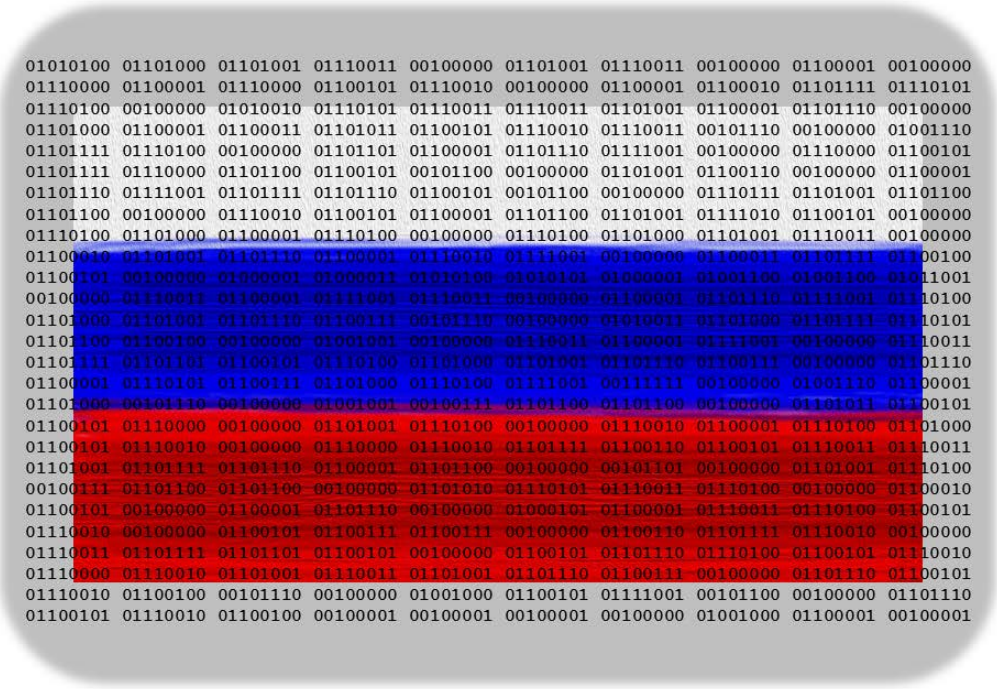
# Russia's Approach to Cyber Warfare

Michael Connell and Sarah Vogler

March 2017



CNA
ANALYSIS & SOLUTIONS

CNA
ANALYSIS & SOLUTIONS

CNA's Occasional Paper series is published by CNA, but the opinions expressed are those of the author(s) and do not necessarily reflect the views of CNA or the Department of the Navy.

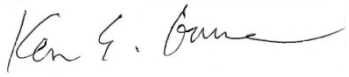
**Distribution**

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
PUBLIC RELEASE. 3/24/2017

Other requests for this document shall be referred to CNA Document Center at inquiries@cna.org.

**Photography Credit:** Cover art designed by Christopher Steinitz, CNA.

**Approved by:** **March 2017**



Ken E. Gause, RTL
International Affairs Group
Center for Strategic Studies

This work was performed under Federal Government Contract No. N00014-16-D-5003.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 03-2017 | 1Rev | |

**4. TITLE AND SUBTITLE**
Russia's Approach to Cyber Warfare

**5a. CONTRACT NUMBER**
N00014-16-D-5003

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**
0605154N

**6. AUTHOR(S)**
Michael Connell, Sarah Vogler

**5d. PROJECT NUMBER**
**R0148**

**5e. TASK NUMBER**
B69000

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Center for Naval Analyses
3003 Washington Blvd
Arlington, VA 22201

**8. PERFORMING ORGANIZATION REPORT NUMBER**
DOP-2016-U-014231-1Rev

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Office of the Chief of Naval Operation
(OPNAV N81)
Navy Department Pentagon
Washington, DC 20350

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

Russia views cyber very differently than its western counterparts, from the way Russian theorists define cyberwarfare to how the Kremlin employs its cyber capabilities. The paper examines the Russian approach to cyber warfare, addressing both its theoretical and its practical underpinnings.

**15. SUBJECT TERMS**
Russia, Cyber, Hacking, APT 28, APT 29, Ukraine, Baltic, Estonia, Georgia, NATO

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Knowledge Center/Robert Richards |
| U | U | U | SAR | 38 | 19b. TELEPHONE NUMBER *(include area code)* 703-824-2123 |

# Executive Summary

Russia views cyber very differently than its western counterparts, from the way Russian theorists define cyberwarfare to how the Kremlin employs its cyber capabilities. The paper examines the Russian approach to cyber warfare, addressing both its theoretical and its practical underpinnings. The following is a summary of its key findings:

- Russian officials are convinced that Moscow is locked in an ongoing, existential struggle with internal and external forces that are seeking to challenge its security in the information realm. The internet, and the free flow of information it engenders, is viewed as both a threat and an opportunity in this regard.

- Russian military theorists generally do not use the terms cyber or cyberwarfare. Instead, they conceptualize cyber operations within the broader framework of information warfare, a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations.

- In keeping with traditional Soviet notions of battling constant threats from abroad and within, Moscow perceives the struggle within "information space" to be more or less constant and unending. This suggests that the Kremlin will have a relatively low bar for employing cyber in ways that U.S. decision makers are likely to view as offensive and escalatory in nature.

- Offensive cyber is playing a greater role in conventional Russian military operations and may potentially play a role in the future in Russia's strategic deterrence framework. Although the Russian military has been slow to embrace cyber for both structural and doctrinal reasons, the Kremlin has signaled that it intends to bolster the offensive as well as the defensive cyber capabilities of its armed forces. During the contingencies in Georgia and Ukraine, Russia appeared to employ cyber as a conventional force enabler.

- The Georgia and Ukraine conflicts also provided opportunities for Russia to refine their cyberwarfare techniques and procedures and to demonstrate their capabilities on the world stage. These demonstrations may later serve as a basis to signal or deter Russia's adversaries.

- Hacktivists and cyber-criminal syndicates have been a central feature of Russian offensive cyber operations, because of the anonymity they afford and the ease with which they can be mobilized. However, the crowd-sourced

approach that has typified how the Kremlin has utilized hackers and criminal networks in the past is likely to be replaced by more tailored approaches, with the FSB and other government agencies playing a more central role.

# Contents

Introduction ..... 1

Cyber as a Subcomponent of Information Warfare (IW) ..... 3

Organizations and agencies ..... 7

Hacktivists and criminals ..... 10

Estonia (2007): A Cyber Milestone ..... 13

Georgia (2008): Cyber in Conjunction with Conventional Operations ..... 17

Ukraine (2013-present): Cyber Used to Generate Kinetic Effects ..... 19

Bots, Leaks, and Trolls: Cyber's Role in Enabling Russian Propaganda ..... 23

Conclusion ..... 27

This page intentionally left blank.

