2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

The Past, Present, and Future of Russia's Cyber Strategy and Forces

Bilyana Lilly
Policy Researcher
Pardee RAND Graduate School
RAND Corporation
Santa Monica, CA, United States
blilly@rand.org

Joe Cheravitch
Defense Analyst
Defense and Political Sciences
RAND Corporation
Arlington, VA, United States
jcheravi@rand.org

Abstract: Russian cyberattacks against military and civilian infrastructure in the West have become a persistent challenge. Despite the importance of this topic and the excellent scholarship already published on these issues, there is a need for more detailed data and analysis on the role of cyberattacks in Russia's security strategy and its reflection in the evolution of Russia's cyber forces. A better understanding of Russia's strategy and cyber actors, particularly the growing role of the military in these issues, can facilitate an improvement in Western governments' policies to defend against future Russian activity. To address this issue, this article will outline the role of information and cyber operations in Russia's information warfare doctrine and will analyze the recruitment efforts and modus operandi of Russia's cyber departments, particularly psychological and cyber operations units within military intelligence. The paper will conclude by examining the likely future of Russia's behavior in cyberspace and how various state-sponsored actors might influence it. The paper asserts that although Russia's doctrine suggests a defensive and cooperative posture in response to threats in the information space, officials' promulgations and military literature reveal a predilection for the development of offensive cyber capabilities and operations, which are shaped by Russia's threat perceptions and doctrine, and the institutional cultures of the departments within the military conducting them.

Keywords: *Russia, cyber, cyber strategy, information warfare, information operations, FSB, GRU*

This paper represents independent work by the authors and does not represent the views of the RAND Corporation.

1. INTRODUCTION

Cyber operations attributed to Moscow are not conducted in a strategic vacuum. They are enabled and shaped by broader geopolitical considerations and the institutional culture of Russia's military, intelligence, and political leadership, as well as by Moscow's evolving approach to asymmetric interstate competition that falls short of all-out conflict. To understand the motivations behind and the constraints of Russia's use of cyber and information operations against perceived adversaries, decision-makers must thoroughly study existing policy and doctrine, particularly its evolution from the immediate post-Soviet period until now, while at the same time striving to attain a more sophisticated comprehension of the actors responsible for executing cyberattacks and digital influence campaigns. This involves research into Russian publications and official documents and more nuanced and updated investigations into the actors behind these efforts, which is now possible in the wake of key Russian campaigns, such as the 2016 effort to undermine the U.S. presidential election, that have generated an unprecedented amount of public information on specific units and personalities. Such investigations can help gird the international community against future operations, while assisting policymakers in determining the viability and course of cyber diplomacy and deterrence.

This article aims to show that there is more continuity than contrast between Russian cyber perspectives and practice. Russia's cyber posture, nested in Russia's concept of information warfare, is reflected in the offensive cyber operations launched by Russian government departments, whose institutional culture, expertise, and modus operandi have affected and will continue to affect Russia's cyber signature. This article reviews a combination of Russian primary and secondary open sources, scholarship of international researchers, and information available through online and traditional media. This article is further informed by an examination of modern publications, historical accounts, and unique, previously unpublished sources.

2. RUSSIA'S DOCTRINE AND STRATEGY ON CYBER SECURITY

A. A Shift in Russia's Understanding of Warfare

Over the past two decades, Russia's military and political leadership has undergone a fundamental modification of its conception of warfare and the role of cyber operations in this evolving view. Various scholars, such as Timothy Thomas, Martti J. Kari, Keir Giles, Oscar Jonsson, Brandon Valeriano, Benjamin Jensen, Ryan Maness, Stephen Blank, and Katri Pynnöniemi, have published seminal works in which they have analyzed various nuances of these dynamics (Thomas 2019; Kari 2019; Giles 2016;

Jonsson 2019; Jensen, Valeriano, and Maness 2019; Blank 2017; Kari and Pynnöniemi 2019; Medvedev 2015).[1] This section expounds this literature and serves as a reference guide to understand the trajectory of Russian cyber doctrine, cyber literature, and the assumptions that underpin them. It lays the foundation for the subsequent analysis on the evolution of Russia's cyber forces, which highlights the parallels between the existing doctrine and the Russian military scientific literature on one hand, and the organizational culture of Russia's main cyber departments and the nature of Russia's cyber operations on the other.

Russia's conceptualization of warfare has shifted from a general consensus that the baseline of warfare is armed violence to an agreement that the baseline for warfare has broadened to include a tailored amalgamation of armed violence and non-military measures (Chekinov and Bogdanov 2015a, 34; Chekinov and Bogdanov 2015b, 43; Jonsson 2019, 3–5; Gerasimov 2013; Burenok 2018, 61–66). Understanding these evolving nuances of Russia's military outlook is critical to Western decision-makers because the variation in the thinking of warfare between Moscow and the West also entails differences in understanding foreign policy signals and levers. Such differences may have wide-ranging consequences for deterring Russia and understanding Russia's red lines, and for facilitating the creation of a long-term strategy that addresses the causes of Russia's behavior.

Some of the terms that Western and Russian scholars have used to describe Moscow's shifting character of warfare include 'hybrid warfare', 'new generation warfare', 'the Gerasimov Doctrine', 'political warfare', 'hostile measures', 'cross-domain coercion', and 'gray zone tactics' (Chivvis 2017; Adamsky 2015; Morris et al. 2019; Galeotti 2018; Kofman 2016). Although these terms contain certain subtle and useful differences, they essentially attempt to capture an established understanding in Russia's strategic perceptions that warfare now includes non-military measures that an adversary can effectively use before, or in place of, overt military force (Jonsson 2019, Chapter 1).

It is worth noting that discussions over the employment of non-military measures in Russian warfare are not a novel phenomenon; however, these discussions were not adopted by a critical mass of Russia's military establishment until recent years. Russian military scholars have been expounding on the utility of such measures since before the Communist Revolution. During Napoleon's ill-fated campaign in Russia, Tsarist troops and Cossacks widely distributed leaflets aimed at lowering the morale of a conventionally superior enemy, including messages attempting to fracture the multinational invading coalition (Academy of Sciences 1962). The early Red Army similarly saw the utility of psychological warfare in applying pressure to populations behind the front. As a manual on military intelligence published during

1 The authors would like to express their gratitude to Martti J. Kari for his prompt and insightful comments on some of the arguments outlined in this article.

the ‘War Scare’ of the late 1920s states, “Political sentiment of the population in an enemy’s rear plays a big role in an opponent’s successful activities; because of this it’s extremely important to generate sentiments among populations against the enemy and use them to organize people’s uprisings and partisan detachments in the enemy’s rear” (Shil’bakh and Sventsitskiy, 1927). Additionally, Evgeny Messner, a pre-Revolutionary leading thinker in Russia’s strategic thought who wrote about the value and advantages of non-military measures, wrote extensively about the dissolution of boundaries between war and peace and the use of information operations to affect societal cohesion, which are reflected in the writings of a number of influential Russian military scholars who have outlined their vision of the evolving character of warfare since the 1990s (Jonsson 2019, 38–40; Gerasimov 2019; Chekinov and Bogdanov 2013). Despite the difference in means, as exemplified by the use of digital technologies today, the strategy undergirding modern Russian military cyberattacks and information operations was laid over a century earlier.

Despite the increasing number of articles on the use of non-military measures throughout the 1990s and 2000s, Russian military elites’ thinking changed most significantly between the early 2000s and the Ukraine crisis, when a consensus formed among senior Russian leaders and military theorists that the boundary between war and peace had become blurred and nonviolent measures of warfare could be so effective as to be considered violent, rendering them a tool of warfare (Jonsson 2019, 6–7, 153). The chief of Russia’s Armed Forces, Valery Gerasimov, wrote that the rules of warfare were changing and revolts modeled on the Arab Spring possibly presaged future wars where the protest potential of the non-military actors and the use of political, economic, and other non-military measures would be widely employed (Gerasimov 2014, 2013). Military scholars such as Colonel Chekinov and Lieutenant General Bogdanov further expounded on this argument, stating that the aggressive side will first use non-military measures, such as information technology aimed at engaging public institutions in a targeted country, including the media, cultural institutions, religious organizations, NGOs, and foreign-sponsored movements (Chekinov and Bogdanov 2013, 17). General Gerasimov reemphasized the employment of mixed tactics and the maintenance of asymmetrical and classic potential at the 2019 conference of the Russian Academy of Military Sciences. He noted the changing character of war and the evolving “coordinated use of military and non-military measures” and even suggested the primacy of non-military measures over military power, used only when impossible “to achieve the goals set by non-military methods” (Gerasimov 2019).

Recent amendments of Russia’s main strategic documents also reflect an evolving view of warfare. The 2010 Russian Military Doctrine stated that integrated non-military and military means is a characteristic of modern military conflicts (President of Russia 2010). The updated 2014 doctrine reinforced this concept and listed it as the

first characteristic of modern military conflicts: "the integrated use of military force, political, economic, informational and other non-military measures implemented with widespread use of the protest potential of the population and special operations forces" (Rossiyskaya Gazeta 2014). The 2013 Foreign Policy Concept listed economic, scientific, and IT factors as being important as military capabilities to influence politics in a given state (Ministry of Foreign Affairs 2013). These speeches and doctrinal documents illustrate the conceptual flip that evolved in Russia's perceptions of modern warfare.

