978-9934-564-90-1

RUSSIA'S STRATEGY IN CYBERSPACE

Published by the
NATO Strategic Communications
Centre of Excellence

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

ISBN: 978-9934-564-90-1
Authors: Janne Hakala, Jazlyn Melnychuk
Project manager: Sanda Svetoka
Design: Kārlis Ulmanis

Riga, June 2021
NATO STRATCOM COE
11b Kalnciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

Aknowledgments

This publication is developed in the framework of the joint cooperation project of the NATO StratCom COE and NATO Cooperative Cyber Defence COE.
We would also like to thank Dr Juha Kukkola, Dr Ieva Bērziņa, Varis Teivāns and Mark Laity for advice and review of the publication.

Contents

INTRODUCTION

Headlines connecting Russia to the vague notion of 'cyber' have become daily bread for Western publics and decision makers alike. From the damage done by NotPetya or attacks against Ukraine and Georgia, to Russia's hacking and leaking operations in US and European elections, Russia's offensive operations are consistent threat. An increasingly important tool in what Russia views as the ongoing "information confrontation," Russia utilizes cyber operations alongside other military and non-military means to pursue strategic objectives.

On the other hand, recent years have seen Russia's attempts to close and secure its own digital information space. By using a combination of legal and technical means, the Kremlin tries to impose control both over digital infrastructure and content, efforts which are aimed at ensuring independence from the global Internet network and thus enhancing their information security.

Russia sees activities in cyberspace as a subset to the all-encompassing framework of 'information confrontation,' which is derived from the Russian understanding of relations between states and, more specifically, a subset of the struggle between great powers for influence in the world. According to Russian thinkers, the information confrontation is constant and ongoing, and any means can be used to gain superiority in this confrontation. Activities in cyberspace are one of several tools of warfare in the information environment, including psychological operations, electronic warfare (EW), and kinetic action. In practice, cyberspace can be used both for physical attacks on infrastructure, and cognitive attacks such as disinformation. However, the center of gravity in the 'information confrontation' lies in peoples' minds and perception of events, both domestically and internationally.

This report seeks to clarify the role of cyberspace in Russian strategic thinking. It will analyse cyber operations as a subset of Russia's 'information confrontation' and explore how this philosophy is put into practice. The report will examine both offensive measures, such as participation in the information war, and defensive measures, such as Russia's efforts to secure its own information space from foreign influence. Finally, it will conclude with several policy recommendations for NATO strategic communications in addressing Russia's offensive activities in cyberspace.

RUSSIA'S "INFORMATION CONFRONTATION"

Russian Conceptions of 'Cyber'

Russia's conceptualization of 'information confrontation' and the role of cyberspace within it is outlined in strategic policy documents, such as National Security Strategy (2015), Foreign Policy Concept (2016), Information Security Doctrine (2016), Military doctrine (2014), Conceptual Views on the Activity of the Armed Forces in the Information Space (2016), as well as works and publications by Russian military thinkers.

From the Russian perspective, cyber warfare or the Russian equivalent 'information-technological warfare,'[1] is only a part of the overarching concept of **"information confrontation"** (*informatsionnoe protivoborstvo*). The Russian Ministry of Defence describes the information confrontation as the clash of national interests and ideas, where superiority is sought by targeting the adversary's information infrastructure while protecting its own objects from similar influence.[2] The translation of the term *informatsionnoe protivoborstvo* into English has proven difficult, and has often incorrectly been translated as 'information warfare'[3] *('informacionnaja vojna')*, despite the fact that *protivoborstvo* refers to 'counter-struggle', 'countermeasure' or 'counteraction' rather than 'warfare'.[4] This paper uses the term 'information confrontation' due to its established status in discussions regarding hostile Russian informational activities.

The confrontation includes a significant psychological remit, whereby an actor attempts to affect informational resources (documents in information systems) as well as the minds of the adversary's military personnel and population at large.[5] Ultimately, cyber operations (or information-technical means) are one of many methods used to gain superiority in the information confrontation. Russia, and particularly Russian President Putin's regime, sees the information confrontation as a constant geopolitical zero-sum competition between great powers, political and economic systems, and civilizations.[6]

Protecting 'Information': Cognitive and Technical

Publicly available Russian doctrines and policy documents do not explicitly reference cyber operations. Furthermore, Russian documents do not use the term 'cybersecurity', but refer instead to '**information security.**' This term differs from

> Russia perceives the information space in very geopolitical terms, with their domestic information space representing a continuation of territorial state borders, which they view as constantly being violated by foreign intrusions.[13]

the Western notion of 'information security' (or in short: infosec) in that it encompasses not only the protection of critical digital networks, but society's cognitive integrity as well.[7] There are several reasons why Russian military thinkers apply the term 'cyber' when talking about Western threats and activities, but are reluctant to link the term to Russia's own capabilities and actions. Some authors argue that this deliberate choice is related to negative connotations around Soviet-era 'cybernetics,' as well as the importance the term 'information security' holds for Russia's own domestic politics[8].

When discussing the operational environment, Russia uses the term '**information space**' (*informatsionnoe prostranstvo*), or '**information sphere'** (*informatsionnaya sfera*), which again is more comprehensive than the Western concept of 'cyberspace' or 'cyber domain.' The 2016 Russian Doctrine of Information Security defines the **information sphere** as:

"a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet […], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere".[9]

The **information space** refers to activities to form, transform, and store information, as well as '*influencing individual and public consciousness, information infrastructure and information itself.*'[10]

According to Ofer Fridman, Russia conceptualizes cyberspace as the intersection between hardware, software, infrastructure, and content[11]. In this framework, the **information-technological** layer includes hardware, software and infrastructure, while the **information-psychological** layer includes hardware, software and content.' Irrespective of the means used – technological (for example, destroying digital infrastructure)

or psychological (manipulating a message on social media) – activities in cyberspace are understood in terms of their effect in the information space.[12] Importantly, Russia perceives the information space in very geopolitical terms, with their domestic information space representing a **continuation of territorial state borders,** which they view as constantly being violated by foreign intrusions.[13]

NATO doctrine understands cyberspace as an operational domain and considers it as part of the **information environment**. This environment is *'[…] comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information'*. The information processed through this environment provides the base for cognitive processes that affect individual decision-making and subsequently, behaviour. Those processes happen in three dimensions – physical, virtual and cognitive – and cyberspace involves all three of them. In this respect, NATO's concept of the information environment is not that different from Russia's understanding of 'information space' and the role of cyberspace within it.

Similarly, the Russian concept of '**information weapons**' (practically absent in Western parlance) includes more than just digital measures.[14] Although the Russian Armed Forces vaguely defines them as "*information technologies, means and methods used for the purposes of waging information war,*" in practice the concept covers a wide array of activities (often with an emphasis on affecting the human mind); this includes the spreading of disinformation, electronic warfare, the degradation of navigation support, psychological pressure, and the destruction of adversary computer capabilities.[15]

Contrary to the Western view of interstate conflict that is based on the international legal order outlined in international treaty and customary law (specifically the UN Charter and the Geneva Conventions) that makes a clear distinction between war and peace, Russia's 'information confrontation' is constant and ongoing. This view is exploited by Russia to undertake activities beneath the threshold of armed conflict, allowing it to remain unpredictable and pursue strategic objectives short of causing kinetic conflict.[16] A key goal of Western democracies is to maintain a free, stable and open Internet, where fundamental rights and freedoms are ensured. In this regard, 'information security' is perceived as the protection of data and systems, but not imposing control over the attitudes and beliefs that the users of those systems are expressing. At the same time, the principles of openness and freedom of speech upheld in Western democracies might be exploited by information and cyberattacks. Russia seeks to exploit this openness to gain '**information superiority,**' notwithstanding whether it is in a conventional conflict with its opponents or not.