# Introduction

Understanding the behavior of adversaries in the cyber domain can often be challenging. Attribution issues, the technical nature of cyberwarfare, its recent and rapid evolution, its ephemeral effects, and the covert ways in which it is often used tend to obscure the motivations and strategies of the actors involved. The conceptual challenges associated with cyber mean that threats are often analyzed from a purely tactical and defensive perspective. Media reporting and forensic analysis usually focus on the origins and vectors of cyberattacks, the techniques and tools they use, their impact, and how their effects can be defended against or mitigated. Broader strategic questions, such as why the adversary conducts cyberattacks, what they are intended to achieve, how the adversary perceives risk and escalation in cyberspace, and whether the attacks can be deterred, are often overlooked or given only cursory notice.

Because of the relative dearth of analysis in this area, we tend to mirror image when analyzing our adversaries in cyberspace, to an even greater degree than in other warfare domains. We make uninformed assumptions about their motivations, intentions, and risk calculus based on U.S. thinking about cyber. However, this can be misleading, and in some instances, dangerous. Adversaries—whether state or non-state actors—are likely to view interactions in cyberspace very differently than we do. How they integrate cyber into other warfare domains, how they calculate risk and perceive escalation in cyberspace, and the strategies they use to achieve their objectives in cyberspace are all likely to vary by considerable degrees. In more succinct terms, a one-size-fits-all approach to dealing with adversaries in cyberspace will not work.

This paper is an attempt to address these issues as they pertain to a particularly potent cyber adversary: Russia. Russia's cyber capabilities are highly advanced, and Moscow has demonstrated a willingness to employ offensive cyber in situations other than war to affect political and economic outcomes in neighboring states and to deter its adversaries. According to James Clapper, the Director of National Intelligence,

> Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny. Russian cyber operations are likely to target US interests to support several strategic objectives: intelligence gathering to support Russian decision-making in the Ukraine and Syrian crises, influence operations to support military and political objectives, and continuing preparation of the cyber environment for future contingencies.[1]

From the way Russia defines cyberwarfare to its employment for strategic use, Russia views cyber differently than its western counterparts. As James Wirtz has noted, "Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives."[2] To counter this strategy, U.S. policymakers and military planners need to understand how Russia integrates cyberwarfare concepts into its broader military and security strategies. This paper addresses this issue from a theoretical as well as a practical perspective, first by analyzing Russian doctrine and official writings and statements about cyberwarfare and then by examining how Russian cyber forces have operated in real-world scenarios.

[1] James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*. Senate Armed Services Committee, February 9, 2016. Accessed at https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

[2] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power Into Grand Strategy," in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications: Tallinn, 2015, 31.

# Cyber as a Subcomponent of Information Warfare (IW)

The Russians generally do not use the terms cyber *(kiber)* or cyberwarfare *(kibervoyna),* except when referring to Western or other foreign writings on the topic. Instead, like the Chinese, they tend to use the word informatization, thereby conceptualizing cyber operations within the broader rubric of information warfare (*informatsionnaya voyna*). The term, as it is employed by Russian military theorists, is a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations.[3] In other words, cyber is regarded as a mechanism for enabling the state to dominate the information landscape, which is regarded as a warfare domain in its own right. Ideally, it is to be employed as part of a whole of government effort, along with other, more traditional, weapons of information warfare that would be familiar to any student of Russian or Soviet military doctrine, including disinformation operations, PsyOps, electronic warfare, and political subversion.

The ramifications of this conceptual distinction—both for how the Russians use cyber and under what circumstances—are considerable. According to the Military Doctrine of the Russian Federation (2010), one of the features of modern military conflicts is "*the prior implementation of measures of information warfare* in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force."[4] By implication, the tools of information warfare can—in fact, should—be brought to bear before the onset of military operations in order to achieve the state's objectives without having to resort

[3] For a more detailed examination of cyber's role in Russian information warfare doctrine, see Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," London: Chatham House, March 2016; Timothy L. Thomas, "Nation-State Cyber Strategies: Examples From China and Russia," accessed at http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-20.pdf; and Wirtz, op cit.

[4] *The Military Doctrine of the Russian Federation*, approved by Russian Federation presidential edict on February 5, 2010 (translated). Accessed at http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

to the use of force, or, should force be required, disorienting and demoralizing the adversary and ensuring that the state is able to justify its actions in the eyes of the public. Thus, information warfare, and by extension cyber, becomes a legitimate tool of the state in peacetime as well as wartime.[5]

General Valery Gerasimov, Chief of the General Staff of the Russian Federation, alluded more generally to the peacetime employment of information operations in his now famous article, "The Value of Science in Prediction":

> In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template. The experience of military conflicts — including those connected with the so called coloured revolutions in North Africa and the Middle East — confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war.[6]

He goes on to state, "The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy. In North Africa, we witnessed the use of technologies for influencing state structures and the population with the help of information networks."[7]

Russian military thinkers on information operations IO and asymmetric military tactics, Col. S.G. Chekinov (Res.) and Lt. Gen. S.A. Bogdanov (Ret.), observed that information could be used to disorganize governance, organize anti-government protests, delude adversaries, influence public opinion, and reduce an opponent's will to resist.[8] Cyber IO affords the Russian government covert means to achieve these

[5] Timothy L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008," in *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Ed. Stephen J. Blank and Richard Weitz (U.S. Army War College, Carlisle, PA: Strategic Studies Institute, 2010), 266. Accessed at http://www.strategicstudiesinstitute.army.mil/pdffiles/pub997.pdf.

[6] Quoted in Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," BLOG: In Moscow's Shadows. Accessed at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[7] Ibid.

[8] These observations were published in the Russian military journal, *Military Thought,* after the annexation of Crimea. Col. Sergei G. Chekinov (Res.) and Lt. Gen. Sergei A. Bogdanov (Ret.). "The Art of War in the Early 21st Century: Issues and Opinions." *Military Thought,* 2015 (24) via Margarita Levin Jaitner, "Russian Information Warfare: Lessons From Ukraine," Chapter 10 in

objectives, allowing Russia to maintain a degree of plausible deniability with regard to its participation in disinformation campaigns. Furthermore, Chekinov and Bogdanov noted that a critical component of IO is to begin information operations before the onset of traditional military operations as a means of preparing the potential battle space.[9] Again, cyber IO facilitates this concept. This perspective is consistent with Gerasimov's observation that "in the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory."[10]

Offensive cyber is thus relegated to a supporting—albeit significant—role in helping the state achieve information dominance in all the stages of conflict. In keeping with traditional Leninist notions of battling constant threats from abroad and within, the confrontation within "information space" is more or less constant and unending.[11] It knows no boundaries, physical or temporal. This contrasts sharply with Western—and particularly U.S.—conceptions of cyber, which is viewed as a separate domain, distinct from information warfare and its associated psychological aspects.