B. Russia's Official Views on Information Warfare

Outlining the contours of Russia's view on warfare is critical for grasping Russia's cyber strategy because Russia's view on cybersecurity is nested in Russia's evolving understanding of the nature of war and is shaped by its concept of information warfare.[2] Cybersecurity is perceived as a Western notion in Russian debates, while the semantic Russian equivalent is information security (*informatsionnaya bezopastnost*). Military scholars and official documents present slightly varying definitions of information warfare and information security, but it is generally well-established that information security is a component of information warfare, which is a term that has a technical as well as a psychological or cognitive component. Information warfare is an integral part of interstate conflict and its aim is to establish information superiority over the adversary by using technical and psychological means, while cyber operations are a mechanism used by the state to dominate the information environment, which is considered a domain of warfare (Thomas 2019, 5–5, 7–8, 7–9; Connell and Vogler 2017, 3). Russia's Ministry of Defense 2011 Concept on the Activities of the Armed Forces of the Russian Federation in the Information Space provided a clear definition of information warfare:

> …the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercing the state to take decisions for the benefit of the opposing force (Ministry of Defense of the Russian Federation 2011).

This definition emphasizes the two main elements of information warfare, namely the technical element of information infrastructure, which consists of a mix of "technical tools and systems of formation, creation, transformation, transmission, usage and storage of information" (roughly corresponding to issues pertaining to information

2 Russia's military literature and doctrine use three terms that can be roughly translated as information warfare. These are *informatsionnoe protivoborstvo* (information struggle or information confrontation), *informatsionnaya voina* (information war) and *informatsionnaya borba* (information fight). Explaining the nuances of each term is beyond the scope of this paper and for the purposes of this research, we will use the translation "information warfare". Also see Giles 2016, p. 7, footnote 8.

and cybersecurity in the West), and the psychological component of information warfare, which involves cognitively influencing the population and decision-makers of the opposing state to erode their will to fight and their decision-making structures and processes (Ministry of Defense of the Russian Federation 2011; Chekinov and Bogdanov 2015b, 45).

The information sphere and the concept of information warfare fits well within Russia's understanding of the changing character of war because, as General Gerasimov asserted, "without having clearly defined national borders, [the information sphere] provides the possibility of remote, covert influence not only on critical information infrastructures, but also on the country's population, directly affecting the state's national security." These characteristics render studying issues of preparation and conduct of informational activities "the most important task of military science" (Gerasimov 2019). Considering its multifaceted and unconventional nature, information warfare, and by extension cyber operations, may commence prior to the official announcement of war and can be deployed to achieve political objectives without resorting to the use of military force (President of Russia 2010).

C. Main Threats Posed in the Information Sphere

The threat posed by information means has gradually gained prominence in Russian doctrine since the start of the 21st century. In line with the Soviet tradition of portraying Russia as a besieged fortress defending itself against constant internal and external threats, Moscow also views the struggle in the information sphere as constant and unending (Kari 2019, 84, 72–6; Kari and Pynnöniemi 2019, 21; Connell and Vogler 2017). The 2000 National Security Concept highlighted that Russia's national security is threatened in the information sphere by countries that are attempting to dominate the information sphere while developing their concept of information wars. The Security Concept presented a holistic understanding of the term by focusing on threats that are related to both the technical and the psychological aspects of information warfare (Ministry of Foreign Affairs of the Russian Federation 2000). Russia's 2010 Military Doctrine further elevated the status of information warfare and signaled a shift in the formal understanding of threats to the nation by listing the increasing role of information warfare for the first time as a characteristic of contemporary military conflicts and the imperative for Russia's military to develop forces and means of information warfare (President of Russia 2010).

The 2000 and the 2016 Russian Information Security Doctrines further codified Russia's official view on the role of information threats in contemporary warfare (Table 1). The 2000 doctrine provided a broad definition of the information sphere, which is a "combination of information, information infrastructure, entities involved in the collection, generation, distribution and use of information, as well as a system

for regulating the resulting public relations" (*Nezavisimaya Gazeta* 2000; President of Russia 2016). This definition is in line with the understanding that Russia's information sphere includes a technical and a cognitive component. Based on this broad definition, the concept includes a wide array of threats to information security. They range from more technical threats, such as threats to the security of information and telecommunication facilities and systems that include "the introduction of electronic devices for intercepting information in the technical means of processing, storing and transmitting information," and broader threats to societal cohesion, such as "decrease in the spiritual, moral and creative potential of the Russian population" (*Nezavisimaya Gazeta* 2000).

The 2013 Security Council's Basic Principles on International Information Security confirmed this broad understanding and the panoply of threats related to information security and saw information technology as a weapon that can be used for political and military purposes to violate a state's sovereignty and territorial integrity (Security Council of the Russian Federation 2013). The updated 2016 Information Security Doctrine continued in the spirit of its conceptual predecessors by reemphasizing the growing threat posed to Russia in the information sphere by various adversaries (President of Russia 2016). The doctrine emphasized increasing threats emanating from the information cognitive space, primarily driven by foreign actors, and their effects on social values and stability (President of Russia 2016). These documents illustrate the belief that Russia's posture in the information sphere is shaped in response to threats to Russia that are forcing the state into defending itself.

D. Russia's Doctrinal Response to Threats in the Information Sphere: Defensive and Cooperative Posture

Russia's officially expressed strategy to manage threats in the information sphere is as multifaceted and broad as the threats themselves, yet the strategy is generally consistent in its omission of offensive or adversarial actions (Table I). In official documents, the government lists policy goals that outline a primarily defensive and collaborative posture designed in response to aggressive adversaries and entities that threaten Russia, which aims to contain or prevent aggression in cyberspace through legal frameworks and partners. Such national-level policies include the "development and adoption of regulatory legal acts of the Russian Federation establishing the liability of legal entities and individuals for unauthorized access to information, its illegal copying, distortion and illegal use" and enhancement of "the security of critical information infrastructure" (*Nezavisimaya Gazeta* 2000; President of Russia 2016). International policy recommendations range from the "formation of a system of international information security" to "the formation of mechanisms for international cooperation in countering the threats of the use of information and communication technologies for terrorist purposes" (Security Council of the Russian Federation 2013).

TABLE I. A SELECTED LIST OF MAIN THREATS AND RECOMMENDED POLICY RESPONSES AS OUTLINED IN MAIN RUSSIAN INFORMATION SECURITY DOCUMENTS

Document	Threats		Recommended Policy Response
	Psychological	Technical	
Information Security Doctrine (Nezavisimaya Gazeta 2000)	• irrational, excessive restriction of access to socially necessary information; unlawful use of special means of influence • ousting Russian news agencies, the media from the domestic information market and increasing the dependence of the spiritual, economic and political spheres of public life in Russia on foreign information structures • a decrease in the spiritual, moral and creative potential of the Russian population	• development and distribution of programs that interfere with the normal functioning of information and information and telecommunication systems, including information protection systems • compromise of keys and means of cryptographic information protection • destruction, damage, or theft of machines and other storage media	• introduction of amendments and addenda to the legislation of the Russian Federation regulating relations in the field of ensuring information security in order to create and improve the system of ensuring information security of the Russian Federation • clarification of the status of foreign news agencies, media and journalists, as well as investors when attracting foreigners' investments for the development of information infrastructure in Russia; • legislative priority for the development of national communications networks and domestic production of space communications satellites
Conceptual Views on the Activities of the Armed Forces in the Information Space (Ministry of Defense 2011)	• threats of a political nature in the information space	• widespread use of computer technology in command and control systems of troops and weapons	The activities of the Armed Forces of the Russian Federation in the information space are built on the basis of a set of principles: legality, cooperation with friendly states and international organizations; and containment and prevention of military conflicts in the information space
Convention on Ensuring International Information Security (Ministry of Foreign Affairs 2011)	• factors creating a danger to the individual, society, state and their interests in the information space • actions in the information space in order to undermine the political, economic and social systems of another state, psychological treatment of the population, destabilizing society • using the information infrastructure to disseminate information that incites ethnic, racial and inter-confessional enmity, racist and xenophobic written materials	• targeted destructive impact in the information space on the critical structures of another state • countering access to the latest information and communication technologies, creating conditions for technological dependence in the field of informatization to the detriment of other states • information expansion, acquisition of control over the national information resources of another state	State parties should: • maintain international peace and security and promote international economic stability and progress, the general welfare of peoples and international cooperation, free from discrimination • refrain from developing and adopting plans and doctrines that can provoke an increase in threats in the information space, as well as cause tensions between states and the emergence of "information wars" • refrain from any action aimed at the complete or partial violation of the integrity of the information space of another state
Basic Principles for State Policy in the Field of International Information Security until 2020 (Security Council 2013)	• carrying out hostile acts and acts of aggression aimed at discrediting sovereignty, violating the territorial integrity of states and posing a threat to international peace, security and strategic stability • interfering in the internal affairs of sovereign states, disturbing public order, inciting interethnic hostility	• destroy elements of critical information infrastructure • crimes, including those related to unlawful access to computer information, with the creation, use and distribution of malicious computer programs	• formation of a system of international information security at the bilateral, multilateral, regional and global levels • creating conditions to reduce the risk of using information and communication technologies for hostile acts and acts of aggression aimed at discrediting sovereignty, violating the territorial integrity of states and posing a threat to international peace, security and strategic stability
Information Security Doctrine (President of Russia 2016)	• increasing use by the special services of individual states of information and psychological influence aimed at destabilizing the domestic political and social situation in various regions of the world and leading to the undermining of sovereignty and territorial integrity • increase in materials in foreign media containing a biased assessment of the government policy of the Russian Federation	• increase in the scale and coordination of computer attacks on objects of critical information infrastructure, increased intelligence activities of foreign states against the Russian Federation, as well as an increase in threats to the use of information technologies in order to cause damage territorial sovereignty integrity, political and social stability of the Russian Federation	• strategic deterrence and prevention of military conflicts that may arise as a result of the use of information technology; forecasting, detection and assessment of information threats, including threats to the Armed Forces of the Russian Federation in the information sphere • neutralization of information-psychological impact, including aimed at undermining the historical foundations and patriotic traditions associated with the defense of the Fatherland