NATIONAL SECURITY INTERESTS AND STRATEGIC OBJECTIVES

Events that sparked capability development

Russian thinking and capabilities regarding information confrontation have been developed by learning from mistakes both at home and abroad. In the 1980s, the Soviet Union began to draw attention to a so called 'Revolution in Military Affairs' that affected warfare via informatization. Calls for revolution were however disregarded,[17] which is why the Soviets were utterly shocked by the coalition's success in the 1991 **Gulf War**.[18] Consequently the importance of information technologies was eventually internalized.[19]

In the **Second Chechen War** of 1999, the Russians managed to dominate the traditional media environment, but were unable to overcome the global perception of a heroic Chechen independence struggle due to the rebels' use of the Internet. Russian security services thus sought to harness the Internet to impact audiences. Disinformation campaigns were conducted domestically in a coordinated fashion, while Chechen information campaigning was targeted through cyber means.[20]

In the **Russo - Georgian War** of 2008, the Georgians gained the upper hand in the information space by drowning out Russian news coverage abroad by reporting on Russian air raids on civilian targets.[21] Eventually this led to discussions on the creation of 'Information Troops' within the military to engage in a direct dialogue with the target audiences.[22]

A few years later, the 2011-2013 **Moscow protests** about unfair elections and the Putin-Medvedev role swap demonstrated how social media could be used to generate public unrest. Already the Arab uprisings had demonstrated the effectiveness of social media in regime change, which contributed significantly to the Kremlin's anxiousness of the same being repeated in Russia. Russian officials understood that automatically-generated social media content was not enough to affect the conversation, which led to substantial investments in human capabilities to impact online debates by recruiting people with knowledge of foreign languages. This capability is exemplified in the Internet Research Agency, a state-affiliated troll farm dedicated to influencing audiences at home and abroad. These events helped Russia develop the information campaign capabilities that facilitated the annexation of Crimea in 2014.[23]

Russia's Threat Perception

As a vast country with significant natural resources but few natural borders, Russia has repeatedly had to mobilize its society to counter foreign aggressions. This has contributed to a profound sense of insecurity whereby the security of Russia can best be guaranteed by exerting control beyond its borders, in its perceived "sphere of influence."[24] Russia has thus tended to define its security in a zero-sum way that embodies the classic security dilemma, whereby they are secure when their adversaries feel insecure. After the fall of the Soviet Union, many Westerners believed relations with Russia would restart. However, Russian skepticism of the West festered in the 1990s, due largely to the serious economic shock felt in the ill-handled transition to a market economy, and the lack of a new unifying national identity after the break-up of Soviet Union.

This mistrust of the West is further exemplified in Russia's view that NATO's enlargement to former Soviet states represents aggression towards its claimed "sphere of influence." Russia also accuses the West of foreign interference, for allegedly inciting Color Revolutions.[25] Former KGB officer Igor Panarin has argued that the West's use of informational tools during the 20th century led the Russians to destroy their own country, first with the fall of the Russian tsars in 1917, and later with the collapse of the Soviet Union in 1991.[26] Additionally, the 2011 Arab Spring revolutions sweeping the Middle-East and North Africa fit into the Russian narrative of consistent Western attempts at ousting hostile regimes, primarily through informational tools.[27] This threat perception has been highlighted in the 2016 Information Security Doctrine, which states that:

> *"Intelligence services of certain States are increasingly using information and psychological tools with a view of destabilizing the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other States. Religious, ethnic, human rights organizations and other organizations, as well as separate groups of people, are involved in these activities and information technologies are extensively used towards this end".28*

The Kremlin's ongoing offensive stance assumes that there is a systemic, continuous struggle between great powers, and therefore it must defend itself from consistent influence operations by the West. This approach was outlined in the 2000 National Security Concept, which states that to prevent wars and armed conflicts, Russia should give preference to non-military means and to engage in "*counteraction against the threat of rivalry in the information sphere*".[29] What is important in their perception is that Russia's own actions are perceived as defensive, the aim being to prevent potential conflicts and retaliation, and to control their escalation by staying below the West's threshold for armed conflict.[30]

Information tools may work in tandem, as Russian military thinkers posit that by targeting not only the leadership and military, but the entire mass consciousness of the population, strategic effects may be achieved.[35]

Strategic Deterrence

The importance of information technology in the information confrontation is derived from Russia's '**strategic deterrence**' concept. It is based on the understanding that nuclear weapons do not sufficiently deter the whole spectrum of modern security threats,[31] which is why strategic deterrence includes not only nuclear and conventional military power, but also an array of non-military tools, such as ideological, political, diplomatic, economic, and – centrally – informational and digital measures.[32] It is therefore important to understand that, in spite of its name, strategic deterrence is not only about deterrence in the Western understanding of the term, but rather a comprehensive approach to achieving strategic goals.[33] Russia has recognized that aspiring for military parity with the US is costly and must be avoided given the fate of the Soviet Union and the economic stagnation of modern-day Russia.[34]

Therefore, the Kremlin is eager to exploit the vulnerabilities of strategic challengers even in peacetime. More recent efforts such as the annexation of Crimea, or interference in the 2016 US election, have reaffirmed for Russia the effectiveness of information weapons to achieve strategic objectives without triggering red lines of military confrontation. This may be a key reason why cyber-attacks aimed at physically impacting infrastructure are wielded more sparingly, as they may trigger a more dramatic response, making escalation harder to control.

The overall goal of the information confrontation is to achieve **strategic effects and gain superiority over opponents**, whether it is done by military or non-military means. To this end, cyber operations can play an essential role in compensating for conventional force, as disabling critical civil infrastructure such as energy, transport, and C2 (Command and Control) capabilities can dramatically weaken an adversary's war-fighting capabilities. Information tools may work in tandem, as Russian military thinkers posit that by targeting not only the leadership and military, but the entire mass consciousness of the population, strategic effects may be achieved.[35] This Russian strategic thinking operationalises the protection of their own information space though an extensive web of code, legal controls, and surveillance measures which will be explored in the following section.

Principles of Russia's 'information confrontation' playbook

The Russian perception of information as a means to galvanize its domestic population and to win over global public opinion by misdirection has its roots in Soviet practices.[36] Current tactics resemble concepts from Soviet-era theories and such as 'reflexive control', 'active measures' and 'maskirovka'. However, in many ways Russia's approach to 'information confrontation' is unique to today, as Russia is constantly adapting to new circumstances and technology.

'**Active measures**' (*aktivnyye meropriyatiya*) refers to operations aiming at affecting other nations' policies. This however should not to be mistaken with public diplomacy, in which practically all states continuously engage. The difference between the two is that whereas the aims and sources of public diplomacy activities are open, active measures tend to be undertaken secretly, violate laws and involve blackmail, bribes, disinformation, and the exploitation of a target nation's individuals and political influence.[37]

The theory of **reflexive control** seeks to lead the target to unknowingly act in a predefined manner, often against their own interest.[38] This could be done by influencing the adversary's channels of information and sending them messages which shift the flow of information in Russia's favor. The adversary, acting on a manipulated information space, makes a decision that has at its core been incited by Moscow.[39] A country's susceptibility to reflexive control largely emanates from unchecked access to its information space by all actors, where false or misleading information is often not attributable and control measures are limited. Democratic information spaces are especially vulnerable to such efforts.

