessed August 7, 2019, https://www.justice.gov/storage/report_volume1.pdf.
190. Thomas Rid, "All Signs Point to Russia Being Behind the DNC Hack," *Vice*, July 25, 2016, accessed November 18, 2019, https://www.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack.
191. Ilya Arkhipov & Boris Groendahl, "Putin Teases that His Troll-Factory Ally Is Just Like Soros," Bloomberg, June 4, 2018, accessed August 8, 2019, <https://www.bloomberg.com/news/articles/2018-06-04/putin-teases-that-his-troll-factory-ally-is-just-like-soros>.
192. *United States of America v. Viktor Borisovich Netyksho et al.*, United States District Court for the District of Columbia, Case 1:18-cr-00215-ABJ, July 13, 2018, accessed August 2, 2019, <https://www.justice.gov/file/1080281/download>.
193. Randi Nord, "Thousands of Files from Soros' Foundation Hacked and Released," *Geopolitics Alert*, August 15, 2016, accessed August 7, 2019, <https://geopoliticsalert.com/thousands-files-soros-foundation-hacked-released>.
194. "CyberBerkut hacked NED: U.S. is preparing a color revolution in Russia according to Ukrainian model," *CyberBerkut*, October 22, 2016, accessed October 4, 2019, <https://archive.is/0ENmH#selection-513.18-519.28>
195. Sarah Hurst, "Russia's war on George Soros goes global," *Kharvkiv Human Rights Protection Group*, April 9, 2017, accessed August 7, 2019, <https://khp.org/en/index.php?id=1491771331>.
196. Darya Korsunskaya, "Putin says Russia must prevent 'color revolution,'" Reuters, November 20, 2014, accessed August 8, 2019, <https://www.reuters.com/article/us-russia-putin-security-idUSKCN0J41J620141120>.
197. Steve Gutterman & Gleb Bryanski, "Putin says U.S. stoked Russian protests," Reuters, December 8, 2011, accessed August 8, 2019, <https://www.reuters.com/article/us-russia/putin-says-u-s-stoked-russian-protests-idUSTRE7B610S20111208>.
198. "В реестр некоммерческих организаций, выполняющих функции иностранного агента, включена Автономная некоммерческая организация «Центр антикоррупционных исследований и инициатив «Трансперенси Интернешнл – Р»," Ministry of Justice of the Russian Federation, April 7, 2015, accessed August 7, 2019, <https://minjust.ru/ru/press/news/v-reestr-nekommercheskih-organizacij-vypolnyayushchih-funkcii-inostrannogo-agenta-5>.

199. Jennifer Ablan, "Russia bans George Soros foundation as state security 'threat,'" Reuters, November 30, 2015, accessed August 7, 2019, <https://www.reuters.com/article/russia-soros/russia-bans-george-soros-foundation-as-state-security-threat-idUSL1N13P22Y20151130>.
200. Ivan Nechepurenko, "Pro-Democracy Nonprofit Is Banned in Russia," *The New York Times*, March 11, 2016, accessed November 18, 2019, <https://www.nytimes.com/2016/03/12/world/europe/national-democratic-institute-banned-russia.html>.
201. "Russia Adds International Republican Institute to Growing List of "Undesirable Organizations," " International Republican Institute, August 18, 2016, accessed August 7, 2019, <https://www.iri.org/resource/russia-adds-international-republican-institute-growing-list-%E2%80%9Cundesirable-organizations%E2%80%9D>.
202. Evan Gershkovich, "The Kremlin Sees Signs of Foreign Interference All Around," *The Moscow Times*, August 14, 2019, accessed November 18, 2019, <https://www.themoscowtimes.com/2019/08/14/the-kremlin-sees-signs-of-foreign-interference-all-around-a66839>.
203. "mta-sts.mail.hudsonorg-my-sharepoint.com," VirusTotal, last updated March 2019, accessed August 7, 2019, <https://www.virustotal.com/gui/domain/mta-sts.mail.hudsonorg-my-sharepoint.com/relations>.
204. Ben Judah & Nate Sibley, "The Enablers: How Western Professionals Import Corruption and Strengthen Authoritarianism," Hudson Institute, September 5, 2018, accessed August 7, 2019, <https://www.hudson.org/policycenters/31-kleptocracy-initiative>.
205. Fancy Bear Phishing, AlienVault, last updated July 18, 2019, accessed August 7, 2019, https://otx.alienvault.com/pulse/5d2db9cc8e1eb4d4d4be15e5?utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_subscribed;
206. Kevin Poulsen, "Russia's Election Hackers Are Back – and Targeting George Soros," *The Daily Beast*, July 15, 2019, accessed August 7, 2019, <https://www.thedailybeast.com/russias-election-hackers-are-backand-targeting-george-soros-and-his-open-society-foundations>.
207. Adam Taylor, "A recent history of terrorist attacks in Russia," *The Washington Post*, April 3, 2017, accessed August 8, 2019, <https://www.washingtonpost.com/news/worldviews/wp/2017/04/03/the-recent-history-of-terrorist-attacks-in-russia/>.
208. "Why Russia Will Send More Troops to Central Asia," Stratfor, April 11, 2015, accessed August 7, 2019, <https://worldview.stratfor.com/article/why-russia-will-send-more-troops-central-asia>.
209. "Invisible War," Human Rights Watch, June 18, 2015, accessed August 8, 2019, <https://www.hrw.org/report/2015/06/18/invisible-war/russias-abusive-response-dagestan-insurgency>.
210. Andrew E. Kramer, "A Russian Region Neither at War Nor at Peace, but Facing a Crackdown," *The New York Times*, October 9, 2013, accessed August 8, 2019, <https://www.nytimes.com/2013/10/10/world/europe/a-russian-region-neither-at-war-nor-at-peace-but-facing-a-crackdown.html>;
211. Michael Church, "Russia's bitter relationship with Chechnya will be in the spotlight during Sochi 2014 Winter Olympics in February," *The Independent*, December 26, 2013, accessed August 8, 2019, <https://www.independent.co.uk/news/world/europe/russia-s-bitter-relationship-with-chechnya-will-be-in-the-spotlight-during-sochi-2014-winter-9026259.html>.
212. "APT28: A Window Into Russia's Cyber Espionage Operations?" FireEye, October 27, 2014, accessed August 8, 2019, <https://www2.fireeye.com/rs/fireeye/images/rpt-apt28.pdf>.
213. "Olympics: Putin says Russia's Sochi 'risk' paid off," *The Straits Times*, February 4, 2019, accessed November 18, 2019, <https://www.straitstimes.com/sport/olympics-putin-says-russias-sochi-risk-paid-off>.
214. "How the Russian Orthodox Church Influences Russia's Behavior," National Interest, July 8, 2019, accessed August 8, 2019, <https://nationalinterest.org/feature/how-russian-orthodox-church-influences-russias-behavior-66091>.
215. Dmitry Adamsky, "How the Russian Church Learned to Stop Worrying and Love the Bomb," *Foreign Policy*, June 14, 2019, accessed August 8, 2019, <https://www.foreignaffairs.com/articles/russian-federation/2019-06-14/how-russian-church-learned-stop-worrying-and-love-bomb>.
216. Raphael Satter, "Moscow, Kiev in tug-of-war over religious future of Ukraine," Associated Press, August 27, 2018, August 27, 2018, <https://apnews.com/c892a7746e994c928bef6a7ffa4096c2>.

217. "We are creating another pillar of Ukrainian independence: President on the founding of the Autocephalous Ukrainian Orthodox Church," Religious Information Service of Ukraine, December 8, 2018, https://risu.org.ua/en/index/all_news/state/national_religious_question/73820/.
218. Raphael Satter, "Ungodly espionage: Russian hackers targeted Orthodox clergy," Associated Press, August 27, 2018, accessed August 8, 2019, <https://www.apnews.com/26815e0d06d348f4b85350e96b78f6a8>.
219. Feike Hacquebord, "Two Years of Pawn Storm," Trend Micro Forward-Looking Threat Research Team, April 25, 2017, accessed September 16, 2019, https://media.scmagazine.com/documents/295/trend_micro-two-years-of-pawn-_73730.pdf.
220. "Soviet Union and the Olympics," Wilson Center Digital Archive, accessed August 7, 2019, <https://digitalarchive.wilson-center.org/collection/266/soviet-union-and-the-olympics>.
221. Gabrielle Tetrault-Farber, "Traces of Soviet Doping Culture Linger in Russia," *The Moscow Times*, December 5, 2013, accessed August 7, 2019, <https://www.themoscowtimes.com/2013/12/05/traces-of-soviet-doping-culture-linger-in-russia-a30243>
222. Kurt Johnson, "Rio 2016: What Russia's doping scandal owes to the Soviet Union," ABC News, August 18, 2016, accessed August 7, 2019, <https://www.abc.net.au/news/2016-08-18/russia-olympic-doping-scandal-hangover-ussr-soviet-era/7756632>.
223. Lawrence Ostlere, "McLaren report: more than 1,000 Russian athletes involved in doping conspiracy," *The Guardian*, December 9, 2016, accessed August 7, 2019, <https://www.theguardian.com/sport/live/2016/dec/09/mclaren-report-into-doping-in-sport-part-two-live>.
224. Independent Commission Report #1, Final Report, November 9, 2015, accessed September 16, 2019, https://wada-main-prod.s3.amazonaws.com/resources/files/wada_independent_commission_report_1_en.pdf
225. Hyung-Jin Kim, "IOC bans Russia from 2018 Winter Olympics," CBC Sports, December 5, 2017, accessed August 7, 2019, <https://www.cbc.ca/sports/olympics/ioc-russia-doping-1.4432781>.
226. United States of America v. Aleksei Sergeyevich Morenets et al., United States District Court for the Western District of Pennsylvania, Case 2:18-cr-00263-MRH, March 10, 2018, accessed August 2, 2019, <https://www.justice.gov/opa/page/file/1098481/download>.
227. Press Release, International Association of Athletics Federations, April 3, 2017, accessed August 7, 2019, <https://www.iaaf.org/news/press-release/iaaf-cyber-attack>.
228. Therapeutic Use Exemptions, World Anti-Doping Agency, accessed August 7, 2019, <https://www.wada-ama.org/en/what-we-do/science-medical/therapeutic-use-exemptions>.
229. Office of Public Affairs, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Department of Justice, October 4, 2018, accessed August 7, 2019, <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and>
230. "wada-arna.org," DomainTools, accessed August 7, 2019, <https://research.domaintools.com/research/whois-history/search/?q=wada-arna.org>.
231. "WADA Hack: Leaked Documents Expose U.S. Athletics' Hypocrisy," Sputnik News, September 14, 2016, accessed September 16, 2019, <https://sputniknews.com/us/201609141045279660-wada-hack-us-hypocrisy/>.
232. Russian Embassy, UK (@RussianEmbassy), Twitter, September 15, 2016, accessed September 16, 2019, <https://twitter.com/RussianEmbassy/status/776343061504860161>.
233. Ellen Nakashima, "Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say," *The Washington Post*, February 24, 2018, accessed August 7, 2019, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.1026c50a5e53.
234. GreAT, "OlympicDestroyer is here to trick the industry," Kaspersky SecureList, March 8, 2018, accessed August 8, 2019, <https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/>.