E. Cybersecurity beyond Russia's Doctrine: The Value of Cyber Weapons

Although Russia does not have an explicit cybersecurity doctrine and its formal documents discussing Russia's posture in the information sphere show a primarily defensive posture, Russia's theoretical military literature provides additional useful insights into the role of cyber capabilities, especially offensive cyber capabilities, in Russia's view of conflict. Military scholars elaborate on the appositeness of cyber weapons in modern warfare, on their versatility and effectiveness, and on their affordability. Offensive cyber capabilities fit within the concept of information warfare because cyberspace allows for blurring of the boundaries between war and peace, as damage can be inflicted on an adversary during peace time without crossing the threshold of armed conflict or declaring war as a legal act. Enabled by a lack of clear legal framework to serve as the foundation for prosecuting the perpetrators of cyber operations, an adversary can conduct hostile or destructive cyber operations from any location and can weaken the enemy's ability to defend themselves and retaliate (Vorob'ev and Kiselev 2013, 33–4; Kuznetsov et al. 2018, Parshin and Bashkirov 2019, 5; Antonovich 2011; Thomas 2010, 287; Starodubtsev, Bukharin and Semyonov 2012; Jonsson 2019, 108). Another military virtue of cyber weapons, as then First Deputy Chief of the General Staff, General Aleksander Burutin, and others argued, is that these weapons can help an adversary achieve information supremacy without crossing borders or establishing physical presence on the enemy's territory (Thomas 2010, 287; Parshin and Bashkirov 2019, 6). Even perhaps more importantly for Russia, offensive cyber capabilities can be considered as asymmetric actions that can help a technologically and economically weaker state (which Russia considers itself to be vis-à-vis the United States) to neutralize a stronger opponent (Selivanov 2020, 50; Kari 2019; Burenok 2018). Offensive actions in cyberspace may also be preferable to defensive ones, as the former are deemed faster than the latter (Mikryunov 2015, 117).

Russian military scientists have repeatedly noted the destructive capacity and versatility of cyber weapons, which can be employed against civilian, military, and government targets. In line with Russia's doctrinal understanding of information warfare, scholars argue that the deployment of cyber weapons can affect adversaries' infrastructure as well as their psychology. In an article prepared on behalf of the Defense Ministry, Bazylev et al. elaborated on the technical impact of cyber weapons and argued that such weapons can critically affect facilities in the transportation or energy sectors, and can even lead to a financial crisis (Bazylev et al. 2012, 24–25, Jonsson 2019, 108). Military scientists Kiselev and Kostenko expounded that cyber weapons can endanger not only critical infrastructure elements such as supervisory control and data acquisition (SCADA) systems and smart power systems but also military systems (Kiselev and Kostenko 2015, 4). During conflict, such weapons can render the enemy's control infrastructure dysfunctional and the higher the level of automation of objects and processes of the targets, the greater results that can be

achieved because of the existence of vulnerabilities in these systems (Starodubtsev, Bukharin and Semyonov 2012, 29-30; Kuznetsov et al. 2018, 5). In addition to their technological effects, these weapons can "completely disorganize state and military administration, demoralize and disorient the population, and create mass panic" (Bazylev et al. 2012, 24-5, Jonsson 2019, 108). Former Deputy chief of the General Staff, Colonel-General Anatoliy Nogovitsyn, and others further elaborated on the offensive role of cyber tools and their dual impact, explaining that they can destroy military, administrative, and industrial sites, while also inflicting information and psychological damage on the enemy's troops, leadership, and population (Thomas 2010, 287; Parshin and Bashkirov 2019, 4, 8-9).

Another positive characteristic of cyber weapons discussed by military scientists is their relatively low cost. The development and creation of such weapons is estimated to be much cheaper than other types of weapons, while the use of either leads to comparable damage (Parshin and Bashkirov 2019, 6; Romashkina and Kildobskiy 2015, 134; Putin 2012; Jonsson 2019, 109). A study further elaborates that the total defeat of the information infrastructures of major powers such as the United States or Russia could be conducted by up to 600 "information warriors." Training these warriors and executing the actual attack would take about two years and cost no more than 100 million dollars (Bazylev et al. 2012, 24-5). Another potential reason for the relative affordability of such weapons is that operational plans for their use may be developed by non-military experts (Starodubtsev, Bukharin, and Semyonov 2012). Despite the lack of explicit discussion on specific Russian cyber operations or developments of cyber weapons, the literature offers certain clues as to how Russia's military elite views cyber warfare and offensive cyber capabilities on a theoretical level, which demonstrates a realization of the value of cyber weapons as having high levels of effectiveness and versatility, high affordability, and fitting within the current character of warfare.

The analysis of Russia's doctrine, speeches of Russia's elite, and the military scientific literature paints a general picture of Russia's vision of cybersecurity, which is situated in Russia's understanding of information security and information warfare. Although Russia's official documents describe Russia's view on information warfare as defensive, Russia's military literature shows an active debate on the value of developing and fielding both defensive and offensive cyber capabilities. The interest in discussing cyber weapons in Russian military journals, coupled with proactive Western cyber policies, such as the strategy of persistent engagement and the concept of defending forward that is endorsed by U.S. Cyber Command, may provide sufficient justification that will prompt the Russian leadership to formally include the development and deployment of cyber weapons in its information warfare doctrine (U.S. Cyber Command 2018). On the other hand, the continuous omission of an

official endorsement of offensive cyber capabilities in its doctrine allows the Russian government to claim plausible deniability and maintain a narrative (as questionable as that narrative is among Western observers) of a defensive power under threat by an aggressive West – a classic justification for a number of Russian policies, including investments in military modernization.

To further understand Russia's cyber strategy and policy, this article will examine the evolution and institutional character of the structures of Russia's government that are involved in the conduct of Russia's information and cyber operations, which appear to follow Russian doctrine and literature on the importance of developing cyber capabilities that have both technical and psychological effects.

3. THE EVOLUTION OF FSB AND GRU CYBER AND INFORMATION OPERATIONS

A. The Initial Years of Russia's Cyber Operations: The FSB and Non-state Actors

Throughout most of post-Soviet Russia, the Federal Security Service (FSB) maintained the "commanding heights" of external cyber operations. In the unregulated space of the Russian internet in the 1990s and early 2000s, the FSB developed relationships that helped it coopt or coerce independent Russian hackers and specialists into cyber operations. Layers of unofficial hackers helped circumvent the human capital challenges that long impaired Russia's early development of cyber-capable cadres. For instance, an anonymous source within one of the FSB's leading hacking departments, the Center for Information Security (CIS), claimed that the unit employed illegal hackers to make up for its staffing deficiencies (Turovsky 2018, 149), while another source claimed that one of the leading CIS hackers, when recruiting external support, often created an "atmosphere that Russia needed help," even more so after the 1990s, when attacks against banks in Europe and the U.S. could help alleviate financial shortfalls (Turovsky and Rothrock, 2018). The FSB's inheritance of the bulk of the Federal Agency of Government Communications and Information (FAPSI), a loose analog to the U.S. National Security Agency that was disbanded in 2003, alongside the Kvant Scientific Research Institute that has assisted the FSB's technological research for over a decade, provided the FSB with a significant advantage in fostering an offensive cyber capability (U.S. Department of The Treasury 2018). As longtime cybersecurity correspondent Andy Greenberg wrote of the period, "…the GRU [the Main Intelligence Directorate of Russia's military] had taken a backseat to the FSB throughout Russia's inchoate cyberwars in Estonia and Georgia, relegated to traditional intelligence in direct support of the military rather than the exciting new realm of digital offensive operations" (Greenberg 2019, 236).

For a while, this fluid basis for cyber operations served Moscow's interests. The "Siberian Network Brigade," a group of Russian students from Tomsk University, enjoyed legal cover from their local FSB branch as they launched Distributed Denial of Service (DDoS) attacks against Chechen websites in the early 2000s (Gazeta.ru 2006; Newsru.com 2002). The renowned example of attacks against Estonia in 2007 similarly involved an amorphous coalition of state-sponsored hacking that mostly continues to defy firm attribution. At the same time, malware most likely associated with the FSB penetrated U.S. defense networks to facilitate one of the most significant breaches of classified data in history (Council on Foreign Relations 2008). Throughout the early 2000s, there was little reason for Moscow to seriously consider an alternative to an FSB-led cyber program, and the latter's prominence in executive leadership circles ensured its lead. As Keir Giles noted in 2011, the prospect of "information troops" in Russia's military, which would include cyber operations, was officially discounted by the FSB at the time (Giles 2011).