Another method of information confrontation inherited from the Soviet-era is known as **maskirovka,** which includes concealment and deception. Used primarily as a military term, the aim of *maskirovka* is to convince the adversary of the presence of objectives or units in places where they are not. The idea behind such actions is to lead the target into error, force them to take measures not corresponding to reality, and to disrupt their C2 and undermine their troops' morale.[40] Traditionally, it was the GRU (the Main Intelligence Directorate) that was responsible for *maskirovka*, but military operations in Ukraine indicate that various state and non-state actors have been involved in such actions, including the FSB (the Federal Security Service) and the Night Wolves. Moreover, *maskirovka* is not solely limited to military targets anymore, but also includes the civilian population.[41]

SECURING THE INFORMATION SPACE - 'DIGITAL SOVEREIGNTY'

In October 2019, 'Russia's sovereign internet' law came into force, effectively allowing the government to disconnect from the global Internet at their discretion. To this end, the Kremlin aims to have only 10% of Russian Internet traffic routed through foreign servers by 2024.[42] The Kremlin views control over its domestic information space as essential to their security – a threat to the information space might be perceived as a threat to state sovereignty. This section will explore the implementation of 'digital sovereignty' concept through exploring the measures that are taken to secure Russia's domestic information space.

Digital sovereignty (*tsifrovoi suverenitet*) is in this context used primarily as a political term, and can be understood as the right and capability of a government to determine its fate within its own information space.[43] Russian information technology expert, Igor Ashmanov, divides digital sovereignty in two: **electronic sovereignty**, which encompasses robust Internet infrastructure protected from malware and malicious cyber actors; and **information sovereignty**, the self-sufficient control of information and resistance to information attacks. Thus, the ideal state of affairs would consist of autonomous hard- and software, Internet infrastructure, subordinated mass media, a unifying ideology, and a strong legal system.[44] An essential component of digital sovereignty is the **Russian Internet** (RuNet) – a Russian language-based, relatively closed segment of the Internet consisting of popular research engines and social media sites such as Yandex, Vkontakte and Odnoklassniki. Although seemingly harmless, this system has enabled Russia to reach out to and influence Russian-speaking minorities in neighbouring countries, extending Russia's sphere of influence in the digital environment.[45] In recent years, RuNet has begun to transform from an alternative online environment into a space where the Kremlin actively suppresses undesired information – an aspiration which is outlined in the 2016 Information Security Doctrine.[46] Interestingly, Russia's growing interest in detaching the Russian Internet may negate some benefits of RuNet, as it will limit their ability to impose control outside their borders through these platforms.

Russian defence and security elites acknowledged the significance of the Internet as a security threat after 2012, when political opposition used it extensively to mobilize, first against the fraudulent Duma election and then against Putin's re-election.[47] Several steps were taken to implement the concept of 'digital

sovereignty,' namely to create Russia's own national Internet segment that would make it self-sufficient and independent from developments outside its borders, thus ensuring protection from both internal and external threats.

A closed network would provide Russia with considerable advantages in different phases of information confrontation. Russia would gain in terms of its societal resilience and recovery, integrity of command, and overall performance in times of mobilization. The system would also create a deterrence-by-denial effect that would discourage the adversary from taking hostile actions due to their expected futility.[48] Conflict in the information space between Russia and her adversaries would thus gain a very asymmetric character, as the states operating within open networks would face a considerably constrained operating environment, whereas Russia, as a closed-network nation, would be able to operate with comparative freedom.[49]

Juha Kukkola outlines several sets of measures (or sub-systems) that help Russia 'nationalize' their domestic information infrastructure, such as:[50]

1. **Scientific – industrial bases**: the development of Russian-produced hardware and software, and provision to security services and military.

2. **State authentication and encryption:** efforts to make data traffic within Russia accessible to security services and military, and to protect data from foreign exploitation.

3. **Blacklisting and content management**: the removal and restriction of websites.

4. **Targeted surveillance systems and massive data traffic localisation and retention:** carried out by Internet Service Providers (ISP), as ordered by the state. It is highly centralised and the objectives are counterintelligence, law enforcement and political control.

5. **Efforts to protect Critical Information Infrastructure (CII) through extensive legal regime:** based on state ownership or control of CII and legal obligations on private actors to protect it. This includes backups of top-level domain name servers (DNS), routing registers, and Internet Exchange Points (IXP). It allows for the functioning of the national segment and its disconnection from the global network.

6. **Information-technological and information-psychological countermeasures:** managed by state-controlled or affiliated news services, and educational, patriotic and religious institutions, as well

> Several steps were taken to implement the concept of 'digital sovereignty,' namely to create Russia's own national Internet segment that would make it self-sufficient and independent from developments outside its borders, thus ensuring protection from both internal and external threats.

as through the cyber capability of security services and the military. It controls the domestic information environment and conducts external overt and covert espionage, and influence and cyber operations abroad to prevent possible threats from emerging.

7. **Feedback, monitoring, control and management:** a subsystem which provides real-time analysis and reactions to all information threats.

Domestic information security is supported by systems such as SORM and GosSOPKA, as well as a system for the centralized management of the public telecommunications network (currently under development).

SORM (System of Operative-Search Measures) is a Soviet-era surveillance technology which the government began adapting to the emerging digital domain in 1998.[51] The SORM enables the tracking of telephone and internet traffic, not only at a metadata level, but also contents and data traffic. Internet and other telecommunication service providers are obligated to install probes in their networks connecting them to the Federal Security Service (FSB). The most recent generation of the system (SORM-3) includes deep packet inspection capabilities.[52] Other Russian security services can request access to SORM. While there is no direct evidence of the use of SORM abroad except for some former Soviet countries, it naturally affects foreign nationals travelling to Russia.

System for the centralized management of the public telecommunications network is currently under development and will be controlled from the Centre of Monitoring and Managing of the Public Communication Networks (TsMUSSOP) by the Radio Frequency Service. It foresees that Internet Service Providers (ISPs) are required to install certain equipment into their networks which can monitor and filter traffic, and if needed completely block it. This would, in theory, disconnect the Russian segment of Internet from the global network.[53]

Laws regulating information space and CII

These technical measures are accompanied by a heavy-handed **legal regime**. This regime is two-fold, combining both laws that nationalize the protection of critical information infrastructure, and those which are directed at controlling content and data flow in the Internet.

To assert complete control over the information space, the Russian government has passed a network of laws that effectively nationalize the protection of CII. These regulations grew out of previous regulations on emergencies governing energy and transportation.[54]

A 2012 policy[55] firmly defined CII and introduced the national cyber security system **GosSOPKA** (Government System for Detecting, Preventing and Eliminating Effects of Computer Attacks). GosSOPKA is designed to "shield" all government information resources under the hood of a single system with a constantly monitored perimeter. This shield would extend to all resources and critical infrastructure, so they all share information about cyberattacks with a central office, which would determine how an attack was mounted and distribute security recommendations to the rest of the system.[56]

In 2017, the Law on the Critical Infrastructure was adopted, specifying FSB control over the system and affirming the final conceptual form of GosSOPKA and requiring all components in this network to share data with it.[57] In sum, "to protect its 'significant objects' a vertical, hierarchical, and centralized system is being built which has the possibility to connect all strategic sectors of the nation to a system of cyber security operated by the FSB."[58]

Several important laws that are aimed at regulating domestic information space and imposing censorship have been passed since 2012. Of note is what is known as the Yarovaya Law, a package of laws passed in 2016 which, under the guise of fighting terrorism, requires ISPs to provide the Kremlin with access to the personal data of their users[59]. The law also increases punishments for hate speech, extremism, and notably criminalizes participation in riots. Other key laws, as compiled from the Swedish Center for Russian Studies, are outlined below.[60]

2012

Internet Blacklist, 139-FZ / 2012-07-28: This law launched a central blacklist monitored by RozKomnadzor (the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications) that can be enforced without a court order. The list now holds 100,000 IP-addresses.