235. Jim Finkle, "'Olympic Destroyer' malware targeted Pyeongchang Games: firms," Reuters, February 12, 2018, accessed August 8, 2019, <https://www.reuters.com/article/us-olympics-2018-cyber/olympic-destroyer-malware-targeted-pyeongchang-games-firms-idUSKBN1FW22O>.
236. Rebecca R. Ruiz, "U.S. Athletes Reassured After New Russian Hack," *The New York Times*, October 14, 2016, accessed August 7, 2019, <http://www.nytimes.com/2016/10/15/sports/us-officials-reassure-athletes-after-new-russian-hack-of-medical-files.html>;
237. Office of Public Affairs, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Department of Justice, October 4, 2018, accessed August 7, 2019, <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and>.
238. "Cyber Security Update: WADA's Incident Response," World Anti-Doping Agency, October 5, 2016, accessed August 7, 2019, <https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response>.
239. Chris Bing, "Winter Olympics cyberattacks meant to 'send a message,'" Cyberscoop, February 12, 2018, accessed August 8, 2019, <https://www.cyberscoop.com/winter-olympics-cyberattacks-olympic-destroyer-fireeye-talos/>.
240. Guzel Yusupova, "Why Ethnic Politics in Russia Will Return," PONARS Eurasia Policy Memo 584, March 2019, accessed November 12, 2019, <http://www.ponarseurasia.org/memo/why-ethnic-politics-russia-will-return>.
241. Konstantin Fischer, "The Kremlin's Love and Fear of Separatism," Institute of Modern Russia, November 12, 2015, accessed November 12, 2019, <https://imrussia.org/en/politics/2469-the-kremlin%E2%80%99s-love-and-fear-of-separatism>.
242. John Sipher, "Western Covert Action and Russian Active Measures: Hypocrisy or Divergent Values?," Just Security, January 22, 2019, accessed November 12, 2019, <https://www.justsecurity.org/62324/western-covert-action-russian-active-measures/>.
243. Roman Hryvinskyy "Ukrainian Muslims: A history of solidarity," Euromaidan Press, January 31, 2016, accessed August 8, 2019, <http://euromaidanpress.com/2016/01/31/ukrainian-moslems-a-history-of-solidarity/>.
244. Cnaan Liphshiz, "Ukrainian Jewish leader claims Russians manipulated U.S. lawmakers," Jewish Telegraphic Agency, May 2, 2018, accessed August 8, 2019, <https://www.jta.org/2018/05/02/global/congressmens-letter-ukraine-anti-semitism-may-russian-conspiracy-jewish-leader-suggests>
245. Veronika Melkozerova, "Ukrainian Jewish leaders challenge report on rising anti-Semitism," Kyiv Post, January 29, 2018, accessed August 8, 2019, <https://www.kyivpost.com/lifestyle/people/journalism-of-tolerance/ukrainian-jewish-leaders-challenge-report-rising-anti-semitism.html>.
246. Ann Schneible, "Pope Francis lauds fidelity of Ukrainian Greek-Catholics," Catholic News Agency, March 6, 2016, accessed August 8, 2019, <https://www.catholicnewsagency.com/news/pope-francis-lauds-fidelity-of-ukrainian-greek-catholics-95113>.
247. BBC Staff, "Ukraine crisis: EU signs association deal," BBC, March 21, 2014, accessed August 2, 2019, <http://www.bbc.co.uk/news/world-europe-26680250>.
248. BBC Staff, "Ukraine to seek Nato membership, says PM Yatsenyuk," BBC, August 29, 2014, accessed August 2, 2019, [https://www.bbc.com/news/world-europe-28978699](http://www.bbc.com/news/world-europe-28978699).
249. "Від аптечок до технологій: як Захід допомагає українській," Center for Public Monitoring and Control, January 29, 2018, accessed August 5, 2019, <https://naglyad.org/uk/2018/01/29/vid-aptechok-do-tehnologij-yak-zahid-dopomagaye-ukrayinskij-armiyi/>.
250. Robert Lipovsky and Anton Cherepanov, "Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," ESET, last modified October 14, 2014, accessed August 4, 2019, <https://youtu.be/l77CGqQvPE4?t=801>.
251. "BlackEnergy & Quedagh," F-Secure, September 2014, accessed August 2, 2019, https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.
252. Stephen Ward, "iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign," iSIGHTPARTNERS, October 14, 2014, accessed August 2, 2019, <https://web.archive.org/web/20141031204521/https://www.isightpartners.com/2014/10/cve-2014-4114/>.
253. Ariel Cohen, "Ukraine's Most Important Battle Is for Energy Independence," *Forbes*, June 30, 2019, accessed November 19, 2019, <https://www.forbes.com/sites/arielcohen/2019/06/30/ukraines-most-important-battle-is-for-energy-independence/#665c8ce430d3>.

254. Feike Hacquebord, "Operation Pawn Storm Ramps Up Its Activities; Targets NATO, White House," Trend Micro Security Intelligence Blog, April 16, 2015, accessed August 7, 2019, <https://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/>.
255. "Energoatom seeks to extend links with Westinghouse," World Nuclear News, March 11, 2015, accessed August 7, 2019, "Russia Must be Called to Account for the MH-17 Tragedy," Voice of America, Editorials, June 3, 2018, accessed November 19, 2019, <http://www.world-nuclear-news.org/C-Energoatom-seeks-to-extend-links-with-Westinghouse-11031501.html>.
256. "MH17 missile owned by Russian brigade, investigators say," CNN, May 24, 2018, accessed November 19, 2019, <https://www.bbc.com/news/world-europe-44235402>; <https://editorials.voanews.com/a/russia-called-account-mh-17/4419902.html>.
257. Uutiset, "Suomi salaa mukana ammutun koneen tutkinnassa," Iltalehti, August 22, 2015, accessed August 6, 2019, <https://www.iltalehti.fi/uutiset/a/2015082220215354>.
258. YLE, "Russian cyber-espionage group hits Sanoma," YLE, May 30, 2016, accessed August 6, 2019, https://yle.fi/uutiset/osasto/news/russian_cyber-espionage_group_hits_sanoma/8919118.
259. Veli-Pekka Kivimäki, "Geolocating the MH17 Buk Convoy in Russia," Bellingcat, September 29, 2014, accessed August 6, 2019, <https://www.bellingcat.com/resources/case-studies/2014/09/29/geolocating-the-mh17-buk-convoy-in-russia/>.
260. Luke Harding, "How Russian spies bungled cyber-attack on weapons watchdog," *The Guardian*, October 4, 2018, accessed December 10, 2019, <https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog>
261. Genmaj. O. Eichlelsheim, "GRU Close Access Cyber Operation Against OPCW," Defense Intelligence & Security Service, October 4, 2018, accessed December 10, 2019, <https://info.publicintelligence.net/NL-MoD-RussianOperationOPCW.pdf>
262. Bellingcat Investigation Team, "JIT Indictments and Reactions: Analyzing New Evidence Linking Separatists and Russian Officials to MH17," Bellingcat, July 17, 2019, accessed August 8, 2019, <https://www.bellingcat.com/news/uk-and-europe/2019/07/17/jit-indictments-and-reactions-analyzing-new-evidence-linking-separatists-and-russian-officials-to-mh17/>.
263. Bellingcat Investigation Team, "The GRU Globetrotters: Mission London," Bellingcat, June 28, 2019, accessed August 8, 2019, <https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/>.
264. Bellingcat Investigation Team, "Second GRU Officer Indicted in Montenegro Coup Unmasked," Bellingcat, November 22, 2018, accessed August 8, 2019, <https://www.bellingcat.com/news/uk-and-europe/2018/11/22/second-gru-officer-indicted-montenegro-coup-unmasked/>.
265. Joseph Cox, "Kremlin-Linked Hackers Expose a Network of Fake Tech-News Sites," *The Daily Beast*, November 30, 2017, accessed August 8, 2019, <https://www.thedailybeast.com/kremlin-linked-hackers-expose-a-network-of-fake-tech-news-sites>.
266. Joseph Cox, "Dodgy 'Hackers' Target Bellingcat Investigators Who Call BS on Moscow," *The Daily Beast*, March 13, 2018, accessed August 8, 2019, <https://www.thedailybeast.com/polish-hackers-target-investigators-who-call-bs-on-moscow>.
267. Associated Press, "Ukraine, Poland Want Continued Sanctions on Russia," *Voice of America*, August 31, 2019, accessed November 19, 2019, <https://www.voanews.com/europe/ukraine-poland-want-continued-sanctions-russia>.
268. "Ukraine is grateful to Poland for supporting its interests in the European Union and NATO-President," Official Website of the President of Ukraine, Volodymyr Zelensky, June 4, 2019, accessed November 19, 2019, <https://www.president.gov.ua/en/news/ukrayina-duzhe-vdyachna-polshi-za-pidtrimku-svoyih-interesiv-55757>
269. "Poland's neighbourly support for implementation of Ukraine' -EU association agreement," Polish aid, accessed November 19, 2019, <https://polskapomoc.gov.pl/Poland%E2%80%99s,neighbourly,support,for,implementation,of,Ukraine-EU,association,agreement,2998.html>.
270. "NATO Sees Ukraine Incursion Risk After Russian Troop Buildup," *Newsmax*, August 5, 2014, accessed August 6, 2019, <https://www.newsmax.com/world/Europe/NATO-Ukraine-Russia/2014/08/06/id/587185/>.
271. Aric Toler, "Addressing the Aeroflot MH17 Conspiracy Theory," Bellingcat, August 8, 2018, accessed August 6, 2019, <https://www.bellingcat.com/news/uk-and-europe/2018/08/08/addressing-aeroflot-mh17-conspiracy-theory/>.
272. Anna Mostovych, "SBU gives evidence on RF plans to bring down Aeroflot plane to int'l experts," *Euro Maidan Press*, August 8, 2014, accessed August 6, 2019, <https://euromaidanpress.com/2014/08/09/sbu-gives-evidence-on-rf-plans-to-bring-down-aeroflot-plane-to-intl-experts/>.