Ironically, some of the FSB's earlier operations perhaps helped bring about the eventual ascension of the Russian military's cyber program, which languished under post-Soviet malaise, meager budgets, and personnel deficiencies. The cyberattacks on Estonia and Georgia, plus the exploitation of U.S. defense networks by Russia and other states, prompted the U.S. to strengthen its own military program, most notably with the foundation of the U.S. Cyber Command in 2009. Other events concurrent to the Cyber Command's development, such as the revelations surrounding the unprecedentedly sophisticated "Stuxnet" malware targeting Iran's nuclear program, reinvigorated concerns among Russian security and defense observers about U.S. predominance in cyberspace. U.S. efforts to apparently militarize its growing cyber capabilities necessitated that Moscow redouble efforts to improve those within its military. Unproductive negotiations between Russian and Western interlocutors about regulating evolving cyber capabilities, caught in fundamental divides on issues like international internet governance, dwindled the prospect of "cyber arms control" between Moscow and its perceived adversaries (Krikunov 2011, 32–7; Tikk and Kerttunen 2018; Kavanaugh 2015). While loose, ad-hoc coalitions of cyber actors outside the state's direct purview may have been sufficient for Russia's earlier cyber ambitions, the apparently widening gap in capabilities between it and other states and alliances, chiefly NATO, exacerbated preexisting fears about unpreparedness for what was increasingly viewed as an inevitable information confrontation with the West.

B. The Advent of the GRU to Information Warfare

In mid-2013, after receiving presidential approval, Russian Defense Minister Sergey Shoygu launched a "big hunt" for programmers to fill the ranks of new "military science units" (*voennye nauchnye roty*) that would advance the military's research and development through the coming years, with an emphasis on cyber operations,

signals intelligence, and electronic warfare.[3] Of the four original science companies, one belonged to the GRU, which had an unmistakable focus on computing and information technology.[4] In May the following year, sources within Russia's Ministry of Defense announced the establishment of an "information operations force" (*voyska informatsionnykh operatsiy*), which, according to the Russian press, was partly predicated on the growth brought through the science units and the development of which was catalyzed by the leaks of classified U.S. programs by Edward Snowden (TASS 2014; Saltykov 2014). Moreover, the 2014 Military Doctrine listed the "development of forces and means of information confrontation" as a main task of equipping Russia's modernizing armed forces (*Rossiyskaya Gazet*a 2014). By early 2017, Shoygu was confident enough in the force to announce its readiness before Russia's national legislature. Between his "big hunt" and 2017, the attribution of Russia's most significant cyber operations to the GRU by Western intelligence agencies and a range of private cybersecurity and investigative organizations evidenced the arrival of the GRU as the probable leader in large-scale cyberattacks.

As the Main Intelligence Directorate of Russia's General Staff came to the fore in offensive cyber operations, it brought with it a culture of aggression and recklessness; the same day that the GRU's Main Center for Special Technologies launched the costliest cyberattack to date, the 'NotPetya' wiperware that led to over $10 billion in damages, a car bomb in Ukraine's capital killed a Ukrainian special forces officer (Greenberg 2017; Nakashima 2018).

The GRU's seemingly high tolerance for operational risk is in many ways incongruent with the traditionally furtive realm of cyber operations, which consist far more often of quiet espionage efforts than large-scale attacks. A former FSB cyber officer who was arrested in late 2016, possibly in an effort to expose GRU hackers by leaking information about them, claimed that the GRU "impertinently, roughly, and brutishly breaks into servers," which always led to their attribution (Turovsky 2018, 198). Whatever the GRU's apparent missteps, the organization at least publicly maintains President Putin's confidence, and the continuous attribution of Russian cyber and

3 For example, *Rossiyskaya Gazeta*, a state-controlled press outlet, ran an article in 2013 titled "Private [military rank] Hacker" (*ryadovoy khaker*) that accompanied the rollout of the science units (Gavrilov 2013). Moreover, as journalists with Meduza acutely noticed, science-unit recruitment was likely bolstered by a 40-part TV show aired by the Zvezda network that glamorized new recruits' work in a Russian military cyber unit (Turovsky 2016). Though most science units conduct some research outside of computer science or information technology, almost all have some cyber research component, which is certainly true of the four original units established in 2013. Moreover, the newest such units, assigned to the 'ERA' technopolis based in Anapa, Russia, concentrate on cyber-relevant projects, judging from official documents and press reporting (Ministry of Defense of the Russian Federation 2018; Ren.tv 2019).

4 For example, the GRU's science unit maintained a stand at the military's 2015 "Innovation Day," where it displayed materials with a clear focus on computer science research (Livejournal.com 2015). Additionally, an archived copy of an anonymous resume from a former member of that unit demonstrates an exclusive background in computer programming. According to the official website of Bauman State Technical University, the GRU's science company is based in Zagoryanskiy and is designated as Unit Number 36360 (Bauman Moscow State Technical University).

information operations to it show that the GRU is likely to continue conducting these campaigns (Balforth 2018). The graduates of computer science programs brought into the GRU's ranks through its own science unit(s) and other initiatives are most likely distant from their counterparts in Russian "*spetsnaz*" units. As Andrey Soldatov explained, the "stereotypical portraiture of a GRU hacker" is "far from universal," as the organization recruits non-military types "conscripted for their services with little choice in the matter" (Greenberg 2019, 242). But, to the extent science unit(s) recruiting advertisements, which feature a Kalashnikov assault rifle propped next to a computer, suggest the culture into which these recruits enter, GRU operators are likely to continue meshing a daring culture of special operations with digital activity, an undoubtedly alluring prospect for at least some of Russia's youth (*Nauchnaya Rota* REB 2015).[5] The importance that Russian defense officials place on their work only reinforces this aura of exigency and adventure. A vice-admiral who reportedly delivered a science-unit recruiting pitch to university students in 2013 compared their future work to the Soviet Union's development of an atomic bomb, which echoed a similar comparison by Moscow's foremost cyber-diplomat, Andrey Krutskikh, in 2016 (Habr.com 2013; Ignatius 2017).

C. GRU's Organizational Culture and the Conduct of Information Operations

Another aspect of GRU culture has driven its adoption of cyber operations and has largely been unexplored: its history and growing fixation on information operations. Contrary to most of the GRU's cyber units,[6] its information operations forces have a deep history; the Red Army dedicated a force to "special propaganda" (*spetsprop*) shortly before World War II, and these forces represent a component of Russian information warfare as indispensable as technical capabilities. *Spetsprop* units broadcasted messages and distributed leaflets and products to enemy forces to reduce their morale and entice surrender, and they worked to influence civilian populations behind the frontlines and when promoting civil-military operations in the wake of advancing armies, though efforts to foster public support were quickly undone by mass arrests and deportations. After 1991, these units were rebranded and placed exclusively under the GRU.[7] The GRU organized many of these specialists into eight "psychological operations groups" during the throes of the first Chechen War and dispersed them throughout Russia's military districts (Kozlov 2010, 176).

Nonetheless, disappointment in the military's ability to counter perceived Western information warfare aimed at Russia during the Georgian War (Iasiello 2017) drove

5 The same unit that posted the above recruiting video was tangentially associated with the GRU's "Fancy Bear" hacking team when, in 2015, it posted another recruiting video that featured the emblem associated with the group, though it was subsequently taken down (Turovskiy 2016).

6 The exception to this is Unit 26165, or the 85th Main Special Service Center, which was founded in the 1970s to conduct signals intelligence.

7 During the Soviet era, special propaganda units belonged to the Main Military Political Directorate (GlavPUr). Following the collapse of the Soviet Union, they were renamed "Centers for Foreign Military Information and Communication" (*Argumenty Vremeni* 2018).

defense officials to rejuvenate *spetsprop* in the 21st century. Officials realized that modern propaganda, like that seen to be used by NATO, needed to be digital. An official in the GRU's information operations training pipeline,[8] for instance, claimed in accordance with the Russian information warfare doctrine sometime after the Georgian War:

> The features of modern information confrontation show that it is [as] directed at both information-technical systems … as it is on human psychology. Activity against an enemy is organized and conducted in two aspects (directions): technological and psychological (Cheshuin 2009).

New aspects of information warfare, such as DDoS attacks, would be introduced to the information operations faculty of Russia's Military University of the Defense Ministry following the Georgian War and combined with old operational practices, such as disinformation (Cheshuin 2009).

As much as cyberattacks provided a new means for asymmetric tactics, modern information communications technology also provided the GRU with an updated arena for propaganda techniques that extended back to the foundation of *spetsprop*. Roughly 80 years before GRU specialists attempted to stir Polish-Ukrainian tensions in Lviv through social media, Red Army propagandists pitted the two nationalities against one another in the same region to ease the Soviet invasion of eastern Poland at the onset of World War II (Diresta and Grossman 2019, 55; Repko 1999, 267). Similar to special propagandists' use of German radio networks to entice surrender during that war, the modern GRU orchestrated the demoralizing text messages that have been sent to Ukrainian soldiers since 2014 (Burtsev 1981, 166–67; Tribun 2018).