Perhaps not surprisingly, given the broad conception of IW in Russian theory, the focus of Russia's cyber operations also tends to be strategic and long term in nature, rather than operational or tactical. According to Steven Blank,

> while Russian theorists have discussed what they call the information-strike operation against enemy forces, which was evidenced in the 2008 war with Georgia, most actual uses of information weapons in operations have aimed at the domestic "nerves of government" or of society, not combat forces or military command and control. Indeed, the "information-psychological" aspect that covers the use of the press and the media broadly conceived

Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression Against Ukraine, NATO CCD COE Publications, Tallinn, 2015 (89).

[9] Col. Sergei G. Chekinov (Res.) and Lt. Gen. Sergei A. Bogdanov (Ret.). "The Art of War in the Early 21st Century: Issues and Opinions." *Military Thought*, 2015 (24) via Margarita Levin Jaitner, "Russian Information Warfare: Lessons from Ukraine," Chapter 10 in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications, Tallinn, 2015 (89).

[10] Col. S.G. Chekinov and Lt. Gen. S.A. Bogdanov. "The Nature and Content of a New-Generation War." *Voyenna mysl* [Military Thought in English Translation], No.4, (October 2013) at http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf via Bret Perry. "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations." *Small Wars Journal,* August 2015. Available at http://smallwarsjournal.com/print/27014#_edn35, accessed September 15, 2015.

[11] Thomas, 266.

> against a target's information space is a key category among many in the Russian definition of IO and IW.[12]

This strategic emphasis has, in turn, influenced—or been influenced by—how Russia has organized and postured its cyber forces.

[12] Stephen J. Blank, "Information Warfare a la Russe," in *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*, Phil Williams and Dighton Fiddner (Eds.), Strategic Studies Institute and U.S. Army War College Press, August 2016, 219-220.

# Organizations and agencies

The Russian military is a relative latecomer to the cyber arena. For many years, cyber was the exclusive domain of the state's security services. The Federal Security Service *(Federal'naya Sluzhba Bezopastnosti*: FSB), for instance, appears to be the Federation's lead actor for coordinating cyber propaganda and disinformation campaigns. It also maintains and operates SORM, the State's internal cyber surveillance system.[13] The Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications *(Roskomnadzor),* which is responsible for overseeing the media, including the electronic media, and mass communications, information technology and telecommunications), controls information blacklists and regulates the media. Directorate K of the Ministry of Internal Affairs *(Ministerstvo Vnutrennikh Del*: MVD) focuses on cyber crime.[14] For a brief period in the 1990s, Russia had a separate information security agency, the Federal Agency for Government Communications and Information *(Federal'noe Agentstvo Pravitelstvennoi Svyazi I Informatsii*: FAPSI). In 2003, however, FAPSI was disbanded, and its components were absorbed into the FSB, the MVD, the Federal Protective Service of the Russian Federation (FSO RF), and the SVR, Russia's foreign intelligence service.[15] Together, these agencies have established the parameters of Russian cyber doctrine and been responsible for coordinating most of the state's internal and external cyber operations.[16]

[13] See Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, Public Affairs, 2015.

[14] Sergei A. Medvedev, "Offense-defense Theory Analysis of Russian Cyber Capability," Monterey, California: Naval Post Graduate School, MA Thesis, March 2015, 58.

[15] According to Giles, "…the FSB received the Main Directorate for Radio-Electronic Reconnaissance on Communications Networks *(Glavnoye upravlenye radioelektronnoy razvedki sredstv svyazi*, GURRSS). The influence of this body in directing policy today could be inferred from the fact that the former chief of FAPSI and of the GURRSS, Vladislav Sherstyuk, holds the information security portfolio on the Security Council and is also the head of the Department of Information Security at Moscow State University." "'Information Troops' -- a Russian Cyber Command?" 2011 3rd International Conference on Cyber Conflict, C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011.

[16] Interview, Moscow, April 2016.

By contrast, the military's cyber remit was, until recently, limited to those areas where cyber overlaps with the field of electronic warfare. However, this changed somewhat in the wake of Russia's conflict with Georgia in 2008. Although the conflict resulted in a victory for Russia's forces, it also exposed serious operational and organizational deficiencies, including in the area of information operations. As a result, the Ministry of Defense (MOD) announced—along with other military reforms—that it would establish a branch in the military responsible for conducting information operations, complete with specially trained and equipped troops. According to one source,

> these troops would include hackers, journalists, specialists in strategic communications and psychological operations, and, crucially, linguists to overcome Russia's now perceived language capability deficit. This combination of skills would enable the Information Troops to engage with target audiences on a broad front, since for information warfare objectives the use of "mass information armies" conducting a direct dialogue with people on the internet is more effective than a "mediated" dialogue between the leaders of states and the peoples of the world.[17]

Little came of this proposal, however. The military had entered an already crowded field, and the FSB, which resented the military's intrusion onto its turf, publicly opposed the initiative.[18] The idea did not die, however, and, in 2013, the government announced that it would be creating a cyber unit in the military whose responsibilities would include offensive and defensive cyber operations, as well as a cyber research and development agency, called the Foundation for Advanced Military Research.[19] Major-General Yuri Kuznetsov confirmed to local media in January 2014 that the country was seeking to complete the staggered formation of these military cyber units by 2017, but their current status is unknown. According to Moscow-based sources, the military is having trouble recruiting qualified applicants for its cyber forces.[20] Not surprisingly, recruits have better and more lucrative prospects in the

[17] Giles, "Russia's 'New' Tools," 29.

[18] Interview, Moscow, May 2016. University graduates with computer science backgrounds are difficult to recruit because they tend to have better job options in the private tech sector. Conscripts, on the other hand, are not a viable option because their term of service in the Russian military (one year) is too short for them to be trained and utilized in an effective manner.

[19] Official sources in the MOD reported that the budget for this agency for 2013 amounted to 2.3 billion rubles ($70 million). See http://day.kyiv.ua/ru/article/ekonomika/krym-rossiyskaya-kiberstrategiya-voyny.