Foreign Agents Law, 190-FX / 2012-11-21: NGOs that receive funding from outside Russia and are engaged in "political activities" are required to register as foreign agents, increasing the government's powers to investigate them.

2013

Prosecutorial Internet blockage, 398-FZ / 2013-12-28: Gives the Prosecutor General's office authority to block websites it deems in contradiction to legislation without a trial.

2014

Dissemination of Historical Narratives, 128-FZ / 2014-05-05: Legislates prison sentences of up to five years for "false information" about the USSR's role in WWII. National television networks use these narratives to mobilize the population in support of the Kremlin's foreign policy objectives. In 2016, a Russian citizen paid a 200,000 ruble fine for posting that the USSR collaborated with the Nazis to invade Poland in 1939.

Law on Bloggers, 97-FZ / 2014-05-05: Bloggers with over 3000 daily site visitors must register with authorities and are held responsible for any comments by third parties on their content.

Law on data localization, 242-FZ / 2014-07-21: Requires the localization of data collected on Russian citizens to be localized to the Russian Federation by 2020 and authorities informed of their whereabouts.

Law on phone number provision for Wi-Fi, government decree no. 758 / 2014-07-31: Users of public Wi-Fi must provide their phone number. As buying a sim card requires a passport, this law makes it virtually impossible to browse the internet anonymously.

Foreign ownership of media companies, 305-FZ / 2014-05-02: Prohibits foreign investors from owning more than 20% of a media company operating in Russia.

2016

'Yarovaya' package of laws, 374-FZ and 375-FZ / 2016-07-06: requires ITC providers to store content and related metadata, and disclose them to authorities without court order; online services (f.e. messaging, e-mail, social networks) that use encrypted data can be accessed by FSB.

2017

Legislation regulating messenger services, 241-FZ / 2017-07-29: requires ISPs with messenger services including WhatsApp to save messages and pictures for six months and give authorities decryption keys.

Law outlawing VPN, 276-FZ / 2017-07-29: bans proxy-services and VPNs.

2019

Sovereign Internet law, 90-FZ / 05-01-2019: requires the installation of software that can filter, reroute and track online traffic and allow Rozkomnadzor to cut Russia off from the global Internet "in case of an emergency." The law came into force on 1 November 2019.

STATE ACTORS AND PROXIES

The actors that support Russia's activities in the information confrontation include both state, with a significant role reserved for Russia's intelligence agencies, and proxies[61]. Publicly available information does not provide details on the organization and decision-making process in Russia's power structures. However, some Western researchers claim that contrary to the hierarchical vertical of power during the Soviet times, it is more decentralized today. The Kremlin tends to set a broad framework for goals to be achieved, expecting subordinates to elaborate and realize the policy. Thus, subordinates are empowered to achieve stated objectives based on the leadership's intent, conditions on the ground, and the actor's consequent judgment.[62] This section will explore the actors and their functions for the Kremlin's activities in cyberspace.

Russian intelligence agencies have three key characteristics. Firstly, their top priority is securing the regime – through preventive action at home and abroad. Secondly, they engage in **competitive intelligence**, fighting for resources and the Kremlin's favor. Thirdly, they view themselves not merely as tools of decision making, but also of direct action.[63]

FSB (the Federal Security Service) is considered the most powerful special service, largely viewed as the successor to the KGB (Committee for State Security in the Soviet Union). Notwithstanding its originally domestic focus, its actions are increasingly being conducted abroad. The service is responsible for counter-intelligence and intelligence collection, including in cyberspace. The FSB is also important actor in securing Russia's domestic information space, and it works in cooperation with federal agencies, such as Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass media), Minsifri (Ministry of Digital Development, Communications and Mass Communications of Russian Federation) and others.[64] For example, FSB has the authority to conduct wiretapping and oversee Russian data traffic via a monitoring system in which all Internet service providers in Russia are obliged to take part.[65]

Western intelligence communities have linked the FSB with **Turla APT** (advanced persistent threat), also known as *Snake, Uroburos*, and *Venomous Bear,* espionage activities. Its quality of programming is significantly more sophisticated and its infrastructure more complex than other attackers with alleged ties to Russia, and its targets are more carefully selected and of more long-term value.[66] *Turla* is believed to be one of the longest-known cyber espionage groups, from the Agent.btz worm that was discovered inside US military

networks in 2008, to more recent espionage campaigns that hijacked satellite internet connections to hide its command and control servers, and silently commandeered Iranian hackers' servers to piggyback on their spying.[67]

GRU or GU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation) is a military external intelligence agency. Perceived as a 'back-seater' to the FSB in earlier cyber operations against Estonia in 2007 and Georgia in 2008, the GRU has become more visible in offensive cyber operations. Western intelligence agencies have attributed most recent significant attacks to this agency.[68] While it is difficult to assess whether the GRU has taken a leading role among other special services in conducting operations in cyberspace, their activities have been more widely discovered and described in detail in publicly available information.

The GRU possess capabilities that can be effectively used for both information-technical and information-psychological dimensions of the information confrontation. The 85th Special Service Centre (Unit 26165), which has been traditionally responsible for signal intelligence and cryptography, and the Main Centre for Special Technologies (Unit 74455), have been responsible for computer-based operations. Unit 74455 is known for hack and leak operations during the 2016 US Presidential election, the creation of *NotPetya* and other malware used for attacking Ukraine's infrastructure, and represents the technical dimension. The 72nd Special Service Centre (Unit 54777), a nucleus of the GRU's psychological warfare apparatus, has been working closely with 'technical' units since at least 2014 and complementing cyberattacks with digital information operations through proxies and front organisations.[69]

Unit 26165 is suspected to be behind the activities of **APT28** (also known as *Fancy Bear, Pawn Storm, Sofacy, Strontium*). It has been one of the most active APT groups that has used highly sophisticated tools for its operations worldwide, particularly targeting the Kremlin's opponents. Although the group's activities have been identified by security companies since 2004, these attacks have only been publicly attributed since 2014.[70] It has been discovered that the group is responsible for interference in the 2014 Ukraine and 2016 US elections, attacks on the German parliament (Bundestag) in 2015, an attack on French television TV5Monde (masking as *Cyber Caliphate* hackers group initially associated with Islamic State), the attempted attack on the Organisation for the Prohibition of Chemical Weapons (OPCW), the 2018 PyeongChang Winter Olympics and more. Both US special counsel Mueller's indictments[71] and EU officials[72] identify APT28 as GRU's Unit 26165.

CyberBerkut is another GRU-related hacktivist-style group, which has been active since the beginning of Russia's conflict with Ukraine. The group appropriated former

> The GRU possess capabilities that can be effectively used for both information-technical and information-psychological dimensions of the information confrontation.