These units' activity since the early 2000s demonstrates their "digitalization," including their eventual involvement in cyberattacks. During the Second Chechen War, they launched an unsophisticated "e-newspaper" titled "Morning" (*Utro*) to color events surrounding the conflict (Kompromat.ru 2002). The GRU's efforts to conduct online influence operations probably evolved somewhat by the start of the Ukraine crisis in 2014, though their use of a Facebook primer containing basic instructions on using the platform indicates operators were still somewhat unfamiliar with waging an internet-based information war (Nakashima 2017). Only a year later, however, the GRU combined cyberattacks, primarily against France's TV5 Le Monde, with influence operations through ISIS social media cutouts as part of its "CyberCaliphate" campaign (Sengupta 2018). Like the apparent recklessness in hacking used to support the campaign, CyberCaliphate involved direct physical threats via social media

8 The "Faculty of Foreign Military Information" at Russia's "Military University of the Defense Ministry" (VUMO) has long served as the main training pipeline for Soviet and Russian psychological warfare units, and its history extends back to the foundation of special propaganda. According to information on a Russian website on academic institutions in the Moscow area, the faculty directly sends its graduates to the GRU (Moscow-Russia.ru).

against U.S. military spouses, exemplifying that digital aggression would carry over into influence operations (Slatter 2018). The involvement of the nucleus of the GRU's psychological warfare apparatus, the 72nd Special Service Center (Unit 54777), demonstrated that information operation specialists would work alongside GRU cyber units throughout the campaign (Troianovski and Nakashima 2018).

According to Western intelligence officials, the 72nd Special Service Center (Unit 54777) has been in lock-step with GRU hackers since at least 2014, complementing cyberattacks with digital information operations through proxies and front organizations (Troianovski and Nakashima 2018). Before the Ukraine crisis, Unit 54777 had 80 specialists split among five sections: a Center for Foreign Military Information; a department for organizing and conducting psychological or information operations; a department for organizing "teleradio" broadcasts; a department for working with mass media; and an editorial-publications department.[9] The unit sent advisors to Russia's various military branches, such as the ground forces and navy, and levels of command that reached from GRU leadership to tactical units manning frontline loudspeaker vehicles.[10] This plausibly served as a prototype for the "information confrontation" chain-of-command revealed by Gerasimov during a staff exercise in 2016 (Izvestiya 2016). Though unverified, Ukrainian accounts of regional GRU information operations units conducting cyber and electronic warfare operations probably demonstrate the capabilities of local commands to conduct operations at lower echelons (Tribun 2018).

D. GRU's Organizational Culture and the Conduct of Technical Cyber Operations

While the GRU's cyberattacks have attracted much research and analysis throughout the past six years, less effort has been given to discerning how the organization's history influences contemporary operations. Russian military intelligence's cyber operations are rooted in the history of its technical intelligence that, while perhaps not as extensive as that of information operations, predates World War I. Technical intelligence, primarily cryptography and signals intelligence, underwent its most significant and expansive development during the Soviet period. Early Soviet military leadership recognized its importance, expanding the number of "radio-reconnaissance stations" throughout the U.S.S.R. and abroad throughout the 1920s, allowing signals intelligence to play a central role in the Sino-Soviet conflict in 1929 (Kozlov 2013, 411). Soviet military signals intelligence and cryptography achieved notable prewar successes in the Far East, surpassing British and equaling U.S. collection capabilities in that theater by 1939 (Haslam 2015, 98). Despite at least occasional effectiveness, the Soviet military's early technical intelligence capabilities mostly existed in the shadow of the internal security services, such as the subordination of decryption specialists to the Joint State Political Directorate (OGPU) (Larin 2017, 65). World

9 Discussion with experts, May 2018. Helsinki.
10 Ibid.

War II prompted breakneck growth to Soviet military technical intelligence, and – by 1942 – military cryptologists successfully cracked the German military's "Enigma" machine, and eventually began intercepting and deciphering German communications with enough regularity to force German signal officers to forbid marking "the Fuhrer's radio messages in any special way" (Kahn 1996, 649). Throughout ebbs and flows in terms of political influence, resources, and relations with the more powerful KGB, the GRU continued to expand its signals intelligence capabilities during the Cold War; by the Gorbachev era, the Soviet military possessed 40 signals intelligence regiments, 170 battalions, and over 700 companies (Andrew and Mitrokhin 1999, 353).

One of the most significant developments for Soviet military signals intelligence during the late Cold War was the establishment of the 85th Main Special Service Center (Unit 26165), which was responsible for GRU cryptography through a variety of technical means, including the "Bulat" computer system (Shevyakin 2014, 104). The center's independence from the GRU's signals intelligence directorate and direct subordination to GRU leadership exemplified the importance of their work. Whatever the center's prominence in the Cold War, it very likely suffered from the same post-Soviet reductions that affected the broader Russian military and its intelligence capabilities. Nonetheless, officers like Viktor Netyshko, who would eventually head the center during its efforts to influence the 2016 U.S. presidential election, ensured that the 85th would continue its mission and development of cyber capabilities no matter the shortfalls, albeit at a reduced capacity. Fewer resources, including access to recruits during a period when the military was supposed to drastically expand its cyber specialists, likely influenced the eventual agreement between Netyshko and the FSB in 2017 to jointly prepare recruits at the latter's cryptography institute probably in part for entry into the military's science unit(s) (Moscow State Budgetary General Education Institute 2017).[11] In the meantime, future leaders of the center pursued scientific and academic research related to the kind of computer science needed to advance cyber operations. In 2003, Netyshko defended a dissertation related to the academic specialty "Mathematical and Programming Software of Computers, Complexes, and Computer Networks," and in 2010 he served as an opponent for a dissertation on computer hacking (Turovsky 2018, 195). Sergey Gizunov, who preceded Netyshko as the center's commander and who simultaneously taught computer science, was awarded the title "Laureate of the Government of the Russian Federation in the Field of Science and Technology" in 2008 (*Rossiyskaya Gazeta* 2009). Gizunov's promotion to GRU deputy director in 2015 likely evidences the growing influence of technically proficient officers experienced in cyber operations.

The 85th Special Service Center, however, represents only a part of the GRU's offensive cyber apparatus. The Main Center for Special Technologies (Unit 74455) has similarly captured significant attention surrounding its involvement in the effort

11 As described in the document, the FSB's Institute of Cryptography, Communications, and Informatics Academy would prepare recruits for entry into the FSB's academy and "targeted groups of military units at technical universities" (*tselevye gruppy Voyskovoy chasti VUZov tekhnicheskovo profilya*).

to influence the 2016 U.S. presidential election and the "NotPetya" cyberattack the following year. Unit 74455's historical roots are far shallower than Unit 26165's history as part of Soviet signals intelligence, and the former's establishment probably reflected the mounting importance of strictly computer-based operations to Russia's military leadership. Its officers are seemingly also closely connected to military computer science research; a commander of one of Unit 74455's departments reportedly teaches "applied information technology" at the Mozhayskiy Military-Space Academy (Faizova et al. 2018). An apparent link between Unit 74455 and the 4th Central Scientific Research Institute, a defense ministry entity historically dedicated to the strategic missile forces, potentially couples GRU hackers with research relevant to evolving military theory and strategy surrounding cyber operations.[12] The continued authorship of articles between 2008 and 2018 related to cyber capabilities in a journal titled *Information Wars* by 4th Central Scientific Research Institute officials probably indicates a growing interest by the organization in cyber issues, such as a 2018 article titled "Threat Models of Joint Information-Technical and Information-Psychological Effects in Hybrid Wars" (Antonov et al. 2018). At the same time, operations attributed to Unit 74455 against Ukrainian, European, and Western targets demonstrated an increasing sophistication that likely partly stemmed from better resourcing and staffing. Marina Kotofil, an industrial control systems expert, remarked about the difference between the 2015 and 2016 operations to disrupt Ukrainian energy grids, "In 2015, they were like a group of brutal street fighters … in 2016, they were ninjas" (Greenberg 2019, 133).

E. Implications of the Rise of Russian Military Cyber and Information Operations for Future State-Sponsored Activity

The fall 2019 cyberattacks committed by the GRU against Georgia exhibited the inseparability of the technical from information elements of contemporary information warfare, using sophisticated malware to black out television and websites while disseminating an image of Georgia's former president, who was indicted on corruption charges in 2013, claiming he would return (Greenberg 2020). This integration is very likely to continue in future campaigns, such as potential cyber flashpoints between Russia and the West surrounding upcoming presidential and parliamentary elections in 2020, and deepening political and societal divisions within several of those states to provide Russian state-sponsored actors with an opportunity to continue undermining perceived adversaries through digital means. As these vulnerabilities to cyber and information operations have worsened, Moscow has likely continued to hone and expand the cyber capabilities to exploit them. A late 2019 report by Check Point Software Technologies, for instance, claimed that state-sponsored actors invested a "significant amount of money and effort" in the first half of 2019 to develop "large-

12 One of the servers used by Unit 74455 to conduct operations related to the effort to undermine the 2016 U.S. presidential elections was based at the same address as the 4th Central Scientific Research Institute (Kritukov 2018). Moreover, a document related to a military court decision in 2010 revealed the transfer of an employee of the institute probably to Unit 74455 to lead "department 24" (Znamensk Garrison Military Court 2011).

scale espionage capabilities," which the firm concluded was an unprecedented investment by Russia in "offensive cyberspace" (Doffman 2019). The imperative to understand these capabilities has perhaps never been greater, and studying the organizational culture and history of the actors responsible for carrying out cyber and information operations offers unparalleled insight into the motivation, strategy, and methods guiding their respective efforts.