[20] Interview, Moscow, April 2016.

private sector, and conscripts serve for too limited a period of time (usually one year) to be effectively trained in a highly specialized field. Over the long term, however, if the Russian military manages to successfully develop its own organic offensive cyber capabilities, the result could be an increasing use of cyber to support conventional military operations.

# Hacktivists and criminals

Cyber hacking groups, or advanced persistent threat (APT) groups, have become a central part of Russia's cyber-IO toolkit. While direct links to the Russian government are difficult to prove conclusively—the Russian government denies that it sponsors any hacker groups—there are a number of groups whose activities are closely aligned with the Kremlin's objectives and worldview. Russia is not unique in this regard: China, Iran, North Korea, and other cyber adversaries have been known to outsource their operations to non-state actors. Where Russia differs from these other adversaries is its success in this regard. To begin with, Russia has been enabled by its ability to draw on a vast, highly skilled, but underemployed community of technical experts. According to David Smith,

> Russia is a typical extractive economy that still enjoys the benefits of the quite good Soviet educational system. Great wealth is concentrated in the hands of a few, while many people with training in math, science and computers look for work. The result is a thriving botnet-for-hire industry.[21]

Russian and other East European hackers are also widely regarded as the best in the world, to the extent that they are sometimes hired by other states to conduct cyberattacks on their behalf. For example, Russian hackers were suspected of being behind North Korea's hack of Sony Pictures.[22]

[21] David Smith, "How Russia Harnesses Cyber Warfare," Defense Dossier, American Foreign Policy Council (August 2012: Issue 4), 9. Accessed at http://www.afpc.org/files/august2012.pdf.

[22] "New Evidence Shows Russian Hackers Have Access to Sony's Network," https://taia.global/2015/02/new-evidence-shows-russian-hackers-have-access-to-sonys-network/ According to TAIA forensics reports, the hackers behind the Sony attack, the self-identified "Guardians of the Peace," are probably a Russian hacker who carries out occasional contract work for the FSB, in this case, working on behalf of the North Korean government. In this See also Thomas Fox-Brewster, "Forget North Korea - Russian Hackers Are Selling Access To Sony Pictures, Claims US Security Firm," Forbes, accessed at http://www.forbes.com/sites/thomasbrewster/2015/02/04/russians-hacked-sony-too-claims-us-firm/#3be85e426f27

Endemic corruption and a weak rule of law have also provided opportunities for collaboration with the cyber underworld. Laws are enforced arbitrarily, as a result of which cyber syndicates thrive. The services provided by these groups include:

- Organization of distributed denial of service (DDoS) attacks
- Testing malware for antivirus detection
- "Packing" of malware (changing malicious software with the help of special software (packers) so that it is not detected by antivirus software)
- Renting out exploit packs
- Renting out dedicated servers
- VPN (providing anonymous access to web resources, protection of the data exchange)
- Renting out abuse-resistant hosting (hosting that does not respond to complaints about malicious content and, therefore, does not disable the server)
- Renting out botnets
- Evaluation of stolen credit card data and services to validate the data.[23]

Syndicates, such as the now infamous (and defunct) Russian Business Network (RBN), are often tolerated because they provide services that the state needs and income to government cronies.[24]

The reasons why Russia relies on cyber proxies are twofold. First, it's cost effective. Proxies require little in the way of technical support. In many of the incidents detailed below, the hackers only needed to be given a target list with vectors of attack and then be unleashed. Hackers can also be mobilized relatively quickly, and disbanded when they are no longer needed. Hacktivists—political/nationalist hackers, of which Russia has many—will often work for free, provided that the issue accords with their own world view. Second, hackers are ideal for operating in the grey zone of information warfare because they provide an extra degree of anonymity for the Kremlin, further compounding the attribution issues associated with

[23] This list is excerpted from Ruslan Stoyanov, "Russian Financial Cybercrime: How It Works," Secure List Report, November 19, 2015. Accessed at https://securelist.com/analysis/publications/72782/russian-financial-cybercrime-how-it-works/

[24] Peter Warren, "Hunt for Russia's Web Criminals," The Guardian Online Edition, November 15, 2007. Accessed at https://www.theguardian.com/technology/2007/nov/15/news.crime.

cyberspace. Even extensive forensic investigations rarely result in a "smoking gun" that can be tied to government computers or associated IP addresses. From a deterrence or compellence perspective, the outcome is ideal for Moscow, because its adversaries expect Russian government involvement, but they usually lack definitive proof to hold the Kremlin to account for its actions. Like classic gangster protection racket schemes, the Kremlin can disavow the actions of its guns-for-hire with a wink, while darkly hinting that more things could "break" unless its adversaries pay up and behave.

# Estonia (2007): A Cyber Milestone

In the previous sections, we outlined some of the theoretical and structural underpinnings of how Russia approaches offensive operations in cyberspace. In this section, we adopt a more empirical approach, examining recent examples of how Russia has employed its offensive cyber capabilities in order to derive observations based on patterns of behavior.

The first case study we examine is that of Estonia. The DDoS attacks against Estonia during April and May 2007 constitute the first large-scale coordinated use of cyber by Russia to affect a strategic outcome in a neighboring state. For a period of about a month, Estonia's internet websites were flooded with pings and network-clogging data, forcing most sites to either shut down or sever their international connections (thus rendering much of the country's ability to communicate or share information efficiently with the outside world unusable). The impact on Estonia was significant; the country prided itself on being at the forefront of information technology and, at the time, approximately 60 percent of the country's 1.3 million people used the internet regularly and the government considered itself effectively "paperless." As Urmas Paet, Estonia's foreign minister at the time put it, "the attacks [were] virtual, psychological, and real."[25]

Estonian officials attributed the cyberattacks to Russia, believing them to be in retaliation for the decision by the Estonian government to move a bronze statue of a Soviet soldier from a central place in Tallinn to a more remote military cemetery. Tensions over the statue had been building, with Russia decrying the removal of the statue which commemorated the sacrifice of Soviet soldiers in the liberation of Estonia from Nazi Germany as an insult to Estonia's minority ethnic Russian population.[26] Following the removal of the statue on April 27, protests and

[25] Joshua Davis. "Hackers Take Down the Most Wired Country in Europe." *Wired* (online), August 21, 2007, available at http://www.wired.com/2007/08/ff-estonia/.

[26] In 2007, approximately 26 percent of Estonia's population was characterized as ethnically Russian by Statistics Estonia (government census bureau). "Population by ethnic nationality, 1 January, year." Tallinn, updated October 13, 2010, available at http://www.stat.ee/34278 via Stephen Herzog. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60, p. 51.

demonstrations by ethnic Russians in Estonia turned violent and resulted in the arrest of 1,300 individuals and the death of one.