273. Reuters, "Polish ex-minister quoted saying Putin offered to divide Ukraine with Poland," *The Telegraph*, October 21, 2014, accessed August 7, 2019, <https://www.telegraph.co.uk/news/worldnews/vladimir-putin/11176025/Polish-ex-minister-quoted-saying-Putin-offered-to-divide-Ukraine-with-Poland.html>.
274. J.C., "Donetsk for me, Lviv for you," *The Economist*, October 21, 2014, accessed November 19, 2019, <https://www.economist.com/eastern-approaches/2014/10/21/donetsk-for-me-lviv-for-you>.
275. Stephen Ward, "iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign." iSIGHT Partners, October 14, 2014, accessed August 5, 2019, <https://web.archive.org/web/20141031204521/https://www.isightpartners.com/2014/10/cve-2014-4114/>
276. Andrew E. Kramer, "Gas Dispute Has Effects Past Russia and Ukraine," January 3, 2009, accessed August 5, 2019, <https://www.nytimes.com/2009/01/04/world/europe/04russia.html>.
277. Oleg Vukmanovic & Agnieszka Barteczko, "Poland's energy security strategy comes at high cost," Reuters, September 9, 2013, accessed August 5, 2019, <https://www.reuters.com/article/poland-energy-lng/polands-energy-security-strategy-comes-at-high-cost-idUSL6N0H22WR20130909>; <https://www.nytimes.com/2019/02/26/business/poland-gas-lng-russia-usa.html>
278. Mohd Razman Abdullah, "Malaysia, Netherlands Call for Immediate Cessation of Hostilities at MH17 Crash Site," Flight MH17 Tragedy, July 31, 2014, accessed August 6, 2019, <http://web10.bernama.com/mh17/index.php?lang=en&sid=newsdetail&id=1057183>.
279. Cert.Gov.Pl, "Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014," March 2015, accessed August 7, 2019, <https://web.archive.org/web/20180218091431/http://www.cert.gov.pl/download/3/172/RaportostaniebezpieczenstwacyberprzestrzeniRPw2014roku.pdf>.
280. "Ukrainian hackers claim attack on Polish websites," AFP, August 14, 2014, accessed August 6, 2019, <https://news.yahoo.com/ukrainian-hackers-claim-attack-polish-websites-193806386.html>;
281. "In Ukraine enacted a ban on freedom of speech," CyberBerkut, December 30, 2014, accessed August 6, 2019, <http://cyber-berkut.org/en/olden/index2.php>.
282. KS, "Sienkiewicz zatrudnił byłą asystentkę," Super Express, August 22, 2013, accessed August 6, 2019, <https://www.se.pl/wiadomosci/polska/sienkiewicz-zatrudni-bya-asystentke-aa-6MHS-NPGR-wdXa.html>.
283. "Poland calls for end to 'Polish mercenaries in Ukraine' reports," Radio Poland, August 20, 2014, accessed August 6, 2019, <http://archiwum.thenews.pl/1/10/Artykul/179300>
284. "Fake: Polish Company ASBS Othago is Fighting on the Side of the Ukrainian Military Forces," Stop Fake, August 15, 2014, accessed August 6, 2019, <https://www.stopfake.org/en/fake-polish-company-asbs-othago-is-fighting-on-the-side-of-the-ukrainian-military/>.
285. Annabelle Chapman, "Secret Tapes in Polish 'Waitergate' Scandal Could Cost Warsaw's Government a Key European Commission Post," *Newsweek*, July 15, 2014, accessed August 6, 2019, <https://www.newsweek.com/secret-tapes-polish-waitergate-scandal-could-cost-warsaws-government-key-european-258912>
286. Michael E. Miller, "Secret recordings, posh restaurants, Cuban cigars and intrigue finally catch up to Polish government," *The Washington Post*, June 11, 2015, accessed August 6, 2019, https://www.washingtonpost.com/news/morning-mix/wp/2015/06/11/sex-lies-and-audio-tape-secret-recordings-finally-catch-up-to-polish-government/?utm_term=.8d377f602af1.
287. Michael Riley, "Cyberspace becomes second front in Russia's clash with NATO," *The Sydney Morning Herald*, October 15, 2015, accessed August 6, 2019, <https://www.smh.com.au/technology/cyberspace-becomes-second-front-in-russias-clash-with-nato-20151015-gk9l54.html>.
288. Vi.curry, "Giełda Papierów Wartościowych zhackowana — wykradziono hasła i dokumenty," Niebezpiecznik, October 23, 2014, accessed October 7, 2019, <https://niebezpiecznik.pl/post/gielda-papierow-wartosciowych-zhackowana/>.
289. Sharon Muthoni & Ryan Faith, "The Russia-France Warship Deal Is Turning into a Mess," Vice News, November 21, 2014, accessed August 8, 2019, https://news.vice.com/en_us/article/zm59nw/the-russia-france-warship-deal-is-turning-into-a-total-mess.

290. Henry Samuel, "France suspends delivery of helicopter assault ships to Russia due to Ukraine crisis," *The Telegraph*, September 3, 2014, accessed August 8, 2019, <https://www.telegraph.co.uk/news/worldnews/europe/france/11073659/France-suspends-delivery-of-helicopter-assault-ships-to-Russia-due-to-Ukraine-crisis.html>.
291. Christopher Harress, "Russia Delays Mistral Legal Action Against France Until February," *International Business Times*, January 14, 2015, accessed August 8, 2019, <https://www.ibtimes.com/russia-delays-mistral-legal-action-against-france-until-february-1783414>.
292. AFP, "Russia behind major cyber attacks, says German spy service," *Asia One*, May 13, 2016, accessed August 6, 2019, <https://www.asiaone.com/world/russia-behind-major-cyber-attacks-says-german-spy-service>.
293. "Reckless campaign of cyber attacks by Russian military intelligence service exposed," National Cybersecurity Centre, United Kingdom, October 3, 2018, accessed August 6, 2019, <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>.
294. Matthew J. Schwartz, "French Officials Detail 'Fancy Bear' Hack of TV5Monde," *Bank Info Security*, June 12, 2017, accessed August 6, 2019, <https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983>.
295. Matt Suiche, "Lessons from TV5Monde 2015 Hack," *Comae*, June 10, 2017, accessed August 6, 2019, <https://blog.comae.io/lessons-from-tv5monde-2015-hack-c4d62f07849d>.
296. "French TV station 'hacked by ISIS' exposes account passwords on air," *RT*, April 10, 2015, accessed August 8, 2019, <https://www.rt.com/news/248741-french-tv-isis-passwords/>.
297. Jamie Campbell, "French TV network TV5Monde 'hacked by cyber caliphate in unprecedented attack' that revealed personal details of French soldiers," *The Independent*, April 9, 2015, accessed August 6, 2019, <https://www.independent.co.uk/news/world/europe/french-tv-network-tv5monde-hijacked-by-isis-hackers-in-unprecedented-attack-that-revealed-personal-10164285.html>.
298. Laura Smith-Spark, "French Muslims warn of growing anti-Islam backlash," <https://www.cnn.com/2015/01/13/europe/france-anti-muslim-threats/index.html>.
299. Nick Riemer, "The roots of Islamophobia in France," *CNN*, January 14, 2015, accessed August 6, 2019, <https://www.cnn.com/2015/01/13/europe/france-anti-muslim-threats/index.html>.
300. Jacobin, August 29, 2016, accessed August 6, 2019, <https://www.jacobinmag.com/2016/08/burkini-ban-islamophobia-valls-france-secularism-islam/>.
301. Dmitri Trenin, "Russia and Germany: From Estranged Partners to Good Neighbors," *Carnegie Moscow Center*, June 6, 2018, accessed August 6, 2019, <https://carnegie.ru/2018/06/06/russia-and-germany-from-estranged-partners-to-good-neighbors-pub-76540>.
302. "Merkel's top foreign policy adviser to meet with team of U.S. President-elect Trump," *DW*, December 17, 2016, accessed August 7, 2019, <https://www.dw.com/en/merkels-top-foreign-policy-adviser-to-meet-with-team-of-us-president-elect-trump/a-36814422>.
303. Juliane Schauble, "Christoph Heusgen, German ambassador to the United Nations, talks about Germany's goals, Donald Trump and German blue helmet missions," *The Germany Times*, March 2019, accessed August 6, 2019, <https://www.german-times.com/christoph-heusgen-german-ambassador-to-the-united-nations-talks-about-germanys-goals-donald-trump-and-german-blue-helmet-missions/>.
304. "Deutscher UN-Repräsentant: Russische Soldaten haben Teile der Ukraine besetzt," Editorial, *Ukraine Journal*, February 13, 2019, accessed August 6, 2019, <https://ukraine-journal.de/deutscher-un-representant-russische-soldaten-haben-teile-der-ukraine-besetzt/>.
305. "Heusgen soll UN-Botschafter werden," *Politik & Kommunikation*, November 28, 2016, accessed August 6, 2019, <https://www.politik-kommunikation.de/personalwechsel/heusgen-soll-un-botschafter-werden-1936115237>.
306. Janosch Delcker, "Merkel's foreign adviser to become Germany's UN ambassador: report," *Politico*, November 25, 2016, accessed August 7, 2016, <https://www.politico.eu/article/merkels-foreign-adviser-christoph-heusgen-germanys-un-ambassador-report/>.