Given the consequences and reach of the GRU's cyber and information operations, which range from debilitating a swath of global shipping through wiperware to attempting to stoke racial tensions in the U.S., understanding the actors behind this activity on a more specific level is critical for anticipating potential future efforts and understanding how to address them (Greenberg 2019, 174–89; Digital Forensics Research Lab 2018). In part, this involves historical research on Russian intelligence. While countless Western publications continue to discuss the Gerasimov Doctrine of 2013, few have paid due attention to mid-level Russian defense and security experts who have warned of impending information confrontation with the West. Even the General Staff's normally diplomatic cyber-sages adopted a peace-through-the-knife approach, expressed in a journal article published as Wikileaks released a trove of DNC data in 2016:

> … the United States can enter into agreements with its geopolitical rivals only if they understand that they are opposed by an information potential as powerful as theirs. Therefore, the dialectic of interconnection and interdependence of political and military measures to counter the outbreak of war dictates the need to create a national information potential sufficient to deter possible aggression (Dylevskiy et al. 2016, 3–11).

That same year, a former deputy chief of the GRU discussed the "crisis" in relations between the West and Moscow against the mounting importance of information warfare, which, on a progressively greater scale, incorporated "cybernetic" operations that could achieve technical and psychological effects (Kondrashov 2016). Comprehending the specifics that guide Russian actors responsible for cyber and information operations can better prepare Western interlocutors and policymakers for managing a threat that will almost certainly exist throughout the near-term future.

4. CONCLUSION

Throughout the past few years, Russia's conceptualization of warfare has shifted to incorporate non-military means alongside armed violence. This transformation is exemplified by the increased relevance of information warfare in Russian doctrine.

According to this doctrine, information warfare consists of cyber and information operations and is an integral element of modern conflict. When discussing information warfare, official doctrine depicts Russia as a state nobly adhering to a defensive posture in an environment characterized by aggressive adversaries. The writings of Russian military scientists, however, illustrate an evolving interest in developing cyber weapons due to their effectiveness, appropriateness within the framework on contemporary conflict, and affordability. These analyses of offensive cyber tools seem more accurately aligned with the actual Russian practice of cyber and information operations that developed in parallel to Russia's thinking of contemporary conflict.

The actors and agencies involved in Russia's cyber operations evolved alongside Russia's perception of modern warfare and the threats posed by Western use of information technologies to further its military and foreign policy goals. In the first decades of the post-Soviet period, the FSB had a primary role in conducting cyber operations alongside the support of independent Russian hackers. Around the same time, a consensus formed among Russia's elite that warfare includes military and non-military measures during peace and wartime, and Russia's Defense Ministry increased its efforts to establish an organized and centrally controlled cyber force. These changes, coupled with the operational opportunities presented by Russia's intervention in Ukraine, enabled the GRU to adopt a leading position in offensive cyber operations, bringing a historical penchant for risk-taking and aggression to its operations. Additionally, the GRU's traditional command of information operations provided a natural place for cyber alongside information operations – the two core components of information warfare. These realities further enabled the transformation of Russia's strategic cyber operations from seemingly ad-hoc activities to more organized and centrally controlled campaigns that complement Russia's view of modern warfare.

Russia's conceptualization of information warfare and the units executing these operations are likely to drive future Russian cyber policy and strategy. The notion, for instance, that Russia faces aggressors who are utilizing evolving information communications technology to undermine Russia's military potential and society will almost certainly endure through the immediate future. At the same time, the idea that Russia's enemies are just as vulnerable to information means that Russia will probably safeguard the role of cyber and information operations within Russian doctrine and within the security and military organizations responsible for executing them for years to come. Although Russia's military inarguably will continue to value conventional assets and invest in modern warfighting technology, the growing prominence of unconventional means, particularly digital ones, in its ongoing competition with the West suggests that these capabilities will garner further attention in military doctrine, the writings of Russian military scientists, and state policy. It is possible that Russia's

leadership may choose to formally include research, development, and use of cyber weapons as an official line in its information warfare doctrine. However, this scenario seems unlikely considering that the current defensive nature of Russia's information warfare doctrine may enhance Russian claims of plausible deniability when being accused of conducting offensive cyber operations.

REFERENCES

Academy of Sciences. 1962. *Listovki otechestvennoy voyny* [Leaflets from the Patriotic War]. Moscow: U.S.S.R. Academy of Sciences.

Adamsky, Dmitry. 2015. "Cross-Domain Coercion: The Current Russian Art of Strategy." *Proliferation Papers* 54 (November):1–43.

Andrew, Christopher and Vasili Mitrokhin. 1999. *The Sword and The Shield: The Mitrokhin Archive and The Secret History of The KGB*. New York: Basic Books.

Antonov, S. I. et al. 2018. "*Modely ugroz sovmestnykh informatsionno-tekhnicheskikh i informatsionno-psikhologicheskikh vozdeystviy v gibridnykh voynakh* [Threat Models of Contemporary Information-Technical and Information-Psychological Impacts in Hybrid Wars]." *Informatsionnye Voyny* 2, no. 46:2–5.

Antonovich, P. I. 2011. "*O sushchnosti i soderzhanii kibervoyny* [On the Essence and Content of Cyber War]." *Voennaya Mysl*', no. 7:39–46.

Argumenty Vremeni. 2018. "*Osobyy front* [Special front]." October 1, 2018. https://svgbdvr.ru/voina/osobyi-front.

Balforth, Tom. 2018. "Putin Praises Skills of GRU Spy Agency Accused of UK Poison Attack." *Reuters*, November 2, 2018. https://www.reuters.com/article/us-britain-russia-putin/putin-praises-skills-of-gru-spy-agency-accused-of-uk-poison-attack-idUSKCN1N71YV.

Bazylev, S. I. et al. 2012. "*Deyateln'nost' Vooruzhennykh Sil Rossiyskoy Federatsii v informatsionnom prostranstve: printsipy, pravila, mery doveriya* [Activities of the Armed Forces of the Russian Federation in the Information Space: Principles, Rules, Confidence Building Measures]." *Voennaya Mysl*', no. 6:24–28.

Blank, Stephen. 2017. "Cyber War and Information War a la Russe." Carnegie Endowment for International Peace. October 16. https://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399.

Burenok, V. M., ed. 2018. *Kontseptsii perspektivnogo oblika silovykh kompontentov voennoy organizatsii Rossiyskoi Federatsii* [Concepts of the Perspective Appearance of the Power Components of the Military Organization of the Russian Federation]. Moscow: Russian Academy of Missile and Artillery Sciences (RARAN).

Burtsev, M. I. 1981. *Perelom. Prozreniye* [Fracture. Insight]. Moscow: Voyennoye Izdatel'stvo.

Chekinov, Sergey and Sergey Bogdanov. 2013. "*O haraktere i soderhanii voiny novogo pokoleniia* [On the Character and Contents of the New Generation War]." *Voennaya Mysl*', no. 10:13–24.

Chekinov, Sergey and Sergey Bogdanov. 2015a. "*Voennoe iskusstvo na nachal'nom etape XXI stoletiya: problemy i suzhdeniia* [Military art in the initial stage of the XXI century: problems and judgments]." *Voennaya Mysl*', no. 1 (January):34–45.

Chekinov, Sergey and Sergey Bogdanov. 2015b. "*Prognozirovanie kharaktera i soderzhaniia voin budushchego: problemy i suzhdeniia* [Predicting the character and content of a future warrior: challenges and judgments]." *Voennaya Mysl*', no. 10 (October):41–9.

Cheshuin, S. A. 2009. "*Osobennosti sovremennogo informatsionnogo protivoborstva i ikh uchod pri podgotovke spetsialistov zarubezhnoy voyennoy informatsii v voyennom universitete* [The Features of Modern Information Confrontation During the Training of Specialists of Foreign Military Information at the Military University]." http://www.milpol.ru/sgs/sgs.html.

Chivvis, Christopher. 2017. "Hybrid War: Russian Contemporary Political Warfare." *Bulletin of the Atomic Scientists*, (August):316–21. http://www.tandfonline.com/doi/abs/10.1080/00963402.2017.1362903?journalCode=rbul20;

Connell, Michael and Sarah Vogler. 2017. *Russia's Approach to Cyber Warfare*. Arlington: Center for Naval Analysis.

Council on Foreign Relations. 2008. Connect the Dots on State-Sponsored Cyber Incidents-Agent.btz. November. https://www.cfr.org/interactive/cyber-operations/agentbtz.

Digital Forensics Research Lab. 2018. "#TrollTracker: Russia's Other Troll Team." *Medium*, August 2, 2018. https://medium.com/dfrlab/trolltracker-russias-other-troll-team-4efd2f73f9b5.

Diresta, Renee and Shelby Grossman. 2019. *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019*. Stanford: Stanford Internet Observatory.