During that same time, the first DDoS attacks began targeting Estonian websites. During the first wave, DDoS attacks were used to overwhelm Estonian servers. The targets were Estonian government sites, including Parliament's webpage, websites of political parties, the country's largest banks, and the country's most prominent news and telecommunications outlets. While Estonians insisted on a Russian hand, the activity appeared to be originating from botnets all over the world, including Egypt, Vietnam, and Peru. Indeed, instructions for conducting the ping attacks were posted online, as well as guidance for how to target specific Estonian websites.[27]

Estonia reached out to the world for help. In early May, internet service providers (ISPs) worked with Estonian authorities to block malicious data and defend Estonia's networks.[28] The attacks began to trail off, but a second, more sophisticated wave of attacks hit the country over May 8-9 (in conjunction with Russia's national holiday commemorating Soviet victory over Germany in World War II). In the second wave, botnets – hijacked computers around the world – again flooded Estonian internet addresses with erroneous data, forcing them to shut down or disconnect from international connections. Over the course of May 8-9, 58 separate botnet attacks targeted Estonia. At one point, Hansabank, Estonia's largest bank, was forced to shut down its online operations.[29] A third wave of attacks occurred a week later, wherein hackers who infiltrated individual websites defaced the sites and posted their own messages.[30] By late May 2007, the attacks had subsided.

Although the attacks on Estonia cannot be positively attributed to Russian state actors, their timing, and the effects they generated, suggested they were part of a larger, coordinated information operations campaign by the Kremlin employing multiple tools of influence. After the riots and cyberattacks began, the Russian Federation Council called for the freezing of diplomatic ties with Estonia and the imposition of economic sanctions. When Russian nationalist youth groups attacked the Estonian embassy in Moscow, police failed to intervene. An unofficial blockade also disrupted trade on the border between the two states.[31] The hackers appear to

[27] Davis, 2007.

[28] Mark Lander and John Markoff. "Digital Fears After Data Siege in Estonia." *New York Times* (online). May 29, 2007, available at http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=0.

[29] Landler and Markhoff, 2007.

[30] Davis, 2007.

[31] Medvedev, 21.

have been strategic in their choice of targets, attacking Estonian economic and political centers of gravity, including banks, ISP providers, telecommunications hubs, media outlets, and government websites. The cumulative impact of the attacks was the equivalent of a cyber blockade, in which Tallinn's internal and external communications links were degraded. According to Jaak Aaviksoo, the Estonian Minister of Defense, "It is true to say that the aim of these attackers was to destabilize Estonian society, creating anxiety among people that nothing is functioning, the services are not operable, this was clearly psychological terror in a way."[32]

Assuming that the Russian state was involved in the cyberattacks—at least to the extent that it encouraged and may have coordinated the hackers' actions—they indicate that Moscow probably has a relatively low threshold for conducting offensive cyber operations. The unrest in Estonia posed no immediate threat to the Russian State. Rather, Russia's actions in Estonia should be seen in the context of the Federation's long-term objectives of preserving its influence in its near abroad and safeguarding the interests of Russian minority populations along its borders. Nor was Russia deterred by Estonia's membership in NATO. Throughout the campaign, Estonia had grappled with whether to invoke Article V of the NATO charter, but was ultimately deterred from doing so, partly because European Commission and NATO technical experts were unable to find a "smoking gun" that would tie the attacks to the Kremlin, and also because the modalities of invoking the clause to respond to a non-kinetic attack, at least at the time, were undeveloped. The event, however, did begin a debate within NATO about the parameters of the cyber domain and its implications for the alliance.[33]

The Kremlin may have also been emboldened by the ambiguity its cyber proxies afforded it. During the campaign, the Russian government made statements applauding and encouraging the online hackers, but denied any involvement. After action reports suggest that the hackers were likely well resourced, suggesting state sponsorship, but the Kremlin's involvement could not be conclusively proven. The utility of relying on hackers to assault the Estonian government in the information sphere, despite their relatively low capabilities, must have been reinforced by the fact that Russia was widely suspected of being behind the attacks, while it could still

[32] Quoted in Stephen J. Blank, "Information Warfare a la Russe," 241.

[33] At the Bucharest Summit in 2008, NATO created a unified Policy on Cyber Defense. Alliance members also established the Cyber Defense Management Authority (CDMA) to "centralize cyber defense operational capabilities across the Alliance." Shortly afterwards, Tallinn became home to the NATO Cooperative Cyber Defense Centre of Excellence (CCD CoE), the Atlantic Alliance's cyber-security headquarters." Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses" *Journal of Strategic Security* 4, no. 2 (2011): 54-55.

plausibly deny its involvement. Hackers thus proved to be a viable option for coercion, without the risk of attribution.

From a tactical perspective, the cyberattacks appear to have accomplished little. After the attacks subsided, relations between the Estonian government and its Russophone minority continued to be strained. The so-called Bronze Soldier, whose relocation from the center of Tallinn had originally sparked the unrest, remained housed in its new location in the Estonian Military Cemetery on the outskirts of the city. In a more strategic sense, however, the impact of the attacks was significant. They demonstrated the utility of the cyber blockade as a means of coercion, especially when employed in concert with other political, economic, and information tools. They also served as a wake-up call for NATO, which subsequently established the Cooperative Cyber Defense Centre for Excellence (CCDCOE) in Tallinn.

# Georgia (2008): Cyber in Conjunction with Conventional Operations

The second case study we examine is that of the Russo-Georgia conflict in 2008. Tensions between the two countries had mounted during the preceding years over Georgia's foreign policy, which had become increasingly pro-western under President Mikheil Saakashvili, and Georgia's relationship with the separatist republics of South Ossetia and Abkhazia. Georgia's military intervention in South Ossetia on August 7, ostensibly to prevent Ossetian shelling of Georgian territory, prompted Russia to mount a large-scale land, air, and sea invasion of Georgia on the following day (August 8). As Russian military forces moved into South Ossetia, a slew of DDoS attacks took down Georgia's networks, cutting off government communications and defacing government websites. Georgian banks, transportation companies, and private telecommunications providers were also attacked, disrupting services.

On the day the war started, Russian hacktivist websites, such as stopgeorgia.ru, provided lists of Georgian sites to attack, along with instructions, downloadable malware, and after-action assessments.[34] This opened up a new avenue as far as anonymity was concerned. Theoretically anyone, anywhere in the world sympathetic to Russia, or against Georgia, could contribute to the attacks. Under the constant information barrage of botnets, Georgia was subjected to a virtual cyber blockade, most of whose perpetrators were ultimately traced to servers in Russia and Turkey that were affiliated with RBN. Not surprisingly, the Russian government denied involvement, with a Russian embassy spokesman stating that it was possible that individuals in Russia or elsewhere had taken it upon themselves to start the attacks.[35] Once again, the involvement of the Russian government could not be proven conclusively, although the timing of the attacks and the forensic evidence provided a strong indication that the Kremlin was at least facilitating the attacks.