307. Alliance News, "Russian Hackers Suspected in Cyberattack on German Parliament," London South East, June 19, 2015, accessed August 6, 2019, http://www.lse.co.uk/AllNews.asp?code=kwdwehme&headline=Russian_Hackers_Suspected_In_Cyberattack_On_German_Parliament.
308. BBC Staff, "Russia 'was behind German parliament hack,'" BBC News, May 13, 2016, accessed August 6, 2019, <http://www.bbc.com/news/technology-36284447>.
309. Max Metzger, "German Intelligence blames Russia for Parliament hack," SC Magazine, May 16, 2016, accessed August 7, 2019, <http://www.scmagazineuk.com/german-intelligence-blames-russia-for-parliament-hack/article/496583/>
310. Der Spiegel Staff, "The Breach from the East," Spiegel Online, March 5, 2018, accessed August 6, 2019, <http://www.spiegel.de/international/germany/cyber-espionage-likely-from-russia-targets-german-government-a-1196520.html>.
311. Raphael S. Cohen & Andrew Radin, "Russia's Hostile Measures in Europe: Understanding the Threat," Rand Corporation, April 15, 2019, accessed November 19, 2019, https://books.google.com/books?id=oW2RDwAAQBAJ&pg=PA120&lp-g=PA120&dq=%22Die+Linke%22+germany+russia+funding&source=bl&ots=ku-9AYcvg9&sig=ACfU3U0bGL_bRjQOAU_0B_6X5-eK4rxKzA&hl=en&sa=X&ved=2ahUKewjmbL5wdHIAhWkwFkKHfLOB3o4ChDoATAEegQICRAB#v=onepage&q=%22Die%20Linke%22%20germany%20russia%20funding&f=false.
312. "Germany's political parties CDU, CSU, SPD, AfD, FDP, Left party, Greens—what you need to know," DW, July 6, 2019, accessed August 6, 2019, <https://www.dw.com/en/germanys-political-parties-cdu-csu-spd-afd-fdp-left-party-greens-what-you-need-to-know/a-38085900>.
313. "Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag," Netzpolitik, June 19, 2015, accessed August 6, 2019, <https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/>.
314. J.C., "Germany's election: a primer," *The Economist*, August 11, 2017, accessed August 6, 2019, <http://www.economist.com/kaffeeklatsch/2017/08/11/germanys-election-a-primer>.
315. James McBride, "What's at Stake in the German Elections?" Council on Foreign Relations, September 15, 2017, accessed August 6, 2019, <https://www.cfr.org/backgrounder/whats-stake-german-elections>.
316. "Agenten-Krimi um Merckels engsten Berater," Bild, November 19, 2017, accessed August 6, 2019, <https://www.bild.de/politik/inland/hacker/fuehren-deutschen-top-diplomaten-vor-53910162.bild.html#fromWall>.
317. "Dame auf P5," Der Spiegel 2017/47, November 18, 2017, accessed August 6, 2019, <http://magazin.spiegel.de/SP/2017/47/154353359/index.html>.
318. Toby Sterling, "Dutch-Russian 'tulips-for oil' trade suffers under crisis, sanctions," Reuters, January 16, 2015, accessed August 6, 2019, <https://www.reuters.com/article/us-netherlands-russia-trade/dutch-russian-tulips-for-oil-trade-suffers-under-crisis-sanctions-idUSKBNOKP1LO20150116>.
319. Tom Balmforth, "Attack on diplomat in Moscow deepens Dutch-Russian Drift," *The Guardian*, October 16, 2013, accessed August 7, 2019, <http://www.theguardian.com/world/2013/oct/16/moscow-assault-dutch-diplomat>.
320. BBC Staff, "MH17: Russia 'liable' for downing airliner over Ukraine," BBC News, May 25, 2018, accessed August 6, 2019, <http://www.bbc.com/news/world-europe-44252150>.
321. Andrew Callus, "'A bomb placed at heart of a political family': Emmanuel Macron launches bid for French president," *The Independent*, November 16, 2016, accessed August 8, 2019, <https://www.independent.co.uk/news/world/europe/emmanuel-macron-france-elections-latest-presidency-marine-le-pen-francois-hollande-nicolas-sarkozy-a7421821.html>
322. Cécile Barbière, "Emmanuel Macron officially enters the French presidential race," Euractiv, November 16, 2016, accessed August 8, 2019, <https://www.euractiv.com/section/elections/news/emmanuel-macron-officially-enters-the-french-presidential-race/>
323. "France-Russian Relations," Global Security, last updated February 9, 2017, accessed August 8, 2019, <http://www.globalsecurity.org/military/world/europe/fr-forrel-ru.htm>.
324. Romina McGuinness, "French politics rocked at latest poll shows nearly a quarter want LE PEN as president," Express, January 6, 2017, accessed August 8, 2019, <http://www.express.co.uk/news/world/751152/french-presidential-election-marine-le-pen-poll-results-macron-fillon-valls>.
325. Manuel Lafont Rapnoull & Jeremy Shapiro, "Macron's foreign policy: Claiming the tradition," Brookings Institution, May 8, 2017, accessed November 19, 2019, <https://www.brookings.edu/blog/order-from-chaos/2017/05/08/macrons-foreign-policy-claiming-the-tradition/>.

326. Cecile Barbieri, "Emanuel Macron officially enters the French presidential race," Euractiv, November 16, 2016, accessed August 8, 2019, <https://www.euractiv.com/section/elections/news/emmanuel-macron-officially-enters-the-french-presidential-race/>.
327. David E. Sanger, "The Hawk on Russia Policy? Hillary Clinton, Not Donald Trump," *The New York Times*, October 20, 2016, accessed August 7, 2019, <https://www.nytimes.com/2016/10/21/us/hillary-clinton-donald-trump-putin-russia.html>.
328. Clinton Ehrlich, "The Kremlin Really Believes That Hillary Wants to Start a War with Russia," *Foreign Policy*, September 7, 2016, accessed September 13, 2019, <https://foreignpolicy.com/2016/09/07/the-kremlin-really-believes-that-hillary-clinton-will-start-a-war-with-russia-donald-trump-vladimir-putin/>.
329. Malta Today Staff, "Updated | Malta condemns developments in Crimea PM to attend extraordinary EU summit," *Malta Today*, March 3, 2014, accessed August 7, 2019, <https://www.maltatoday.com.mt/news/national/36421/malta-in-brussels-condemns-developments-in-crimea-20140303>.
330. Kurt Sansone, "[WATCH] Russia hits back: 'Solution of Malta government is not friendly,'" *Malta Today*, April 18, 2019, accessed August 7, 2019, <https://www.maltatoday.com.mt/news/national/94427/watch-russia-hits-back-solution-of-malta-government-is-not-friendly>.
331. George Galloway, "Maltese Cross-Road: NATO could draw neutral Malta back to wars," *RT*, June 27, 2018, accessed August 7, 2019, <https://www.rt.com/op-ed/431008-malta-eu-muscat-nato/>.
332. Reuters, "CNN, Donna Brazile snap ties amidst renewed WikiLeaks controversy," *The Economic Times*, November 1, 2016, accessed August 7, 2019, <http://web.archive.org/web/20161103091943/http://economictimes.indiatimes.com/magazines/panache/cnn-donna-brazile-snap-ties-amid-renewed-wikileaks-controversy/articleshow/55181385.cms>.
333. Qurium, "Tracing the Source of MACRONGATE, the Macron Offshore Papers," *Qurium*, accessed August 7, 2019, https://www.qurium.org/alerts/france/tracing_macrongate_source/.
334. Selina Wang, "How the Kremlin Tried to Pose as American News Sites on Twitter," *Bloomberg*, December 5, 2017, accessed November 19, 2019, <https://www.bloomberg.com/news/articles/2017-12-05/how-the-kremlin-tried-to-pose-as-american-news-sites-on-twitter>.
335. Andrew Rettman, "Illicit Russian billions pose threat to EU democracy," *EU Observer*, April 21, 2017, accessed November 19, 2019, <https://euobserver.com/foreign/137631>; Matt Bradley, "Europe's Far-Right Enjoys Backing from Russia's Putin," *NBC News*, February 12, 2017, accessed November 19, 2019, <https://www.nbcnews.com/news/world/europe-s-far-right-enjoys-backing-russia-s-putin-n718926>.
336. Cynthia Kroet, "Russia spread fake news during Dutch election: report," *Politico*, April 4, 2017, accessed August 7, 2019, <http://www.politico.eu/article/russia-spread-fake-news-during-dutch-election-report-putin/>.
337. Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'" *Wired*, May 9, 2017, accessed August 6, 2019, <https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/>.
338. *United States of America v Viktor Borisovich Netyksho*, United States District Court for the District of Columbia, July 13, 2018, accessed August 7, 2019, <https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf>
339. Kim Zetter, "Software vendor may have opened a gap for hackers in 2016 swing state," *Politico*, June 5, 2019, accessed August 7, 2019, <https://www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582>;
340. "Report of the Select Committee on Intelligence of the United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S Election Volume 1: Russia Efforts Against Election Infrastructure with Additional Views," U.S. Select Committee on Intelligence, 116th Congress 1st Session, July 25, 2019, accessed August 7, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
341. Chloe Farand, "The Netherlands will count every vote by hand to stop hackers influencing parliamentary election," *The Independent*, February 2, 2017, accessed August 7, 2019, <http://www.independent.co.uk/news/world/europe/netherlands-parliamentary-election-count-vote-by-hand-stop-hackers-cyber-crime-fraud-hacking-a7558701.html>.
342. Dmitry Peskov, "Kremlin says cyber attacks against Russia perpetually initiated from U.S. territory," *TASS Russian News Agency*, February 27, 2019, accessed November 19, 2019, <https://tass.com/world/1046641>.

343. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, February 27, 2019, accessed November 19, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
344. David E. Sanger & Nicole Perloth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019, accessed November 19, 2019, <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.
345. Reuters, "Russia Thwarts U.S. Cyber Attacks on Its Infrastructure—News Agencies," *The Moscow Times*, June 17, 2019, accessed November 19, 2019, <https://www.themoscowtimes.com/2019/06/17/russia-uncovers-attempted-us-cyberattacks-on-its-infrastructure-ria-a66034>.
346. In the Matter of the Seizure of the Domain Name: Toknowall.com, United States District Court for the Western District of Pennsylvania, Magistrate No. 18-665, Case 2:18-mj-00665-LPL, May 23, 2018, accessed November 19, 2019, <http://www.kingpin.cc/wp-content/uploads/2018/05/pawd-2.18-mj-00665-1.pdf>.
347. Katherine Tweed, "Homeland Security: Russian Hackers Infiltrated U.S. Energy Infrastructure," Green Tech Media, November 11, 2014, accessed November 19, 2019, <https://www.greentechmedia.com/articles/read/dhs-russian-hackers-infiltrated-us-energy-infrastructure>.
348. ICS Alert (ICS-ALERT-14-281-01E Ongoing Sophisticated Malware Campaign Compromising ICS (Update E), U.S. Department of Homeland Security CISA, December 10, 2014, accessed November 19, 2019, <https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B>.
349. Sarah Rainsford, "Russia's Putin: U.S. agents gave direct help to Chechens," BBC News, April 27, 2015, accessed November 12, 2019, <https://www.bbc.com/news/world-europe-32487081>.
350. "Rare NATO-Russia talks address military drills, 1987 missile treaty," Reuters, October 31, 2019, accessed November 12, 2019, <https://www.reuters.com/article/us-nato-russia/rare-nato-russia-talks-address-military-drills-1987-missile-treaty-idUSKCN1N52RN>.
351. Ralph S. Clem, "NATO's Expanding Military Exercises Are Sending Risky Messages," War on the Rocks, October 10, 2017, accessed November 12, 2019, <https://warontherocks.com/2017/10/natos-expanding-military-exercises-are-sending-risky-mixed-messages/>.
352. Stratfor, "Russia Targets NATO with Military Exercises," *Forbes*, March 20, 2015, accessed November 12, 2019, <https://www.forbes.com/sites/stratfor/2015/03/20/russia-targets-nato-with-military-exercises/#741d562d6880>.
353. Ryan Browne, "Russia jammed GPS during major NATO military exercise with U.S. troops," CNN, November 14, 2018, accessed November 12, 2019, <https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html>.
354. Anna Wieslander, "What makes an ally? Sweden and Finland as NATO partners," Atlantic Council, April 1, 2019, accessed November 12, 2019, <https://www.atlanticcouncil.org/blogs/new-atlanticist/what-makes-an-ally-sweden-and-finland-as-nato-partners/>.
355. Erkki Bahovski, "Why Doesn't Finland Want to Join NATO?" RKK ICDS, March 27, 2015, accessed August 6, 2019, <https://icds.ee/why-doesnt-finland-want-to-join-nato/>.
356. Ida Männistö, "Could Fear of Another Russian Attack Impel Finland to Join NATO in the Near Future?" NATO Association of Canada, April 13, 2017, accessed August 7, 2019, <https://natoassociation.ca/could-fear-of-another-russian-attack-impel-finland-to-join-nato-in-the-near-future/>.
357. Julian Heissler, "Finland's Reluctance to Join NATO," Heinrich Boll Stiftung, July 12, 2018, accessed August 6, 2019, <https://us.boell.org/2018/07/12/finlands-reluctance-join-nato>.
358. YLE, "NATO-led military drills start on Finland's southern coast," YLE, June 6, 2016, accessed August 7, 2019, https://yle.fi/uutiset/osasto/news/nato-led_military_drills_start_on_finlands_southern_coast/8934380.
359. Su-Po 2016, Suojelu-Poliisi, 2016, accessed August 7, 2019, https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/72827_SUPO_2016_FIN.pdf?b67aaecd4eb2d488.
360. Stephen Blank, "As Kazakhstan Asserts Its Independence, How Will Russia React?" War on the Rocks, July 31, 2018, accessed November 19, 2019, <https://warontherocks.com/2018/07/as-kazakhstan-asserts-its-independence-how-will-russia-react/>.

361. "Relations with Kazakhstan," NATO, last updated March 26, 2019, accessed August 7, 2019, https://www.nato.int/cps/en/natohq/topics_49598.htm.
362. "Оно нам НАТО?," Eurasian News, August 18, 2017, accessed August 7, 2019, <https://web.archive.org/web/20171031142427/https://eurasianews.info/politika/ono-nam-nato.html>.
363. GReAT, "A Slice of 2017 Sofacy Activity," Kaspersky SecureList, February 20, 2018, accessed August 7, 2019, <https://securelist.com/a-slice-of-2017-sofacy-activity/83930/>.
364. Ministry of Defense of the Republic of Kazakhstan, "Kazakhstan hosts 'Steppe Eagle-2017' international peacekeeping exercise," Embassy of the Republic of Kazakhstan in the United Kingdom of Great Britain and Northern Ireland, October 10, 2017, accessed August 8, 2019, <http://mfa.gov.kz/en/london/content-view/kazakhstan-hosts-steppe-eagle-2017-international-peacekeeping-exercise>.
365. Richard Sokolsky, "The New NATO-Russia Military Balance," Implications for European Security," Carnegie Endowment for International Peace, March 13, 2017, accessed November 11, 2019, <https://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222>.
366. Jerome, "ATO Is Over, Military Takes Charge," Military Land, February 24, 2018, accessed August 7, 2019, <http://military-land.net/ukraine/ato-military-takes-charge/>.
367. "Old war, new rules: what comes next as ATO ends and a new operation starts in Donbas?" UA Crisis, May 4, 2018, accessed August 7, 2019, <http://uacrisis.org/66558-joint-forces-operation>.
368. "Poroshenko: ATO over, Joint Forces Operation starting," Unian Information Agency, March 16, 2018, accessed August 7, 2019, <https://www.unian.info/war/10045583-poroshenko-ato-over-joint-forces-operation-starting.html>.
369. "SBU thwarts cyber attack from Russia against chlorine station in Dnipropetrovsk region," Interfax-Ukraine, July 11, 2018, accessed August 5, 2019, <https://en.interfax.com.ua/news/general/517337.html>.
370. Office of Public Affairs, "Justice Department Announces Action to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," Department of Justice, May 23, 2018, accessed August 5, 2019, <https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected>.
371. "СБУ попереджає про можливу масштабну кібератаку на державні структури та приватні компанії напередодні фіналу Ліги Чемпіонів (відео)," Security Service of Ukraine, May 23, 2018, accessed August 5, 2019, <https://ssu.gov.ua/ua/news/1/category/1/view/4823#.KuFdXQG9.dpbs>
372. "SBU thwarts cyber attack from Russia against chlorine station in Dnipropetrovsk region," Interfax-Ukraine, July 11, 2018, accessed August 5, 2019, <https://en.interfax.com.ua/news/general/517337.html>.
373. William Largent, "New VPNFilter malware targets at least 500K networking devices worldwide," Cisco Talos, May 23, 2018, accessed August 5, 2019, <https://blog.talosintelligence.com/2018/05/VPNFilter.html>.
374. "Cyber Actors Target Home and Office Routers and Networked Devices Worldwide," CISA, last modified June 7, 2018, accessed August 16, 2019, <https://www.us-cert.gov/ncas/alerts/TA18-145A>.
375. Alert TA-18-106A "Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices," U.S.-CERT, April 16, 2018, last modified April 20, 2018, accessed August 5, 2019, <https://www.us-cert.gov/ncas/alerts/TA18-106A>.
376. Symantec Security Response Team, "VPNFilter: New Router Malware with Destructive Capabilities," Symantec, May 23, 2018, updated September 26, 2018, accessed August 5, 2019, <https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware>.
377. "SBU thwarts cyber attack from Russia against chlorine station in Dnipropetrovsk region," Interfax-Ukraine, July 11, 2018, accessed August 5, 2019, <https://en.interfax.com.ua/news/general/517337.html>.
378. "«Дніпроазот» на невизначений час зупинив роботу через дорожнечу газу," Radio Svoboda, June 19, 2018, accessed August 5, 2019, <https://www.radiosvoboda.org/a/news/29304556.html>; "Місто Дніпро і прилеглі райони можуть залишитись без води, якщо до завтра «не доїде» хлор – заява," Radio Svoboda, July 16, 2018, accessed August 5, 2019, <https://www.radiosvoboda.org/a/news/29368368.html>.
379. RFE/RL, "UN Warns of Possible Threat of Chemical Disaster In Eastern Ukraine," Radio Free Europe/Radio Liberty, March 11, 2017, accessed August 7, 2019, <https://www.rferl.org/a/ukraine-chemical-disaster-threat-un-osce/28363404.html>;