Ukrainian President Viktor Yanukovych's special police force's name (the Ukrainian word *berkut* referring to a golden eagle) and logo, and aligns itself with Russia's influence efforts in Ukraine. However, its identity as a Ukrainian internal opposition group is largely questioned,[73] and more recent investigations indicate that the group coordinates its actions with the GRU's APT28.[74] The group uses both technical and psychological attacks, and has been involved in cyber-espionage, information operations, and disruptive computer network intrusions, including DDoS (Distributed denial of service) against Ukraine, NATO and German government websites.[75] Focused mainly on attempts to discredit the Ukrainian government, the group was involved in the attempted sabotage of Ukraine's presidential election in 2014.[76]

Unit 74455 is suspected to be behind the activities of *Sandworm* group (also known as *Telebots*, *Voodoo Bear* and *Iron Viking)*. The group has been identified by the cyber security industry as responsible for some of the most destructive cyberattacks.[77] In the US indictment from 19 October 2020, GRU hackers were charged with computer attacks that "used some of the world's most destructive malware to date, including: *KillDisk* and *Industroyer*, which each caused blackouts in Ukraine (in 2015 and 2016); *NotPetya*, which caused nearly $1 billion in losses to the three victims identified in the indictment alone; and *Olympic Destroyer*, which disrupted thousands of computers used to support the 2018 PyeongChang Winter Olympics."[78]

SVR (Foreign Intelligence Service) is one of two external intelligence agencies (GRU is the other), and its main tasks are human and strategic intelligence activities. In contrast to the GRU, which uses cyberspace not only for espionage but also for sabotage and information operations, SVR mostly steals information for traditional espionage purposes, seeking secrets that might help the Kremlin understand the plans and motives of politicians and policymakers[79].

> The reason for the use of cyber criminals might be two-fold: it provides plausible deniability as their link to the government is unclear, and it is cost-effective as hackers can be summoned to unleash attacks only when needed, and patriotic hackers will also often work for free.

The security community has connected SVR to **APT29** (*Cozy Bear/The Dukes*) activities[80]. It is a highly-sophisticated hacker group with constantly evolving tools and highly capable operators. The group's attack infrastructure is complex and expensive. The group tends to exploit legitimate online services for its actions, making them less detectable due to their false benign cover.[81] APT29 has been linked to interference in the 2016 US elections, espionage operations against US state agencies, think thanks and NGOs, Dutch and Norwegian government institutions in 2017, as we all as anti-COVID vaccine data in the US, UK and Canada. APT29 may also be behind one of the largest cyber-espionage campaigns targeted against US federal government, security services and critical infrastructure in 2020, dubbed as the 'SolarWinds hack' (named after the company from which software was compromised), [82] while other experts have noticed similarities to the codes used by *Turla* APT.[83]

Until recent years, the information confrontation was considered a function of intelligence services, which is why the armed forces' actions were limited to areas of overlap between cyber operations and electronic warfare. However, there have been media reports about creation of 'information troops' in the Russian armed forces aimed at conducting information operations.[84] In 2013, the Kremlin also announced the creation of a cyber-unit within the military,[85] which includes a wide variety of specialists including programmers, mathematicians, cryptographers, and electronic warfare and communications experts.[86] However, publicly available information on the status of cyber capabilities within the Russian armed forces is limited.

Covert actors affiliated with the state or so called "proxies" encompass oligarchs, businesses, non-profit organizations, the Russian orthodox church, the media, civilians, gangs, government-organized nongovernmental organizations and criminal organizations. Many actors operate in an independent manner despite receiving

financial support and guidance from the Presidential Administration.[87]

An important actor is '**patriotic hackers'**, which refers to people who are not officially part of the state machinery, but who might act based on their attachment to the state either independently or be given direction by the state. Individuals with a background in computer sciences and mathematics are targeted and lured into hacking activities.[88]

In addition to these groups are **cyber criminals,** who are either paid by intelligence services or, if willing to put their skills to the service of the state, will have their prison sentences significantly reduced.[89] An example of Russia's intelligence services' use of criminal hackers is the Yahoo hack. The FSB used criminals (whose actions led to the losses of hundreds of millions of euros for Western companies and financial institutions) to break into Yahoo, committing one of the most significant data breaches in history.[90]

The reason for the use of cyber criminals might be two-fold: it provides **plausible deniability** as their link to the government is unclear, and it is **cost-effective** as hackers can be summoned to unleash attacks only when needed, and patriotic hackers will also often work for free.

Internet Research Agency (IRA), also known as the troll factory of St. Petersburg, is a private organization that operates at the whim of the Kremlin. Its employees, divided into substance-specific departments, contribute to article discussions, comment on social media based on instructions, and create their own infographics and live videos for popular blogging services in order to facilitate Kremlin's narratives or attack its opponents.[91] The activities of the IRA have been attributable since late 2013 (as the Ukrainian conflict escalated), and they have been active in promoting pro-Kremlin narratives and attacking its opponents in Russia and abroad, as well working to increase polarization through social media in the wake of US presidential elections both in 2016 and 2020. Although the IRA took an active role in manipulating audiences and exacerbating societal tensions in the US, its role and effectiveness should not be overestimated. According to Thomas Rid, the US elections have proven the well-established division of labour between IRA and hackers of Russia's intelligence services. Russian intelligence services are conducting their hack and leak operations, while outsourcing the 'noisy and cheap business of driving wedges through social media' to third-party service providers. The IRA 'worked more like a spammy call center than a tight intelligence agency, with limited operational security, very limited presence on the ground of target area and no known operational coordination with Russian intelligence'.[92] The IRA might not be the only company that is working in support of Russia's security interests, as there are several private companies in the market that offer similar services of social media manipulation[93].

Russia's special services involved in cyber operations

Service	Group	Targets
GRU/GU Main Directorate of the General Staff of the Armed Forces	**APT28** *(Fancy Bear, Pawn Storm, Sofacy, Strontium)*	• Ukraine (elections, critical infrastructure) since 2014 • Germany (parliament) 2015 • US (elections) 2016, mid-term elections 2018 • France (media) 2015, (elections) 2017 • Montenegro (government) 2016 - 2017 • WADA/sports organisations 2014 - 2018 • OPCW 2018 • Winter Olympic Games 2018 • Georgia (parliament, media) 2019
	CyberBerkut	
	CyberCaliphate	
	SandWorm	
FSB Federal Security Service	**Turla APT** *(Snake, Uroburos, Waterbug, Venomous Bear)*	• US government since 1990' • Ukraine since 2014 • 35 countries (acting as Iranian hackers) 2019 • Germany (energy and water companies) 2020
SVR Foreign Intelligence Service	**APT29** *(Cozy Bear, Office Monkeys, Duke, CozyDuke, CozyCar)*	• US (government, military) 2014 – 2015 • US (elections, think tanks, NGOs) 2016 • Norway (government) 2017 • Netherlands (government) 2017 • Anti – COVID vaccine research in UK, US, CAN 2020

> No country has weaponized its cyber capabilities as maliciously or irresponsibly as Russia, wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite.[94]

ACTIVITIES IN CYBERSPACE

Russia holds an array of tools for actions in cyberspace, which are both **information-technical** and **information-psychological** and involve state actors as well as proxies. Each tool, nevertheless, suits best a different purpose, which varies from information gathering to influence on decision-making to complementing kinetic operations. It is also important to distinguish between actions aimed at domestic audiences and those targeting foreign countries and various groups therein.

Russia is unique among contemporary cyber powers in its conceptualisation of the indivisibility of technical and psychological computer network operations, which range from offensive cyber operations on critical infrastructure, to using false social media personas to disseminate messaging that supports Russia's foreign policy or military objectives.[95] More than any other country, Russia attempts to achieve cognitive effects when conducting cyber operations.[96]

Most tactics are intended to affect the 'information confrontation' that is happening in the grey zone between war and peace. This section will analyse how this approach is put into practice by exploring cases of Russia's offensive cyber operations.