[34] Smith, 9.

[35] John Markoff, "Before the Gunfire, Cyberattacks," *NYT Online* (12 August 2008), accessed at http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

The attacks employed by the hacker groups were relatively unsophisticated—mostly brute force DDoS attacks and SQL injects. However, the degree of coordination involved suggests that they were part of a coordinated campaign plan, the planning and preparation for which preceded Russian conventional operations by several weeks. Subsequent forensic investigations revealed that hackers had been probing and occasionally attacking Georgian government servers since at least July 20.[36] In some instances, the attacks were also aligned geographically with Russian conventional operations. For instance, Russian hackers attacked government websites in the city of Gori in eastern Georgia, along with news websites, just before Russian air attacks on the city.[37]

While the overall impact of the cyberattacks was minimal—Georgia's IT infrastructure was limited in 2008, and the Georgian government was eventually able to reroute most of its traffic through servers in other countries, including the United States, Estonia, and Poland—it was the first known instance of wide-scale offensive cyber operations being mounted in conjunction with conventional military operations.

[36] Ibid.

[37] Joseph Mann, "Expert: Cyberattacks on Georgia Websites Tied to Mob, Russian government," *LA Times*, August 13, 2008, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html, featured in David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal,* 2011.

# Ukraine (2013-present): Cyber Used to Generate Kinetic Effects

While the evidence of Russian involvement in the steady barrage of cyberattacks against Ukrainian targets is not definitive, there are strong indicators that the Kremlin has resourced and directed the attacks. Broadly speaking, Russia appears to have used covert cyber activities in coordination with other information tools and military operations to create a general air of confusion and uncertainty regarding the Ukrainian government's ability to secure its information systems, as well as the integrity of any information being communicated.[38] Through this cyber campaign, Russia has been able to quietly and persistently compromise the Ukrainian government and military's ability to communicate and operate, thereby undermining the legitimacy and authority of Ukrainian political and military institutions. In late December, 2015, however, Russia appeared to signal its capability and a willingness to expand its use of offensive cyber operations to achieve kinetic effects by damaging Ukrainian critical infrastructure.

Russian hackers have utilized spear phishing, malware, DDoS attacks, telephone denial of service (TDoS) attacks, and other forms of cyber disruption and espionage to conduct a steady drumbeat of cyberattacks targeting Ukraine's government, military, telecommunications, and private-sector information technology infrastructure. Cyberattacks have been used to interrupt communications, obtain and leak government documents and plans, and deface or take down public and private websites and computer systems. Hackers also sent SMS messages to Ukrainian military personnel encouraging them to defect.[39] These nuisance cyberattacks have coincided with key events of the conflict, such as the Maidan protests, Ukrainian parliamentary elections, and the movement of Russian forces into the Crimea.[40]

[38] Azhar Unwala and Shaheen Gori, "Brandishing the Cybered Bear."

[39] Interview, Moscow, April 2016.

[40] Russia is believed to have conducted low-level information warfare against Ukraine since at least 2009 as part of a broader campaign against NATO and EU countries. "Russian Cyber Espionage Campaign – Sandworm Team," iSight Partners (2014) via Azhar Unwala and Shaheen

In late December 2015, however, pro-Russian cyber actors departed from what were basically nuisance attacks and perpetrated what is believed to be the first cyberattack on another country's electric power grid. In an attack that has been widely attributed to Russia,[41] coordinated and synchronized cyberattacks targeted a three separate distribution centers of a Ukrainian power company in Western Ukraine. Using remote access to control and operate breakers, the attackers took the distribution centers offline causing power outages that affected more than 220,000 Ukrainian residents.[42] The cyber actors then wiped some systems by executing KillDisk malware at the conclusion of the cyberattack.[43]

In reconstructions of the attacks provided by private cyber security firms, the attack has been described as particularly sophisticated: the attackers had spent months conducting reconnaissance in the power company's networks, had obtained system administrator credentials, and then coordinated and synchronized the operation to take down the distribution centers simultaneously.[44] Another indicator of the attack's sophistication is that, while the impact was widespread, the overall effect was limited. Cyber experts speculate that the hackers had the ability to have caused more damage, such as causing physical damage to the breakers to permanently take the power stations offline, but chose not to.[45] Instead, the power was only out for 1-6 hours for the regions hit (but the distribution centers were not fully operational many months after the attack). This restraint may have been meant to signal Russia's capability to attack Ukraine's physical infrastructure, but without doing irreparable damage.

The attackers may have also employed BlackEnergy, a highly advanced cyber surveillance tool, to infiltrate and map the power center networks prior to the

Gori, "Brandishing the Cybered Bear: Information War and the Russian-Ukraine Conflict," Military Cyber Affairs: Volume 1, Issue 1, Article 7 (2015).

[41] Pavel Potilyuk, "Ukraine Sees Russian Hand in Cyber Attacks Against Power Grid." *Reuters (online)*, February 16 2016. Accesed at http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.

[42] Department of Homeland Security, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[43] Ibid.

[44] "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare," Lookingglass Cyber Threat Intelligence Group, CTIG-20150428-01, April 28, 2015; "Analysis of the Cyber Attack on the Ukrainian Power Grid," Electricity Information Sharing and Analysis Center, March 18, 2016.

[45] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired (online), March 3, 2016. Accessed at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

attacks.[46] According to one source, the latest version of BlackEnergy includes a backdoored secure shell (SSH) utility that gives attackers permanent access to infected computers.[47] More recently, Russian hackers have used a highly advanced form of cyber malware—dubbed Ouroboros (a two headed mythological snake)—to map and open backdoors into Ukrainian and other European government systems. According to one report, "Ouroboros has been in development for nearly a decade and is too sophisticated to have been programmed by an individual or a non-state organisation."[48] The relative sophistication of these attacks suggest that they were directed and controlled by a state or military entity, such as the GRU (Russia's military intelligence agency) or FSB, rather than a co-opted hacker group.