Doffman, Zak. 2019. "Russian Secret Weapon Against U.S. 2020 Election Revealed in New Cyberwarfare Report." *Forbes*, September 24, 2019. https://www.forbes.com/sites/zakdoffman/2019/09/24/new-cyberwarfare-report-unveils-russias-secret-weapon-against-us-2020-election/#68503ec468f5.

Dylevskiy, I. N., et al. 2016. "*O dialektike sderzhivaniya i predotvrashcheniya voyennykh konfliktov eru* [On the Dialectic of Deterrence and Prevention of Military Conflicts of the Era]." *Voyennaya Mysl*', no. 7 (July):5–13.

Faizova, Liana, et al. 2018. "*12 Khakerov GRU: v chem SShA obvinili ofitserov Rossiyskoy Voennoy Razvedki* [12 GRU Hackers: Of What the United States Accused the Russian Military Intelligence Officers]." *The Bell*, July 13, 2018. https://thebell.io/ssha-obvinili-12-ofitserov-gru-vo-vzlome-pochty-demokratov-v-2016-godu/.

Galeotti, Mark. 2018. "I'm Sorry for Creating the 'Gerasimov Doctrine'." *Foreign Policy*, March 5, 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

Gavrilov, Yuriy. 2013. "*Ryadovoy Khaker* [Private hacker]." *Rossiyskaya Gazeta*, July 11, 2013. https://rg.ru/2013/07/10/roty-site.html.

Gazeta.ru. 2006. "*Kak Rossiya borolas's «Kavkaz-tsentrom*» [How Russia fought the Kavkaz Center]." March 9, 2006. https://www.gazeta.ru/2006/03/09/oa_191473.shtml.

Gerasimov, Valery. 2013. "*Tsennost' Nauki v Predvidenii* [The Value of Science is in Foresight]." *Voyenno Promyshlennyy Kuryer*. February 26, 2013. http://vpk-news.ru/articles/14632.

Gerasimov, Valery. 2014. "On the Role of Military Force in Contemporary Conflicts." In *Conference Proceedings*, III Moscow Conference on International Security. Moscow: Ministry of Defense of the Russian Federation. https://eng.mil.ru/files/MCIS_report_catalogue_final_ENG_21_10_preview.pdf.

Gerasimov, Valery. 2019. "*Vektory razvitiya voennoy strategii* [Vectors for the Development of Military Strategy]." Red Star, March 4, 2019. http://redstar.ru/vektory-razvitiya-voennoj-strategii/.

Giles, Keir. 2011. "Information Troops – A Russian Cyber Command?" In *3rd International Conference on Cyber Conflict*, edited by C. Czosseck, E. Tyugu, and T. Wingfield, 45–60. Tallinn: CCD COE.

Giles, Keir. 2016. *Handbook of Russian Warfare*. Research Division, NATO Defense College. November.

Greenberg, Andy. 2017. "Petya Ransomware Epidemic May Be Spillover from Cyberwar." *Wired*, June 28, 2017. https://www.wired.com/story/petya-ransomware-ukraine/.

Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday.

Greenberg, Andy. 2020. "The US Blames Russia's GRU for Sweeping Cyberattacks in Georgia." *Wired*, February 20, 2020. https://www.wired.com/story/us-blames-russia-gru-sweeping-cyberattacks-georgia/

Habr.com. 2013. "*O nauchnykh rotakh programmistov* [On the Science Units of Programmers]." *Khabr*, August 16, 2013. https://habr.com/ru/post/285590/.

Harris, S. and B. Devlin. 2019. "U.S. Investigating Sci-Hub Founder." *Washington Post*, December 20, 2019.

Haslam, Jonathan. 2015. Near and Distant Neighbors: *A New History of Soviet Intelligence*. New York: Farrar, Strauss, and Giroux.

Iasiello, Emilio J. 2017. "Russia's Improved Information Operations: From Georgia to Crimea." *Parameters* 47:2.

Ignatius, David. 2017. "Russia's Radical New Strategy for Information Warfare." *Washington Post*, January 18, 2017. https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.

Izvestiya. 2016. "*Informatsionnoye protivoborstvo otrabotali na «Kavkaze-2016»*. Video [Information Confrontation Worked out in Caucasus-2016. Video]." September 14, 2016. https://iz.ru/news/632393.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. 2019. "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." *Journal of Strategic Studies* 42, no. 2:212–34.

Jonsson, Oscar. 2019. *The Russian Understanding of War*. Washington, DC: Georgetown University Press.

Kahn, David. 1996. *The Code-Breakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet*. New York: Scribner.

Kari, Martti J. 2019. *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – A Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats*. JYU Dissertations 122. University of Jyvaskyla. Faculty of Information Technology. October.

Kari, Martti J. and Katri Pynnöniemi. 2019. "Theory of Strategic Culture: An Analytical Framework for Russian Cyber Threat Perception." *Journal of Strategic Studies*, no. 11 (September):1–29.

Kavanaugh, Camino. 2015. "The UN GGE on Cybersecurity: The Important Drudgery of Capacity Building." *Council on Foreign Relations Blog*, April 2015. https://www.cfr.org/blog/un-gge-cybersecurity-important-drudgery-capacity-building

Kiselev, V. and A. Kostenko. 2015. "*Kibervoyna kak osnova gibridnoy operatsii* [Cyberwar as the Basis of Hybrid Operations]," *Armeiskii sbornik* 257, no. 11 (November):3–6.

Kofman, Michael. 2016. "Russian Hybrid Warfare and Other Dark Arts." *War on the Rocks*, March 11, 2016. https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Kompromat.ru. 2002. "'*Utro' i Tsentr Zarubezhnoy Voyennoy Informatsii i Kommunikatsii Ministerstva Obrony Rossiyskoy Federatsii Predstavlyayut 'Chechnya: dokumental'noye kino*' ['Morning' and the Center for Foreign Military Information and Communications of the Ministry of Defense of the Russian Federation Present 'Chechnya: documentary']." November 6, 2002. http://www.compromat.ru/page_12433.htm.

Kondrashov, Vyacheslav Viktorovich. 2016. "*Informatsionnoe protivoborstvo v kiberneticheskom prostranstve* [Information Confrontation in the Cybernetic Space]." Scientific-Research Center of National Security Problems. August. https://nic-pnb.ru/analytics/informatsionnoe-protivoborstvo-v-kiberneticheskom-prostranstve/

Kozlov, Sergey. 2010. *Spetsnaz GRU: bezvremen'ye 1989-1999* [GRU Special Forces: Timelessness 1989–1999]. Moscow: Russkaya Panorama.

Kozlov, Sergey. 2013. "'*Zima-Leto 1942 Goda.' Spetsnaz GRU: istoricheskiye predposylki sozdaniya Spetsnaza 1941-1945* ['Winter-Summer of 1942.' GRU Special Forces: Historical Background of the Creation of the Special Forces 1941–1945]", vol. 2. Moscow: Russkaya Panorama.

Krikunov, A. 2011. "*Kiberprostranstvo vedushchikh gosudarstv v kontekste sovremennykh vyzovov i ugroz* [Cyberspace of Leading States in the Context of Contemporary Challenges and Threats]" *Morskoy Sbornik* 11 (November): 32-37.

Kritukov, Evgeniy. 2018. "*Kak SShA nashli 'sotrudnikov GRU', 'vmeshavshikhsya v vybory*' [How the United States found 'GRU officers', 'interfering in the elections']." *Vzglyad*, July 16, 2018. https://vz.ru/politics/2018/7/16/932761.html.

Kuznetsov, Sergey, Vasily Anisimov, Sergey Teslya, Igor Morozov. 2018. "*Kiberoperatsiya kak vid boyevykh deystviy* [Cyber Operations as a Kind of Mililtary Action]". *Zashchita i bezopasnost'* 1, no. 84:5.

Larin, D. A. 2017. *Kriptograficheskaya sluzhba Rossii: ocherki istorii* [Cryptographic Service of Russia: Essays on History]. Helios ARV.

Livejournal.com. 2015. "*Den' innovatsiy Ministerstva Oborony Rossii* [Innovation day of the Ministry of Defense of Russia]." October 6, 2015. https://bmpd.livejournal.com/1505576.html.

Medvedev, Sergei. 2015. "Offense-Defense Theory Analysis of Russian Cyber Capability." California: Naval Postgraduate School. https://pdfs.semanticscholar.org/19e3/ca12d73661182bd2a9e34dc2df81634deacf.pdf.

Mikryunov, V. Yu. 2015. "*Kak protivostoyat' agressii SSHA* [How to Resist U.S. Aggression]." *Vestnik Akademii voennykh nauk* 51, no. 2: 116–23.

Ministry of Defense of the Russian Federation. 2011. "*Kontseptual'nye vzglyady na deyatel'nost' Vooruzhennykh Sil Rossiyskoy Federatsii v informatsionnom prostranstve* [Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space]." http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

Ministry of Defense of the Russian Federation. 2018. "*Prikazanie OPr/ 156* [Order OPr/156]." March 1. https://www.omgtu.ru/general_information/faculties/faculty_of_transport_oil_and_gas/deanary/news/2018/%D0%AD%D0%A0%D0%90%2009032018.pdf

Ministry of Foreign Affairs of the Russian Federation. 2000. "National Security Concept of the Russian Federation." January 10. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768.