Ukraine

To date, the conflict in Ukraine remains the most complex example of information confrontation, offering a showcase of Russian means and methods. Ukraine has been in military conflict with Russia since the *Maidan* revolution of 2013. This was swiftly followed by the annexation of Crimea by Russia in 2014 and warfighting in the Eastern part of Ukraine. In the framework of this ongoing conflict, Ukraine has served as an essential testing ground for many of Russia's cyber capabilities.

During Russia's operation in Crimea, coordination between EW, cyber operations

and information operations was used in support of kinetic activities. For example, in 2014, Ukrainian telephone provider UKRTelecom claimed that Russian troops in Crimea had tampered with critical fiber optic cables and severed the connection (landline, mobile and Internet services) between the peninsula and the mainland.[97] The cell phones of Ukrainian parliament members were interfered with, and the Ukraine government website was knocked offline. On March 8, DDoS attacks hit the National Security and Defence Council of Ukraine and the Ukrainian state-run news agency Ukrinform. On March 16, the day of the referendum for Crimea's annexation, NATO websites were attacked by the GRU-linked hacktivist group 'CyberBerkut'.[98]

A significant example which combined technical and psychological means of 'information confrontation' was the targeting of Ukraine's presidential election in May 2014. The elections happened in the wake of the ongoing conflict with Russia and were aimed at discrediting the new Ukrainian government, which was established after pro-Russian President Viktor Yanukovich resigned and fled the country. Three days before the presidential election in May 2014, an attack was launched on the Central Electoral Committee's (CEC) network. The attack disabled real-time display of vote count, and culminated with attackers posting a statement on the CEC website claiming a presidential election win for a far-right candidate. The display of the actual vote count was restored 40 minutes before the final announcement on Ukrainian television, yet the doctored CEC image claiming a false-victory was immediately shown across Russian TV channels, suggesting coordination between Russian hackers and Russian media.[99] While this attack did not have long-lasting effects, it is an example of how many Russian operations are aimed simply at disruption and sowing instability and fear.

Disruption of Ukrainian Power Grid and Infrastructure

Ukraine has also been a victim of disruptive cyber-attacks against its power infrastructure, which caused blackouts for large parts of the population in 2015 and 2016. According to security researchers, those were the first instances in history when cyber attackers caused a major electricity cut; they have also 'used some of the world's most destructive malware to date.'[100] In December 2015, regional electric grids were attacked resulting in a blackout for two to six hours affecting 200,000-230,000 people.[101] A similar incident took place in 2016[102], whereby attackers briefly cut power to one fifth of Kiev's residents, and the railway systems were affected as well. Both incidents involved several phases, beginning with spear phishing and credential harvesting, network mapping, the creation of tools for the exfiltration data, the remote seizure of control systems, and finally the installation of malware.[103] Similar attacks against energy infrastructure have also been registered in the

Baltics, intensifying during Russia's military exercises close to the countries' borders.[104]

Another devastating attack on Ukraine's infrastructure is linked to *NotPetya* ransomware, which began the eve of Ukraine's Constitution Day on 27 June 2017. The attack sought to disrupt the Ukrainian financial system, wiped data from the computers of banks, energy firms, senior government officials and airports.[105]Additionally, the radiation monitoring system at the Chernobyl nuclear power plant went offline. Experts believe that the main target of the attack was Ukraine, but *NotPetya* ultimately spread to the rest of the world including logistic companies, hospitals, and pharmaceutical companies, causing around one billion USD in losses. As US Homeland security expert Tom Bossert stated: 'It was the equivalent of using a nuclear bomb to achieve a small tactical victory."[106]Attacks on Ukraine's power grid, as well as the *NotPetya* attack, have been attributed to the *Sandworm* group of GRU's Unit 74455.

Georgia

Russia has a long history of conflict with Georgia, most notably the war of August 2008 after which Georgia lost control of approximately one fifth of its territory. Georgia is one of the first examples where military operations and cyber/information attacks were used in tandem.[107]

Cyber-attacks during the Russo – Georgian war of 2008

On August 7th, 2008, the Georgian military entered the South Ossetian capital, Tskhinvali, claiming to be responding to bombardments by South Ossetian soldiers. The next day Russian tanks, artillery, and reconnaissance forces entered Tskhinvali, and aircraft conducted airstrikes on Georgian positions in the port city Poti. Russian ground forces moved into Georgia, drawing close to the capital, Tbilisi.

At the end of July, hackers took down the website of Georgian President Mikhail Saakashvili and before Russian troops engaged in direct conflict, many governmental websites went down. Hackers knocked the country's largest commercial bank and media outlets offline and defaced the websites of the Georgian President and Ministry of Foreign Affairs. The attacks were coordinated on public forums that distributed instructions on how to flood websites and provided a list of targets. The website StopGeorgia.ru went up with a full target list only a few hours after Russian troops crossed the border. This would have taken preparation and suggests that the site's organizers had been tipped off on the timing of the military operations.[108]

Cyber-attack against Georgia 2019

A more recent example is the massive cyber-attack against Georgia in October 2019, which exemplifies the sophistication and inseparability of technical and psychological elements in Russia's approach to target its opponents. The attack damaged servers within the Georgian president's office, judicial system, government municipalities, and non-governmental organizations, defaced websites and disrupted broadcast of TV stations. On October 28th, 2019, more than 2000 state (including President Administration), private, and public media websites were defaced alluding to the former president Mikhail Saakashvili (attackers posted Saakashvili's image with the text "I'll be back"). Furthermore, the broadcast of two private television stations - Imedi and Maestro – were disrupted.[109] UK and US authorities attributed the attack to the GRU's unit 74455, also known as *Sandworm*.[110]

Georgia's pro-Western president Mikhail Saakashvili played a major role in the 2008 military conflict and has consistently been the target of the Kremlin's smear campaigns. In the 2013 election, Saakashvili was defeated by the opposition candidate from Dream of Georgia, and he left the country. Since then, Saakashvili is wanted in Georgia on criminal charges, which he claims are politically motivated.[111]

Election Interference

As stated above, one of the strategic goals of information confrontation is to gain superiority over the perceived adversary by targeting its political decision-making, as well as the population's sentiments. Elections are particularly vulnerable, as they provide the opportunity for external actors not only to support a favourable candidate, but also to sow doubt that elections have been fair and free, raise questions about the stability of the country, and erode the trust in democratic process in general.

Russian interference has been identified in elections in several countries. Interference in the 2016 US presidential election is the most documented case which shows Russia's *modus operandi* in using both info-technical and info-psychological tools. This interference involved attacks on US election infrastructure, acquiring, and subsequently leaking, the Democratic Congressional Campaign Committee's (DCCC) and Democratic National Committee's (DNC) data, including party's candidate Hillary Clinton's emails, alongside extensive information campaign conducted by IRA and Russia's affiliated media[112] However, targeted information and cyber operations

related to elections have been observed in Ukraine, France, Sweden, European Parliament and other countries. They are characterized by spear phishing campaigns to access data, hack and leak operations, disruptive attacks on election infrastructure, use of online environment for manipulation and spreading of disinformation.

Interference in French presidential elections: 'Macron leaks' in 2017

Interference in the 2017 French presidential election was a coordinated attempt to undermine Emmanuel Macron's candidacy, with extensive disinformation campaign, and a hack and leak operation against Macron's campaign staff - the so called 'Macron leaks'.

Emmanuel Macron (with the newly established political movement 'En Marche') and Marine LePen (the leader of the far-right 'Front National') were the main candidates for the presidential post.