Relations had been strained between Russia and Ukraine ever since Russia annexed Crimea in 2014 and the local Crimean government began nationalizing Ukrainian-owned energy companies, angering the companies' Ukrainian owners. Just before the attack on the Ukrainian substations had occurred, pro-Ukrainian activists physically attacked substations feeding power to Crimea, leaving two million Crimean residents without power. Some have speculated that the subsequent blackouts in Ukraine were retaliation for the physical attacks on the Crimean substations. However, the hackers who infiltrated the Ukrainian power grid had begun to reconnoiter their targets at least six months before they took the grid down. So, while the timing of the cyberattack on the Ukrainian grid suggests that its immediate catalyst may have been the physical attacks on the Crimean substations, the original motivation for the operation is less clear.

It is also possible that the attack on the Ukrainian power grid was done to send a message or a warning. Around the time of the attack, the Ukrainian parliament had been considering a bill to nationalize privately owned power companies in Ukraine, some of which were partially owned by powerful Russian oligarchs.[49] Either way, the attack would seem to fall under the rubric of classic Russian information warfare

[46] Dan Goodin, "First Known Hacker-Caused Power Outage Signals Troubling Escalation," *Ars Technica*, 4 January 2016. Accessed at http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

[47] Ibid.

[48] According to the same report, "The origins of Ouroboros remain unclear, but its programmers appear to have developed it in a GMT+4 timezone – which encompasses Moscow – according to clues left in the code, parts of which also contain fragments of Russian text. It is believed to be an upgrade of the Agent.BTZ attack that penetrated US military systems in 2008." See Sam Jones, "Cyber Snake Plagues Ukraine Networks," Financial Times, 7 March 2014. Accessed at https://www.ft.com/content/615c29ba-a614-11e3-8a2a-00144feab7de.

[49] See Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired* (online), March 3, 2016. Available via https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

principles, in that its impact was mainly psychological. It emphasized the ramifications of Kiev's anti-Russian policies while undermining the confidence of Ukraine's citizens in their government. The attack would also seem to indicate Russia's willingness to expand the scope of its cyber operations into the kinetic-effect realm, although it is probably too early to say whether this will be the beginning of a trend or merely an aberration.

# Bots, Leaks, and Trolls: Cyber's Role in Enabling Russian Propaganda

In addition to the instances we have cited of Russia employing its cyber capabilities to deter, compel, or disorient its adversaries, the Kremlin also uses cyber to disseminate pro-Russian propaganda and undermine popular support for the governments or institutions of its perceived rivals. Its efforts in this regard fall into two general categories:

1. Using cyber espionage to obtain adverse information about political adversaries and then leaking that information publically.

2. Using internet "trolls" (i.e., paid individuals) to create fake blogs and online profiles to swamp news comment sections with misleading, false, or pro-Russian points of view.

As with the other components of information operations, Russian cyber operations are usually designed to be deniable. Cut-outs, front organizations, and false flag operations feature prominently. Hacker groups in particular provide Russia with a covert, non-attributable option for acquiring data and documents that can be used in disinformation campaigns and information operations. They conduct a range of cyber activities, from DDoS attacks and cyber espionage to data/document exfiltration and digital sabotage. Adverse information intended to discredit foreign political leaders or government institutions is sometimes released to third party news outlets, such as Wikileaks. These entities, either wittingly or unwittingly, provide an additional layer of anonymity, camouflaging the source of the information and concealing the motivations for its release.

For example, the hacker groups described as APT 28 (also known as Fancy Bear and Sofacy) and APT 29 (also known as Cozy Bear) are believed to be the groups behind the 2016 leaks of documents from the Democratic National Committee (DNC) servers.[50] These groups are believed to be affiliated with Russia's military intelligence

[50] Jeff Stone, "Meet Fancy Bear and Cozy Bear, Russian Groups Blamed for the DNC Hack." CSM Monitor, June 15, 2016. Available at http://www.csmonitor.com/World/Passcode/2016/0615/Meet-Fancy-Bear-and-Cozy-Bear-Russian-groups-blamed-for-DNC-hack.

agency (GRU).[51] In the past, APT 28 has targeted Ministries of Defense all over Europe and is believed to be the group that targeted the Georgian military during the 2008 Russo-Georgian war. APT 29 has been caught accessing the U.S. White House, State Department, and Joint Chiefs of Staff unclassified websites.[52] In the DNC hack, the two groups appeared to be operating independently. Crowdstrike, which investigated the hack, determined that APT 29 had actually been active in the DNC's servers for almost a year before the breach was detected. During this time, Crowdstrike believes that the APT 29 was able to monitor the DNC's communications and email and chat traffic. It was APT 28 that went directly for the DNC's research on Donald Trump.[53]

The DNC hack has widely been interpreted as a Russian plot to meddle in the 2016 U.S. presidential elections. According to a publically-released intelligence community assessment (ICA), "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."[54]

The DNC hacks are not unprecedented. During the Cold War, the Soviet Union relied on intelligence agents and friendly media outlets to disseminate adverse information or disinformation in order to disparage candidates perceived as hostile to the Kremlin. Nor do the DNC hacks represent the first time Russia has used covert cyber operations to meddle in an election. The hacker group CyberBerkut, which carries out pro-Russian hacking activities in Ukraine, is believed to be the group behind a 2014 attack on Ukraine's election infrastructure. The DNC hack would appear to be part of a pattern of Russia targeting democratic elections, in some cases to favor one candidate over the other, but also as a means of undermining democratic institutions and the concept of a free electoral process as a whole. If they differ from previous instances of election meddling, it is primarily in scope, rather than nature.

Internet trolls are a more overt, but still non-attributable tool for discrediting anti-Russian information on the internet and pushing pro-government points of view. In 2012, WikiLeaks published data and documents supplied by the hacker group, Anonymous, which provided evidence that the Russian government, with Putin's

[51] Ibid. Also see Director of National Intelligence (DNI), "ICA: Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, 6 January 2017.

[52] Jeff Stone, "Meet Fancy Bear and Cozy Bear, Russian Groups Blamed for the DNC Hack." CSM Monitor, June 15, 2016. Available at http://www.csmonitor.com/World/Passcode/2016/0615/Meet-Fancy-Bear-and-Cozy-Bear-Russian-groups-blamed-for-DNC-hack.

[53] Ibid.

[54] DNI, "Assessing Russian Activities," op cit.

approval, was directly paying for a team of professional trolls.[55] This practice has its roots in Russian domestic policy. During the early and mid-2000s, the internet provided a platform for Russian political opposition to get its message out. The government, which had an interest in restricting mediums for oppositional speech, attempted to control the opposition's access and use of the internet. However, it quickly became clear that such efforts would not be successful. The Kremlin appeared to calculate that, if it could not control what political opponents put on the internet, then the government would try to crowd out, or overpower, the opposition's message with a pro-Kremlin messaging campaign.