Ministry of Foreign Affairs of the Russian Federation. 2011. "*Konventsiya ob obespechenii mezhdunarodnoy informatsionnoy bezopasnosti (kontseptsiya)* [Convention on International Information Security (Concept)]." September 22. https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

Ministry of Foreign Affairs of the Russian Federation. 2013. "*Kontseptsiya vneshnoi politiki Rossiyskoi Federatsii* [Foreign Policy Concept of the Russian Federation]." February 12. http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/122186.

Morris, Lyle J. et al. 2019. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. Santa Monica: RAND Corporation. https://www.rand.org/pubs/research_reports/RR2942.html.

Moscow-Russia.ru. n.d. "*Voyennyy Universitet Ministerstva Oborony Rossiyskoy Federatsii* [Military University of the Ministry of Defense of the Russian Federation]." http://moscow-russia.ru/voennyy-universitet-ministerstva-oborony/.

Moscow State Budgetary General Education Institute, School 1517. 2017. "*Soglashenie o sotrudnichestve v oblasti obrazovaniya* [Agreement on cooperation in the area of education]." May 19, 2017. https://1517.mskobr.ru/files/soglashenie_o_sotrudnichestve_v_oblasti_obrazovaniya_1517_akademiya.pdf

Nakashima, Ellen. 2017. "Inside a Russian Disinformation Campaign in Ukraine in 2014." *Washington Post*, December 25, 2017. https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html.

Nakashima, Ellen. 2018. "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes." *Washington Post*, January 13, 2018. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Nauchnaya Rota REB. 2015. "This Is a Recruiting Video for the Military Science Unit Dedicated to Electronic Warfare." *YouTube*. July 8, 2015. https://www.youtube.com/watch?time_continue=2&v=XoaR_0iANVA&feature=emb_logo.

Nezavisimaya Gazeta. 2000. "*Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii* [Doctrine of Information Security of the Russian Federation]." September 15, 2000. http://www.ng.ru/politics/2000-09-15/0_infodoctrine.html.

Newsru.com. 2002. "*Tomskie khakery 3 goda vedut informatsionnuyu voynu protiv chechenskikh ekstremistov* [Hackers from Tomsk conducted an information war against Chechen extremists for three years]." January 30, 2002. https://www.newsru.com/russia/30Jan2002/hakery.html.

Parshin, S. and N. Bashkirov. 2019. "*Kiberugrozy i mezhdunarodnaya stabilnost*' [Cyberthreats and International Stability]." *Zarubezhnoe voennoe obozrenie*, no. 11 (November):3–10.

President of Russia. 2010. "*Voyennaya doktrina Rossiyskoy Federatsii* [Military Doctrine of the Russian Federation]." February 5. http://kremlin.ru/supplement/461.

President of Russia. 2016. "*Ob utverzhdenii doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii* [On Approving the Doctrine of Information Security of the Russian Federation]." May 12. http://kremlin.ru/acts/bank/41460/page/1.

Putin, Vladimir. 2012. "Vladimir Putin: *Byt' sil'nymi: garantii national'noy bezopasnosti dlya Rossii* [Be Strong: National Security Guarantees for Russia]." Rossiyskaya Gazeta no. 35 (February): 5708. https://rg.ru/2012/02/20/putin-armiya.html

Repko, S.I. 1999. *Voyna i propaganda, XV-XX vv*. [War and Propaganda, 15th–20th Centuries] Moscow: Novosti.

Ren.tv. 2019. "*Oruzhie budushchevo: Putin osmotrel sekretnye obraztsy vooruzheniya na 'Armiya-2019*' [Weapons of the Future: Putin Inspected Secret Weapons at 'Army 2019']." June 27, 2019. https://www.youtube.com/watch?v=Dviw_oSN4Yg.

Romashkina, N. P. And A. B. Kildobskiy. 2015. "*Novye metody protivoborstva XXI veka* [New XXI Century Methods of Confrontation]." *Vestnik Akademii voennykh nauk*, no. 1:134–39.

Rossiyskaya Gazeta. 2009. "*Postanovlenie pravitel'stva Rossiyskoy Federatsii ot 10 marta 2009 g. N 221 Moskva 'O prisuzhdenii premiy pravitel'stva Rossiyskoy Federatsii 2008 goda v oblasti nauki i tekhniki*' [Resolution of the Government of the Russian Federation from March 10, 2009 No. 221, Moscow 'On Awarding Prizes of the Government of the Russian Federation in 2008 in the Field of Science and Technology']." No. 0 (4872). March 20, 2014. https://rg.ru/2009/03/20/premii-nauk-tech-dok.html.

Rossiyskaya Gazeta. 2014. "*Voennaya doktrina Rossiyskoy Federatsii* [Military doctrine of the Russian Federation]." no. 298 (6570). December 30, 2014. https://rg.ru/2014/12/30/doktrina-dok.html.

Saltykov,Yevgeniy. 2014. "*V Rossii sozdany kibervoyska* [Cyber Forces Created in Russia]." *Vesti.ru*, May 12, 2014. https://www.vesti.ru/doc.html?id=1573024.

Security Council of the Russian Federation. 2013. "*Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti na period do 2020 goda* [Fundamentals of State Policy of the Russian Federation in the Field of International Information Security for the Period until 2020]." http://www.scrf.gov.ru/security/information/document114/.

Selivanov, V. V. 2020. "*O kompleksirovanii sredstv i sposobov podgotovki asimmetrichnykh otvetov pri obespechenii voyennoy bezopasnosti* [On Integrating Means and Methods for Preparing Asymmetric Responses in Ensuring Military Security]," *Voennaia mysl*', no.1 (January):48–60.

Sengupta, Kim. 2018. "Russian Spy Agency GRU Responsible for International Cyberwar UK Government Says." *Independent*, October 4, 2018. https://www.independent.co.uk/news/world/europe/russia-gru-sergei-skripal-hacking-cyber-war-donald-trump-elections-a8567356.html.

Shevyakin, Aleksandr. 2014. *KGB: sistema bezopasnosti SSSR [KGB: USSR Security System]*. Moscow: Algoritm.

Shil'bakh, K, and V. Sventsitskiy. 1927. *Voennye Razvedki* [Military Intelligence]. Moscow: Military Typography Directorate.

Slatter, Raphael. 2018. "Russian Hacking Europe Russia U.S. News Russian Hackers Posed as IS to Threaten Military Wives." *AP News*, May 8, 2018. https://apnews.com/4d174e45ef5843a0ba82e804f080988f/Russian-hackers-posed-as-IS-to-threaten-military-wives.

Starodubtsev, Y. I., V. V. Bukharin, and S. S. Semyonov. 2012. "*Tekhnosfernaya voyna* [Technosphere war]." *Voyennaya Mysl*' 7: 22–31.

TASS. 2014. "*Istochnik v Minoborony: v Vooruzhennykh Silakh RF sozdany voyska informatsionnykh operatsiy* [Source in the Ministry of Defense: Information Operations Troops Created in the Armed Forces of the Russian Federation]." May 12, 2014. https://tass.ru/politika/1179830.

Thomas, Timothy. 2019. *Russian Military Thought: Concepts and Elements*. The MITRE Corporation. Arlington, VA. August.

Thomas, Timothy. 2010. "Russian Information Warfare Theory: The Consequences of August 2008." In *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, edited by Stephen Blank and Richard Weitz. Carlisle: U.S. Army War College: 265-99.

Tikk, Eneken and Kerttunen, Mika. 2018. *Parabasis Cyber-diplomacy in Stalemate*. Norwegian Institute of International Affairs.

Tribun. 2018. "*Stali izvestny dannye o voyskakh «psikhov» Rossii* [Data on the Psycho Troops of Russia Became Known]." February 6, 2018. https://tribun.com.ua/47273.

Troianovski, Anton and Ellen Nakashima. 2018. "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West." *Washington Post*, December 28, 2018. https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

Turovsky, Daniil. 2016."*Rossiyskiye vooruzhennyye kibersily. Kak gosudarstvo sozdayet voyennyye otryady khakerov* [Russian Armed Cyber Forces like a State Create Military Hacker Units]." *Meduza*, November 7, 2016. https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily.

Turovsky, Daniil. 2018. *Vtorzheniye: kratkaya istoriya russkikh khakerov [Invasion: A Brief History of Russian Hackers]*. Moscow: Inviduum.

Turovsky, Daniil and Rothrock, Kevin. 2018. "'It's Our Time to Serve the Motherland' How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers." *Meduza*, August 7, 2018. https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

U.S. Cyber Command. 2018. "Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command. " June 14. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

U.S. Department of The Treasury. 2018. "Treasury Sanctions Russian Federal Security Service Enablers." June 11 https://home.treasury.gov/news/press-releases/sm0410.

Vorob'ev, I. and V. Kiselev. 2013. "*Kibervoyna* [Cyber War]," Armeiskii sbornik, no. 8 (August):33–4.

Znamensk Garrison Military Court. 2011. "*Obzor sudebnoy praktiki rassmotreniya voennymi sudami grazhdanskikh del v 2010 godu* [Review of Judicial Practice of the Military Courts Review of Civil Cases in 2010]." February 28. http://znamenskygvs.ast.sudrf.ru/modules.php?name=docum_sud&id=336.