380. Wim Zwijnenburg, "Water Filtration Plans and Risk of a Chlorine Mass-Casualty Event in Donetsk," Bellingcat, March 10, 2017, accessed August 7, 2019, <https://www.bellingcat.com/resources/case-studies/2017/03/10/water-filtration-plants-risks-chlorine-mass-casualty-event-donetsk/>.
381. Illia Ponomarenko, "OSCE demands cease-fire near vital Donetsk water plant after fresh shelling," Kyiv Post, May 19, 2018, accessed August 7, 2019, <https://www.kyivpost.com/ukraine-politics/osce-urges-immediate-ceasefire-near-vital-donetsk-filtration-station-fresh-shelling.html>.
382. "Кто стоит за информационной атакой на ООО «АХПС» - позиция коллектива и правозащитников (ФОТО)," МОСТ, June 20, 2018, accessed August 5, 2019, https://web.archive.org/web/20190605154258/https://most-dnepr.info/news/press/162353_stoit_informatsionnoy_atakoy.htm.
383. "Statement re. alleged SBU investigation concerning Lyudyla Kozlovska (updated 26.11.2018)," Open Dialogue, October 12, 2018, accessed November 19, 2019, <https://en.odfoundation.eu/a/8916,statement-re-alleged-sbu-investigation-concerning-lyudmyla-kozlovska-updated-26-11-2018>.
384. Олександр Курбатов, «Стоп корупції»: спадкова хвороба, Detektor Media, March 6, 2019, accessed November 19, 2019, <https://detector.media/community/article/163854/2019-03-06-stop-koruptsii-spadkova-khvoroba/>.
385. Місто Дніпро і прилеглі райони можуть залишитись без води, якщо до завтра «не доїде» хлор – заява," Radio Svoboda, July 16, 2018, accessed August 5, 2019, <https://www.radiosvoboda.org/a/news/29368368.html>; Illia Ponomarenko,
386. Barbara Surk, "Bosnia's Election Exacerbates Old Divisions, to Russia's Satisfaction," *The New York Times*, October 6, 2018, accessed August 8, 2019, <https://www.nytimes.com/2018/10/06/world/europe/bosnia-election-dodik-putin.html>.
387. "Russian FM Lavrov supports resumption of flights to Georgia as Georgians 'realised consequences' of June 20," Agenda. Ge, September 26, 2019, accessed November 19, 2019, <https://agenda.ge/en/news/2019/2582>.
388. "Bilateral meeting with the Minister of Defence of Georgia," NATO, last modified October 25, 2019, accessed December 10, 2019, https://www.nato.int/cps/en/natohq/photos_169927.htm.
389. "Massive cyberattack affects thousands of websites in Georgia," Al Jazeera, October 28, 2019, accessed December 10, 2019, <https://www.aljazeera.com/news/2019/10/massive-cyberattack-affects-thousands-web-sites-georgia-191028183426733.html>
390. "To join NATO, Georgia will have to legalize gay relationship," EUvsDisinfo, October 24, 2019, accessed December 10, 2019, <https://euvsdisinfo.eu/report/stoltenberg-demanded-georgia-to-legalize-gay-relationships-as-an-accession-criteria/>
391. "Religious Belief and National Belonging in Central and Eastern Europe," Pew Research Center, May 10, 2017, accessed December 10, 2019, <https://www.pewforum.org/2017/05/10/social-views-and-morality/>.
392. "Cyber-attack knocks out Georgian websites, comes with a surprise," Atlantic Council's Digital Forensic Research Lab, November 19, 2019, accessed December 10, 2019, <https://medium.com/dfrlab/cyber-attack-knocks-out-georgian-websites-comes-with-a-surprise-93aade6e6179>
393. Lolita C. Baldor, "Mattis condemns Russian influence-peddling in Macedonia," Military Times, September 17, 2018, accessed September 16, 2019, <https://www.militarytimes.com/news/your-military/2018/09/17/mattis-condemns-russian-influence-peddling-in-macedonia/>.
394. Arkady Dubnov, "Reflecting on a Quarter Century of Russia's Relations with Central Asia," The Carnegie Endowment for International Peace, April 19, 2018, accessed August 7, 2019, <https://carnegieendowment.org/2018/04/19/reflecting-on-quarter-century-of-russia-s-relations-with-central-asia-pub-76117>.
395. Paul Stronski, "China and Russia's Uneasy Partnership in Central Asia," The Carnegie Endowment for International Peace, March 29, 2018, accessed August 8, 2019, <https://carnegieendowment.org/2018/03/29/china-and-russia-s-uneasy-partnership-in-central-asia-pub-75984>.
396. Mariusz Marszewski & Krzysztof Strachota, "Russia's ostentatious return to Uzbekistan," October 24, 2018, accessed August 8, 2019, <https://www.osw.waw.pl/en/publikacje/analyses/2018-10-24/russias-ostentatious-return-to-uzbekistan>.
397. "Russia and Uzbekistan strengthen ties as Putin pays state visit," France24, October 19, 2018, accessed August 8, 2019, <https://www.france24.com/en/20181019-russia-uzbekistan-strengthen-ties-putin-pays-state-visit>.
398. "Uzbekistan and Russia: Chilly weather, warm relations," Eurasianet, October 17, 2018, accessed August 8, 2019, <https://eurasianet.org/uzbekistan-and-russia-chilly-weather-warm-relations>.

399. Gilbert Rozman, "The Russian Pivot to Asia," *The Asan Forum*, December 1, 2014, accessed August 8, 2019, <http://www.theasanforum.org/the-russian-pivot-to-asia/>.
400. Xuan Loc Doan, "U.S., Vietnam strategic partners in all but name," *Asia Times*, April 10, 2019, accessed November 19, 2019, <https://www.asiatimes.com/2019/04/opinion/us-vietnam-strategic-partners-in-all-but-name/>.
401. Prashanth Parameswaran, "Vietnam-Russia Military Ties: Look Beyond the Billion Dollar Boast," *The Diplomat*, September 11, 2018, accessed August 8, 2019, <https://thediplomat.com/2018/09/vietnam-russia-military-ties-look-beyond-the-billion-dollar-boast/>.
402. Beba Cibralic & Aaron L. Connelly, "Russia's disinformation game in Southeast Asia," *The Interpreter*, The Lowly Institute, July 23, 2018, accessed August 8, 2019, <https://www.lowyinstitute.org/the-interpreter/russias-disinformation-game-southeast-asia>.
403. Владимир Винокуров, "Арктика – к сотрудничеству или противостоянию?," Независимой газеты, April 19, 2019, accessed August 8, 2019, http://nvo.ng.ru/concepts/2019-04-19/1_1042_arctic.html.
404. Jeff Desjardins, "This infographic shows how gigantic the Arctic's undiscovered oil reserves might be," *Business Insider*, April 7, 2016, accessed August 8, 2019, <https://www.businessinsider.com/how-gigantic-arctics-undiscovered-oil-reserves-might-be-2016-4>.
405. Submission by the Kingdom of Denmark: "Outer limits of the continental shelf beyond 200 nautical miles from the baselines," Commission on the Limits of the Continental Shelf, Division for Ocean Affairs and the Law of the Sea, United Nations, last updated November 2, 2015, accessed August 8, 2019, https://www.un.org/depts/los/clcs_new/submissions_files/submission_dnk_76_2014.htm
406. Mary Thompson-Jones, "NATO's Arctic Exercise Is a Good Start to Standing Up to Russian Militarization of the High North," *National Interest*, November 6, 2018, accessed August 8, 2019, <https://nationalinterest.org/blog/buzz/natos-arctic-exercise-good-start-standing-russian-militarization-high-north-35367>.
407. Валерий ГЕРАСИМОВ, "Векторы развития военной стратегии," March 4, 2019, accessed November 19, 2019, <http://redstar.ru/vektory-razvitiya-voennoj-strategii/>.
408. Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *Crowdstrike Blog*, June 15, 2016, accessed November 19, 2019, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.
409. "U.S. spooks scour China's 5-year plan for hacking clues," *Financial Times*, November 25, 2015, accessed November 19, 2019, <https://www.ft.com/content/40dc895a-92c6-11e5-94e6-c5413829caa5>.
410. Bob Sobczak, "The inside story of the world's most dangerous malware," *E&E News*, March 7, 2019, accessed September 17, 2019, <https://www.eenews.net/stories/1060123327>
411. Alexander Kimburg, "The Darkening Web," Penguin, 2017, accessed August 2, 2019 via https://books.google.com/books?id=pEcsDwAAQBAJ&pg=PA247&lpg=PA247&dq=%22havex%22+AND+%22thysenkrupp%22&source=bl&ots=h-pSSdMGPbD&sig=ACfU3U0ZRc1yKuiU8LJS4eV5i8-mzxbRWA&hl=en&sa=X&ved=2ahUKewi57_HVibXiAhWPvt8KHebbB0oQ6AEwCXoECAkQAQ#v=onepage&q=%22havex%22%20AND%20%22thysenkrupp%22&f=false.
412. Richard Sale, "German Steel Mill Attack: Inside Job," *Industrial Safety and Security Source*, September 9, 2015, accessed August 2, 2019, <https://www.isssource.com/german-steel-mill-attack-inside-job/>; Michael Riley & Jordan Robertson, "Cyberspace Becomes Second Front In Russia's Clash with NATO," *Bloomberg*, October 14, 2015, accessed August 2, 2019, <http://web.archive.org/web/20190513213151/http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato>;
413. Rob Knake, "The Next Cyber Battleground," *Foreign Affairs*, July 19, 2018, accessed August 2, 2019, <https://www.foreignaffairs.com/articles/north-america/2018-07-19/next-cyber-battleground?cid=soc-tw&pgtype=hpg>
414. Die Lage Der IT-Sicherheit In Deutschland, Bundesamt für Sicherheit in der Informationstechnik, 2014, accessed August 2, 2019, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.
415. Office of Public Affairs, "Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," May 23, 2018, accessed August 22, 2019, <https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected>.