"Troll farms," which often employ hundreds of people, were formed to spread pro-Kremlin messaging on the internet. To augment their activities, the government has leveraged pro-Kremlin youth groups, such as *Nashi* and Young Guard of United Russia. During the 2011 Russian Parliamentary elections, evidence of widespread electoral fraud led to a boom in anti-government and anti-Putin protests. These protests were organized over the internet via Facebook and Twitter and reportedly solidified in the minds of the Kremlin that the internet posed a direct threat to government stability.[56] Russia's use of trolls to influence domestic politics and policy intensified following the election experience in 2011; more recently, the use of trolls to crowd out anti-Russian information has been used on the international stage, particularly in Ukraine and Crimea, but in Europe and the United States as well. Trolls are reportedly paid to comment on anti-Russian news articles, "dislike" anti-regime videos on YouTube, use false online profiles on social media sites such as Facebook to overwhelm the comments of anti-Russian posts, and create and maintain pro-Russian blogs.[57] An individual troll often maintains multiple online profiles and blogs.

The information contained in the comments and posts by the trolls ranges from misleading to verifiably fraudulent. Western observers and Russian anti-government activists have noted, however, that the role of the Russian internet troll is not necessarily to persuade its audience to a pro-Russian perspective but rather "to

[55] "Vladimir Putin's Army of Blog Trolls." *Observer*, February 8, 2012. Available at http://observer.com/2012/02/vladimir-putins-army-of-blog-trolls/.

[56] Adrian Chen, "The Agency." *The New York Times*, June 2, 2015. Available at http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

[57] "Vladimir Putin's Army of Blog Trolls." *Observer*, February 8, 2012. Available at http://observer.com/2012/02/vladimir-putins-army-of-blog-trolls/.

overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[58]

[58] Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks." *The New Yorker*, July 27, 2016. Available at http://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks.

# Conclusion

Recent cyber operations—such as the DNC hack and the attack on the Ukrainian power grid—illustrate that Russia's cyber capabilities and tactics continue to evolve and adapt. Estonia, Georgia, and Ukraine have served as testing grounds and signaling arenas for Russia's cyber forces, providing opportunities for them to refine their cyberwarfare techniques and procedures while demonstrating their capabilities on the world stage to influence or deter Russia's adversaries. The simple DDoS attacks and DNS hijackings that typified Russian cyber operations in Estonia and Georgia have since been overshadowed by more sophisticated tactics and malware tools, such as BlackEnergy and Ouroboros.

If the example of Ouroboros is any indication, state-based actors, such as the GRU and FSB, also appear to be playing a more direct role in Russian offensive cyber operations than they did in the past. Non-state hackers, criminal syndicates, and other advanced persistent threats will probably remain a constant feature of Russian offensive cyber operations, both for the anonymity they afford and the ease with which they can be mobilized. However, as governments and companies around the world have hardened their networks, the basic techniques used by hacktivists and other non-state actors—for instance, redirecting traffic—are no longer as useful as they were five or ten years ago. The crowd-sourced approach that has typified how the Kremlin has utilized hackers and criminal networks in the past is likely to be replaced by more tailored approaches, with the FSB and other state agencies conducting network reconnaissance in advance and developing malware to attack specific system vulnerabilities.

The network reconnaissance and prepositioning conducted ahead of the outbreak of conflict in the Georgia and Ukraine cases are indicative in this regard. The cyberattacks perpetrated against those countries were facilitated by spear-phishing campaigns that introduced malware or granted cyber actors remote access to systems sometimes months in advance of the military or diplomatic action, prior to any significant uptick in tensions with Moscow. The network reconnaissance and pre-staging of cyber forces in these cases suggests a degree of advanced planning and target selection that is more aligned with a broader IO campaign plan than the reactive, crowd-sourced approaches employed by hacking groups.

Offensive cyber operations are also likely to figure more prominently in Russian conventional military operations than they did in the past. Although the Russian

military has been slow to embrace cyber for both structural and doctrinal reasons, the Kremlin has signaled that it intends to bolster the offensive as well as the defensive cyber capabilities of its armed forces by establishing special military cyber units and a cyber coordination and deconfliction body, sometimes referred to as a Cyber Defense Center in press—subordinate to the General Staff.[59] The conflict in Georgia provided the first practical example where conventional Russian military operations may have been synchronized with cyber operations.

Cyber may also play a greater role in Russia's future strategic deterrence framework. According to James Clapper, the Director of National Intelligence, Russian hackers have penetrated U.S. industrial control networks that are responsible for operating critical infrastructure.[60] The objective of the hackers appears to have been to develop the capability to remotely access and disrupt the control systems in the event of hostilities. Thus, it is possible that the Kremlin is adopting a hold-at-risk approach against U.S. and allied critical civilian infrastructure in order to influence perceived adversaries and deter unwelcome behavior.

While Russian cyber tactics appear to be evolving, the theoretical and doctrinal underpinnings of Russia's approach to cyber warfare have remained more or less constant. Russian officials are convinced that Moscow is locked in an ongoing, existential struggle with internal and external forces that are seeking to challenge its security in the information realm. Globalization, along with the free flow of information it engenders, is viewed as both a threat and an opportunity in this regard. Russian information warfare doctrine—which encompasses cyber along with other, more traditional tools for shaping the information space—blurs the separation between peacetime and wartime. Cyber operations that in a U.S. context might require Title 10 authorizations and authorities are more likely to be employed by the Russians in a pre-conflict scenario or even peacetime when their capacity to affect a strategic outcome is viewed as more advantageous. This suggests that the Kremlin

[59] Eugene Gerden, "$500 Million for New Russian Cyber Army," *SC Magazine,* November 6, 2014. Accessed at http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/.

[60] According to Clapper's testimony, "Computer security studies assert that Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software ("malware") designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates, according to private sector cyber security experts." See James R. Clapper, "Statement for the Record: Worldwide Cyber Threats," House Permanent Select Committee on Intelligence. September 10, 2015. Accessed at https://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1251-dni-clapper-statement-for-the-record,-worldwide-cyber-threats-before-the-house-permanent-select-committee-on-intelligence

has a relatively low bar for employing cyber in ways that U.S. decision makers are likely to view as threatening and escalatory in nature.

This page intentionally left blank.

CNA
ANALYSIS & SOLUTIONS

DOP-2016-U-014231-1Rev-2




CNA is a not-for-profit research organization
That serves the public interest by providing
in-depth analysis and result-oriented solutions
to help government leaders choose
the best course of action
in setting policy and managing operations.

*Nobody gets closer—*
*to the people, to the data, to the problem.*

CNA
ANALYSIS & SOLUTIONS

www.cna.org • 703-824-2000

3003 Washington Boulevard, Arlington, VA 22201