The campaign against Macron started with rumours and personal attacks which intensified from January – February 2017, which coincided with the time when Macron became a front-runner in the polls due to his most serious rival François Fillon was weakened by scandal. On February 3rd, the Russian-affiliated news agency Sputnik France claimed that Macron was a US agent backed by a very wealthy gay lobby. Information attacks by Russian media, LePen's supporters, and American alt-right trolls were both political (an aristocrat who despises the common man, a rich banker, a globalist puppet, a supporter of Islamism and an advocate of uncontrolled immigration), and personal (age difference between Macron and his wife, rumours of him having an affair with his step-daughter, and speculation about Macron being gay).

Meanwhile, phishing attacks had been targeted against Macron's campaign staff since December 2016. Asa result, the email accounts of at least five of Macron's close collaborators were hacked, and attackers stole 15 gigabytes (GB) of data, including 21,075 emails, and released them on May 5th — just two days before the second and final round of the election.

On May 3rd, 2017, the so called '#MacronGate' rumour spread two hours before the final televised debate between both presidential candidates. A user with a Latvian IP address posted two fake documents on the forum *4chan*, suggesting that Macron had a secret offshore account. During the live televised debate, Le Pen herself alluded to it. The rumour was quickly debunked and several media sources proved these documents to be fabricated.

On May 5th, 2017, only one hour before official campaigning stopped for the period of 'election silence' (a 44-hour political media blackout ahead of the closing of the polls), the hacked files were posted on *Archive.org,* then on *PasteBin* and *4chan*. Pro-Trump accounts were the first to share the link on Twitter, with the hashtag #MacronLeaks, quickly followed by WikiLeaks. The leak was promoted by trolls and fake accounts (bots) appearing in almost half a million tweets in twenty-four hours. Other fake documents spread on Twitter included emails that were not in the dump were from or to people who did not exist.[113]

The attackers did not reach their intended objectives for several reasons, including the structure of the French political system and environment, their own mistakes, as well as a swift reaction by Macron's campaign team, the government, and the media. In the end, Emanuel Macron won the election. However, similarly to 2016 US presidential election, Russia's information efforts did not end with the election day. After the elections, Russia's affiliated media and social media channels continued to spread disinformation about potential election fraud, such as information about low voter turnout, damaged and stolen ballots – all actions aimed at decreasing trust in the election outcome and democratic institutions in general.[114]

Although France did not officially attribute this operation to Russia's operatives, several cybersecurity firms have attributed it to APT 28, the same group has involved in DNC hacking operation during US presidential election a year before.

Targeting Montenegro's Accession to NATO

Cyber operations have been used as part of larger campaigns to hinder the NATO enlargement process, which is perceived as aggressive and threatening by the Kremlin. This was the case of Montenegro as it underwent its final phase of accession negotiations with NATO in late 2016. Russia undertook several forms of attack: Montenegro experience an information campaign by Russian media, threats of embargoes on wine production and other products, an attempted *coup d'état* during the parliamentary election in October 2016, as well as cyber-attacks which can be attributed to Russian special services (ATP28 or Fancy Bear). During this period, Montenegro recorded a sharp rise in the number of cyber-attacks (however not all can be attributed to Russia), mostly targeting state institutions and media outlets. From only 22 such incidents in 2013, almost 400 were recorded in only nine months in 2017.[115]

Attacks against Montenegro (2016 – 2017)

On parliamentary election day on October 16th, 2016, large-scale DDoS attacks targeted state webpages and digital infrastructure, as well as the websites of pro-NATO and pro-EU political parties, civil society webpages and electoral monitors.[116] The same day, Montenegrin authorities discovered an attempted *coup d'etat* against Montenegro's government assisted by Russia's intelligence services. On October 20th, another phishing attack was launched against the parliament of Montenegro, however it did not affect any sensitive information. [117]

A DDos attack larger than the ones targeting elections started on February 15th, 2017, compromising the websites of government and state institutions, as well as some pro-government media. The Montenegrin Ministry of Defence also reported being the target of spear phishing attacks. E-mails that appeared to come from the EU and NATO had attachments that enabled hackers to upload a malware called Gamefish, which has been a signature method used by APT28. Montenegrin officials stated that 'the scope and diversity of the attacks, and the fact that they were being undertaken on a professional level, indicates that this was a synchronised action'. Similar attacks continued in June 2017, after Montenegro officially joined NATO. Cybersecurity firms – FireEye, Trend Micro and ESET – attributed these attacks to APT28. [118]

Influence Campaigns: 'Ghostwriter' and 'Secondary Infektion'

A group called 'Ghostwriter' has been focused on amplifying anti-Western narratives in Poland, Latvia and Lithuania since March 2017. Several separate incidents have been identified in relation to their campaign. They have used fabricated official documents, impersonated government and diplomatic correspondence, spread false narratives and leveraged news sites to spread articles that appear to be legitimate. At least 14 inauthentic personas posing as locals, journalists, and analysts have created or amplified the falsified content.[119]

The timing of 'Ghostwriter' coincides with the arrival of NATO troops in the Baltics and Poland as part of its Enhanced Forward Presence (eFP). The incoming troops were targeted by intense disinformation campaigns in Russian media and on social media.[120] The activities of 'Ghostwriter' were not limited to the creation of fake online personas/bots/media to amplify messages online (a method mostly used by operatives of Internet Research Agency), these activities included technical means, such

> Similar methods of manipulation (forged documents, impersonation, amplification of information by bots/fake personas on social and online media) have been identified in a multi-target campaign dubbed 'Secondary Infektion'.

as compromising webpages and spoofing official e-mails.

Security firms have not attributed 'Ghostwriter' activities to any actor, however they indicated that they serve Russia's security interests, 'primarily seeking to foment distrust of U.S. and NATO troops in Europe by portraying their presence as aggressive and dangerous to local populations, and to undermine military relations between NATO members'[121].

Although no connection or coordination has been proven among both operations, similar methods of manipulation (forged documents, impersonation, amplification of information by bots/fake personas on social and online media) have been identified in a multi-target campaign dubbed 'Secondary Infektion'. Graphica's analysis discovered a 6-year information operation which targeted countries across Europe and North America with fake stories and forged documents. The analysis discovered at least 2500 pieces of content in seven languages across 300 online platforms wielded against Kremlin critics and presidential candidates in the US, France, Germany, Sweden and beyond. The information attacks focused on Ukraine, however they have been active in the US (2016) and French (2017) elections, and against the WADA (World Anti-Doping Agency).[122]

Operation 'Ghostwriter': NATO will leave the Baltics due to COVID-19

On April 21st, 2020, a fake news article on the blog of a well-known Lithuanian journalist (15min.lt) and fact-checker Vilius Petkauskas was published. The piece, titled 'NATO withdraws troops from Lithuania,' was immediately distributed on the marginal websites *TheDuran* and *OpEdNews* (which have previously spread anti – NATO narratives using anonymous online personas with Latvian and Lithuanian-sounding names), as well as

via BlogSpot and Youtube channels created in the name of Petkauskas. Around the same time, a fabricated letter in the name of NATO Secretary General Jens Stoltenberg was sent from spoofed e-mails to the Lithuanian Ministry of Defence, NATO HQ in Brussels, and Lithuanian media and government institutions. The letter stated that NATO was withdrawing its troops from Lithuania due to COVID-19. The letter was immediately debunked as forged by the LTU MoD.