416. "APT28: A Window into Russia's Cyber Espionage Operations," FireEye, October 27, 2014, accessed August 21, 2019, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>.
417. Security Response Attack Investigation Team, "APT28: New Espionage Operations Target Military and Government Organizations," Symantec, October 4, 2018, accessed August 21, 2019, <https://www.symantec.com/blogs/election-security/apt28-espionage-military-government>.
418. Martin Lee, "One year later: The VPNFilter catastrophe that wasn't," Cisco Talos, May 23, 2019, accessed August 22, 2019, <https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html>.
419. Office of Public Affairs, "Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," U.S. Department of Justice, May 23, 2018, accessed August 21, 2019, <https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected>.
420. "En Route with Sednit," ESET We Live Security, October 2016, accessed August 21, 2019, <https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-full.pdf>.
421. GReAT, "Sofacy APT this high profile targets with updated toolset," Kaspersky SecureList, December 4, 2015, accessed August 21, 2019, <https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/>.
422. Robert Falcone & Bryan Lee, "New Sofacy Attacks Against U.S. Government Agency," PaloAlto Networks Unit42, June 14, 2016, accessed August 21, 2019, <https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/>.
423. Jarkko, "Sofacy Recycles Carberp and Metasploit Code," F-Secure, August 9, 2015, accessed August 22, 2019, <https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/>.
424. "Pawn Storm Espionage Attacks Use Decoys, Deliver SEDNIT," Trend Micro, October 22, 2014, accessed August 21, 2019, <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/pawn-storm-espionage-attacks-use-decoys-deliver-sednit>.
425. "From Espionage to Cyber Propaganda: Pawn Storm's Activities over the Past Two Years," Trend Micro, April 25, 2017, accessed August 22, 2019, <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm>.
426. Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike Blog, June 15, 2016, accessed August 21, 2019, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.
427. Editorial Team, "Who is Fancy Bear (APT28)," CrowdStrike Blog, February 12, 2019, accessed August 22, 2019, <https://www.crowdstrike.com/blog/who-is-fancy-bear/>.
428. SecureWorks Counter Threat Unit Threat Intelligence, "IRON TWILIGHT Supports 'Active Measures,'" SecureWorks, March 30, 2017, accessed August 21, 2019, <https://www.secureworks.com/research/iron-twilight-supports-active-measures>.
429. SecureWorks Counter Threat Unit Threat Intelligence, "Threat Group 4127 Targets Hillary Clinton Presidential Campaign," June 16, 2016, accessed September 16, 2019, <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>.
430. Microsoft Defender ATP Research Team, "Microsoft Security Intelligence Report: Strontium," Microsoft Security, November 16, 2015, accessed August 21, 2019, <https://www.microsoft.com/security/blog/2015/11/16/microsoft-security-intelligence-report-strontium/>.
431. Internet Security Threat Report, Volume 22, Symantec, April 2017, accessed September 16, 2019, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>.
432. Cyber Advisory, SnakeMackerel: A Brexit-themed lure document that delivers ZEKAPAB malware, Accenture, 2019, accessed September 16, 2019, https://www.accenture.com/t20181129t203820z__w__us-en/_acnmedia/pdf-90/accenture-snake-mackerel-delivers-zekapab-malware.pdf.
433. Jonathan Leathery, "Microsoft Office Zero-Day CVE-2015-2424 Leveraged by Tsar Team, iSIGHTPARTNERS, July 15, 2015, accessed September 16, 2019, <https://web.archive.org/web/20150720101843/http://www.isightpartners.com/2015/07/microsoft-office-zero-day-cve-2015-2424-leveraged-by-tsar-team/>.

434. Kaspersky Lab ICS CERT, "GreyEnergy's overlap with Zebrocy," Kaspersky Lab SecureList, January 24, 2019, accessed September 16, 2019, <https://securelist.com/greyenergys-overlap-with-zebrocy/89506/>.
435. Bryan Lee & Robert Falcone, "Dear Jooohn: The Sofacy Group's Global Campaign," Palo Alto Networks Unit 42, <https://unit42.paloaltonetworks.com/dear-jooohn-sofacy-groups-global-campaign/>.
436. ESET Research, "Sednit: What's going on with Zebrocy?" ESET WeLiveSecurity, November 20, 2018, accessed September 16, 2019, <https://www.welivesecurity.com/2018/11/20/sednit-whats-going-zebrocy/>.
437. John Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks," FireEye, January 7, 2016, accessed August 20, 2019, <https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html>.
438. "BlackEnergy and Quedagh," F-Secure, September 25, 2014, accessed August 20, 2019, https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.
439. Sandworm Team, MITRE ATT&CK, accessed August 21, 2019, <https://attack.mitre.org/groups/G0034/>.
440. William Gamazo Sanches, "Timeline of Sandworm Attacks," Trend Micro Security Intelligence Blog, November 10, 2014, accessed August 21, 2019, <https://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/>.
441. Weimin Wu, "An Analysis of Windows Zero-Day Vulnerability 'CVE-2014-4114' aka 'Sandworm,'" Trend Micro Security Intelligence Blog, October 14, 2014, accessed August 21, 2019, https://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-windows-zero-day-vulnerability-cve-2014-4114-aka-sandworm/?_ga=2.212675284.1566323956.1566325804-1836814934.1563295694.
442. Udi Shamir, "Analyzing a New Variant of BlackEnergy 3," SentinelOne, June 2017, accessed August 21, 2019, https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf.
443. Anton Cherepanov & Robert Lipovsky, "New TeleBots backdoor: First evidence linking Industroyer to NotPetya," ESET We Live Security, October 11, 2018, accessed August 21, 2019, <https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/>.
444. Joint Analysis Report "Grizzly Steppe—Russian Malicious Cyber Activity," Department of Homeland Security, Federal Bureau of Investigation, JAR-16-20296A, December 29, 2016, accessed August 2, 2019, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.
445. GReAT, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents," Kaspersky Lab SecureList, January 28, 2016, accessed August 20, 2019, <https://usa.kaspersky.com/resource-center/threats/blackenergy>.
446. Anton Cherepanov, "The rise of TeleBots: Analyzing disruptive KillDisk attacks," ESET We Live Security, December 13, 2016, accessed August 20, 2019, <https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/>.
447. Kurt Baumgartner & Maria Garnaeva, "BE2 custom plugins, router abuse, and target profiles," Kaspersky SecureList, November 3, 2014, accessed August 21, 2019, <https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/>.
448. Robert Lipovsky & Anton Cherepanov, "BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry," ESET We Live Security, January 4, 2016, accessed August 21, 2019, <https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/>.
449. Robert Lipovsky, "Back in BlackEnergy*: 2014 Targeted Attacks in Ukraine and Poland," ESET We Live Security, September 22, 2014, accessed August 21, 2019, <https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/>.
450. "BLACKENERGY & QUEDAGH," F-Secure, September 2014, accessed August 21, 2019, https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.
451. Adam Meyers, "CrowdStrike's January Adversary of the Month: VOODOO BEAR," CrowdStrike Blog, January 29, 2018, accessed August 21, 2019, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-vooodoo-bear/>.
452. Raphael Satter, "Another Fancy Fumble?," Medium, August 27, 2018, accessed August 21, 2019, <https://medium.com/@rsatter/another-fancy-fumble-832c177ceb04>.
453. Threat Group Cards: A Threat Actor Encyclopedia," ThaiCERT, June 18, 2019, accessed August 21, 2019, <https://www.scribd.com/document/419048817/A-Threat-Actor-Encyclopedia>.

454. Anton Cherepanov & Robert Lipovsky, "New TeleBots backdoor: First evidence linking Industroyer to NotPetya," ESET We Live Security, October 11, 2018, accessed August 21, 2019, <https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/>.
455. "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," Dragos, June 13, 2017, accessed August 21, 2019, <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf>.
456. Anton Cherepanov & Robert Lipovsky, "GreyEnergy: Updated arsenal of one of the most dangerous threat actors," ESET We Live Security, October 17, 2018, accessed August 21, 2019, <https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/>.
457. GReAT, "Hades, the actor behind Olympic Destroyer is still alive," Kaspersky SEcureList, June 19, 2018, accessed August 21, 2019, <https://securelist.com/olympic-destroyer-is-still-alive/86169/>.
458. "New Strain of Olympic Destroyer Droppers," Check Point Research, November 15, 2018, accessed August 31, 2019, <https://research.checkpoint.com/new-strain-of-olympic-destroyer-droppers/>.
459. Ellen Nakashima, "Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say," *The Washington Post*, February 24, 2018, accessed August 21, 2019, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.
460. "En Route with Sednit," ESET, October 2016, accessed August 22, 2019, <https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-full.pdf>.
461. Bryan Lee et al., "Sofacy Attacks Multiple Government Entities," Palo Alto Networks Unit 42, February 28, 2018, accessed August 23, 2019, <https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/>.
462. Security Response Attack Investigation Team, "APT28: New Espionage Operations Target Military and Government Organizations," Symantec, October 4, 2018, accessed August 23, 2019, <https://www.symantec.com/blogs/election-security/apt28-espionage-military-government>.
463. "APT28: At the Center of the Storm," FireEye, January 2017, accessed August 23, 2019, <https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf>.
464. "APT28: A Window Into Russia's Cyber Espionage Operations?" FireEye, October 27, 2014, accessed August 21, 2019, <https://www2.fireeye.com/rs/fireeye/images/rpt-apt28.pdf>.
465. GReAT, "Zebrocy's Multilanguage Malware Salad," Kaspersky Lab SecureList, June 3, 2019, accessed September 16, 2019, <https://securelist.com/zebrocys-multilanguage-malware-salad/90680/>.
466. "Snakemackerel," Accenture Security, 2018, accessed August 23, 2019, https://www.accenture.com/t20181129t203820z__w__us-en/_acnmedia/pdf-90/accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50.
467. Kurt Baumgartner, "MASHA AND THESE BEARS," Kaspersky Lab, YouTube, April 25, 2018, accessed September 16, 2019, https://youtu.be/-7RM_jqSf9I?t=872.
468. "Software: CHOPSTICK, SPLM, ...," ATT&CK: Adversarial Tactics, Techniques & Common Knowledge, last modified August 3, 2016, accessed August 22, 2019, <https://attack.mitre.org/wiki/Software/S0023>.
469. "APT28: At the Center of the Storm," FireEye, January 2017, accessed August 23, 2019, <https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf>.
470. Lambert Sun et al., "Pawn Storm Update," Trend Micro, February 4, 2015, accessed September 16, 2019, <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/>.
471. "Trojan.Shunnael," Symantec Security Center, last updated June 25, 2016, accessed September 16, 2019, <https://www.symantec.com/security-center/writeup/2015-062518-5557-99>.
472. Graham Cluley, "Lifting the lid on Sednit: A closer look at the software it uses," ESET We Live Security, October 25, 2016, accessed September 16, 2019, <https://www.welivesecurity.com/2016/10/25/lifting-lid-sednit-closer-look-software-uses/>.
473. Robert Falcone & Bryan Lee, "Sofacy Continues Global Attacks and Wheels Out New 'Cannon' Trojan," Palo Alto Networks Unit 42, November 20, 2018, accessed August 23, 2019, <https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/>.

474. "Operation Pawn Storm: Using Decoys to Avoid Detection," TrendMicro, October 23, 2014, accessed August 22, 2019, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf>.
475. Bryan Lee & Rob Downs, "A Look Into Fysbis: Sofacy's Linux Backdoor," Palo Alto Networks Unit 42, February 12, 2016, accessed August 23, 2019, <https://unit42.paloaltonetworks.com/a-look-into-fysbis-sofacys-linux-backdoor/>.
476. Coreshell, MITRE ATT&CK, accessed August 23, 2019, <https://attack.mitre.org/software/S0137/>.
477. "Lojax: First UEFI rootkit found in the wild, courtesy of the Sednit group," ESET Research White papers, September 2018, accessed August 23, 2019, <https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-Lojax.pdf>.
478. Ryan Sherstobitoff & Jessica Saavedra-Morales, "Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victim's Systems," McAfee, February 2, 2018, accessed August 23, 2019, <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems>.
479. Robert Lipovsky, "Back in BlackEnergy*: 2014 Targeted Attacks in Ukraine and Poland," ESET We Live Security, September 22, 2014, accessed August 23, 2019, <https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/>;
480. Joe Stewart, "BlackEnergy Version 2 Threat Analysis," Secureworks, March 3, 2010, accessed August 23, 2019, <https://www.secureworks.com/research/blackenergy2>.
481. "Crashoverride: Analysis of the Threat to Electric Grid Operations," Dragos, June 13, 2017, accessed August 23, 2019, <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf?hsCtaTracking=ec040772-a407-4187-bd1d-e750cb8e1d99%7Ced3e20a3-1321-4fad-b91b-d19eb25b2350>.
482. In the Matter of the Seizure of the Domain Name: Toknowall.com, United States District Court for the Western District of Pennsylvania, Case 2:18-mj-00554-LPL, May 23, 2018, Magistrate No. 18-665, accessed September 16, 2019, <http://www.kingpin.cc/wp-content/uploads/2018/05/pawd-2.18-mj-00665-1.pdf>.
483. Anton Cherepanov, "GreyEnergy: A Successor to Black Energy," ESET We Live Security, October 2018, accessed August 23, 2019, https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf.
484. Swapnil Patil, "Microsoft Office Vulnerabilities Used to Distribute FELIXROOT Backdoor in Recent Campaign," FireEye, July 26, 2018, accessed August 23, 2019, <https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html>.
485. Anton Cherepanov, "WIN32/INDUSTROYER: A new threat for industrial control systems," ESET We Live Security, June 12, 2017, accessed August 23, 2019, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
486. Anton Cherepanov & Robert Lipovsky, "New TeleBots backdoor: First evidence linking Industroyer to NotPetya," ESET We Live Security, October 11, 2018, accessed August 23, 2019, <https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/>.
487. William Largent, "New VPNFilter malware targets at least 500K networking devices worldwide," Cisco Talos, May 23, 2018, accessed August 23, 2019, <https://blog.talosintelligence.com/2018/05/VPNFilter.html>.
488. Anton Cherepanov, "The rise of TeleBots: Analyzing disruptive KillDisk attacks," ESET We Live Security, December 13, 2016, accessed August 22, 2019, <https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/>.
489. Anton Cherepanov, "Analysis of TeleBots' cunning backdoor," ESET We Live Security, July 4, 2017, accessed August 2, 2019, <https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/>.
490. Anton Cherepanov, "XData ransomware making rounds amid global WannaCryptor scare," ESET We Live Security, May 23, 2017, accessed August 23, 2019, <https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/>.
491. Anton Cherepanov, "TeleBots are back: Supply-chain attacks against Ukraine," ESET We Live Security, June 30, 2017, accessed August 23, 2019, <https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/>.
492. Anton Ivanov & Fedor Sinitsyn, "PetrWrap: the new Petya-based ransomware used in targeted attacks," Kaspersky SecureList, March 14, 2017, accessed August 23, 2019, <https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762/>.

493. Alexander Chiu, "New Ransomware Variant 'Nyetya' Compromises Systems Worldwide," June 27, 2017, accessed August 23, 2019, <https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html>.
494. Alex Perekalin, "Bad Rabbit: A new ransomware epidemic is on the rise," Kaspersky Daily, October 26, 2017, accessed August 23, 2019, <https://usa.kaspersky.com/blog/bad-rabbit-ransomware/13106/>.
495. David Maynor et al., "The MeDoc Connection," Cisco Talos, July 5, 2017, accessed August 23, 2019, <https://blog.talosintelligence.com/2017/07/the-medoc-connection.html>.
496. Orkhan Mamedov et al., "Bad Rabbit ransomware," Kaspersky SecureList, October 24, 2017, accessed August 23, 2019, <https://securelist.com/bad-rabbit-ransomware/82851/>.
497. "Is CyberBerkut the new Russian proxy?" Secu(Insight), June 12, 2014, accessed August 23, 2019, <https://web.archive.org/web/20150222102028/http://www.secuinsight.fr/2014/06/12/is-cyberberkut-the-new-russian-proxy/>.
498. Chris Bing, "Russian hacker group 'CyberBerkut' returns to public light with allegations against Clinton," CyberScoop, July 12, 2017, accessed August 23, 2019, <https://www.cyberscoop.com/cyberberkut-returns-hillary-clinton/>.
499. CyberBerkut, last updated January 10, 2018, accessed August 23, 2019, <https://cyber-berkut.org/en/>.
500. Russia Military Power, Defense Intelligence Agency, 2017, accessed August 23, 2019, <https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf>.
501. ThreatConnect Research Team, "Russia Cyber Operations on Steroids," Threat Connect, August 19, 2016, accessed August 26, 2019, <https://threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/>.
502. Kevin Collier, "Real Hacked Files Include Faked Clinton Campaign 'Corruption,'" Voactiv, November 3, 2016, accessed September 23, 2019, <https://www.vocativ.com/372088/bradley-foundation-hack-clinton-campaign-fake-files/index.html>.
503. Joseph Cox, "Dodgy 'Hackers' Target Bellingcat Investigators Who Call BS on Moscow," The Daily Beast, March 13, 2018, accessed August 26, 2019, <https://www.thedailybeast.com/polish-hackers-target-investigators-who-call-bs-on-moscow?ref=scroll>.
504. Scott Shane, "The Fake Americans Russia Created to Influence the Election," *The New York Times*, September 7, 2017, accessed September 9, 2019, <https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html>.
505. "World Anti-Doping Agency Site Hacked; Thousands of Accounts Leaked," HackRead, August 12, 2016, accessed August 26, 2019, https://www.hackread.com/world-anti-doping-agency-site-hacked/?_ga=2.11279415.261315967.1566827080-1375313466.1566574045.
506. Hamza Shaban, "Twitter suspends Guccifer and DCLeaks after Mueller links them to Russian hacking operation," *The Washington Post*, July 16, 2018, accessed August 26, 2019, <https://www.washingtonpost.com/technology/2018/07/16/twitter-suspends-guccifer-dcleaks-after-mueller-links-them-russian-hacking-operation/>.
507. Michael Riley, "Russian Hackers of DNC Said to Nab Secrets From NATO, Soros, Bloomberg, August 11, 2016, accessed August 26, 2019, <https://www.bloomberg.com/news/articles/2016-08-11/russian-hackers-of-dnc-said-to-scoop-up-secrets-from-nato-soros>.
508. Makena Kelly, "Seven Russian hackers charged with hacking anti-doping organizations," The Verge, October 4, 2018, accessed August 26, 2019, <https://www.theverge.com/2018/10/4/17936442/russian-hackers-charged-hacking-anti-doping-mo-farah>.
509. "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Department of Justice, October 4, 2018, accessed September 9, 2019, <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and>.
510. "Хакеры взломали все сайты медиагруппы «Интер»," Golos Pravdy, October 25, 2015, accessed August 26, 2019, <https://golospravdy.eu/xakery-vzlomali-vse-sajty-mediagruppy-inter/>.
511. Dan Lamothe, "U.S. joins other nations in accusing Russia of cyber attack in Republic of Georgia," Washington Post, February 20, 2020, accessed February 27, 2020.
512. Warren Mercer, Paul Rascagneres and Vitor Ventura, "Cyber Conflict" Decoy Document Used In Real Cyber Conflict," Cisco, October 22, 2017, accessed March 1, 2017, <https://blogs.cisco.com/security/talos/cyber-conflict-decoy-document>

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that— together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

For more information, please contact:

cyberinfo@bah.com