On April 22nd, a one-off Youtube account called 'Nikolas Ratas' published the video 'Is it the end of NATO?' with the forged letter. On April 23rd, another opinion piece on the website *The Baltic Word* was posted by Jonas Dringelis (anonymous online persona), which replicated the official LTU MoD position, but also speculated that the news about the withdrawal might be true. On April 24th, the German media outlet *Die Welt* published the article 'How COVID-19 is destabilizing NATO's Eastern flank', mentioning the forged letter and Russia's disinformation attempts. The Kremlin-funded media outlet RT translated it to Russian, but never mentioned that Stoltenberg's letter was forged.[123]

Although the disinformation campaign was quickly debunked and did not spread in mainstream channels in Lithuania, such activities demonstrate efforts to combined 'technical' and 'information' aspects of influence operations in cyberspace.

> Russia's operatives are not afraid of being discovered and do not hesitate to attack the same target again after being identified.

IMPLICATIONS AND OBJECTIVES

Russia does not apply one uniform cyber-attack strategy across all targets, but has grown to adapt and exploit opportunities as they emerge.[124] The incidents shown above suggest that cyber operations have been used both to support both military action (as in case of Georgia and Ukraine) against traditional opponents and targets of influence activities (as in case of US, NATO, Baltic countries, Montenegro etc.), as well as in cases when an opportunity arises to sow instability and fear. Examples are the case of CyberCaliphate actions in France or interference in the democratic processes of European countries. Furthermore, Russia's operatives are not afraid of being discovered and do not hesitate to attack the same target again after being identified (as, for example, the case of WADA), likely due to the lack of consequences suffered for such activities thus far.

Russia has avoided overt escalation in limiting its cyber activities to generating effects currently considered below the threshold of triggering a conventional armed response,[125] at least in the case of currently identified operations. This style of attack is partially enabled by (although this has recently been changing) the Western paradigm of focusing on destructive offensive cyber operations on critical infrastructure, the theoretical peak of which has oftentimes been referred to as a 'cyber Pearl Harbor'.[126] However, two factors might alter Russia's strategic calculus with cyber operations. The first concerns its strategic deterrence concept, whereby Russia would decide to intensify the use of informational means together with other tools in an attempt at de-escalating a geopolitical confrontation, or at terminating an outright war on terms acceptable to Russia.[127] The second factor is the state of Russian internet sovereignty, which, if successful, would significantly decrease Russia's outward-facing attack surface, thereby enabling it to engage in escalatory measures with less risk of facing effective retaliatory action.[128]

A development that affects NATO's ability to respond to cyber threats is the problem of attribution. Russian hackers have been using false flags when posing as the ISIS-related CyberCaliphate group to attack French TV and US military and media, as well as using the code of North Korean hackers during the attack on 2018 Winter Olympics in South Korea. False flags operations have been taken to a new level, with reports that Russian hackers are hijacking the infrastructure of other countries to spy on targets and deliver malware. In October 2019, the Russian hacking group *Turla* infiltrated the servers of *OilRig*, a prominent Iranian hacking group, using their systems to surveil 35 different countries. It has been argued that the purpose of such false flags is not only to create confusion and deniability, but to sow the narrative that attribution is not possible, undermining the credibility of intelligence agencies when attributing cyber-attacks to Kremlin, and undermine any retaliatory action.[129]

CONCLUSION AND RECOMMENDATIONS

From the Russian perspective, the 'information confrontation' is constant, with the tools used to conduct it including all possible means at its disposal. The front-line of Russia's defensive efforts is its domestic information space, which is tightly controlled by data surveillance and a restrictive legal system aimed at the Kremlin's opponents. The Kremlin wields information-psychological and information-technical weapons with the goal of achieving strategic victory without the use of conventional force and without tripping any escalatory wires in the target country. Securing the domestic information space allows not only the protection of society's psychological cohesion from foreign interference, but also protects domestic scientific and technological developments from foreign competition.

Convinced that the West is constantly waging information war against Russia, offensive actions are justified by responses that are supposedly needed to prevent further escalation in this confrontation. NATO's free and open information environment and often dichotomous understanding of 'war-time' vs. 'peacetime' have been exploited by the Kremlin, making the Alliance and its members long overdue for an updated understanding of what constitutes 'cyberspace' and its relationship with the information environment.

NATO's focus should be on building resilience to address the full spectrum of threats, including ones below the threshold of an armed conflict given that for Russia, information confrontation is constant and is unrestrained by the distinction between peacetime and wartime. There is a growing understanding by Western countries that cyberspace is an environment of permanent confrontation. This has led to policy and doctrine change, and to the adoption of the 'persistent engagement' strategy by the U.S Cyber Command, as well as a similar approach by the French Ministry of Armed Forces.[130] Although significant, these efforts only tackle the technical aspects of information confrontation. This deficit is being tackled by the British Armed Forces' introduction of a special cyber operations unit that has both an offensive and defensive remit to the information-psychological dimension, but more needs to be done Alliance-wide.[131]

There have not been significant alterations or contradictions in Russia's official doctrinal and conceptual publications regarding 'information confrontation' since the beginning of Vladimir Putin's presidency in 1999. Instead, doctrinal thinking has been

built and added on previous ones, inheriting some of the concepts and methods even from the Soviet times.[132] Nevertheless, as Russia's capabilities and methods to engage in 'information confrontation' are under constant development, it means that responses should be adaptive and forward-leaning.

This paper recommends several measures the Alliance and its member nations could undertake to enhance their defence capabilities, starting with recognizing the validity of the Russian understanding of cyber as a tool within a broadly defined information sphere encompassing both technical and psychological aspects:

- **Integrating StratCom functions, with an emphasis on cyber operations:** Creating synergy and even fully integrating functions such as psychological operations, public affairs, cyber operations, electronic warfare and some legal aspects would facilitate significant adaptability with the aim of expanding capabilities during peacetime. Allies may consider the creation of rapid reaction communications teams, a comprehensive approach that could be established as an independent resource that can be rapidly deployed to hostile information environments during operations.

- **Increasing risk analysis of information environment** by identifying which populations and infrastructure are the most vulnerable to cyber and information attacks. NATO analysts should be tasked with more pre-emptive research and planning. They should be identifying what hostile messaging populations are the most susceptible to and identify the root problems leading to those vulnerabilities. This will help allies to design policies that protect their populations from foreign influence and promote resilience and unity during cyber-attacks.

- **Enhancing interoperability by increasing cyber-attack crisis management exercises that include other functions of strategic communications**: This element is key to modernizing NATO's mind set in the sense that it encourages the recognition of information attacks and understand how they are yielded in tandem with cyber operations.

- **Support EU and national governments in enhancing digital security, such as through advocating better data privacy and social media regulation:** NATO can play a significant role in supporting national governments and the EU in securing digital environment among allies and partners. This effort should not be about asserting control over the information space, but about building protection mechanisms to assure that private data and the

> NATO's focus should be on building resilience to address the full spectrum of threats, including ones below the threshold of an armed conflict given that for Russia, information confrontation is constant and is unrestrained by the distinction between peacetime and wartime.

digital footprints of citizens do not fall into hostile hands, at the same time safeguarding core democratic values such as freedom of speech.

- **Bolster deterrence including through attribution and working with partners such as the EU and the private sector:** Beyond the vulnerabilities of an open information environment, the information confrontation lacks a significant strategic deterrent as is provided by nuclear parity in the conventional sense. A lack of inaction in the West after several high-level incidences of interference and cyberattacks has created a perception of low-cost/high reward among adversaries. Therefore, creating a credible deterrent in the realms of the information confrontation is essential. Another way to contribute to deterrence is by taking stronger political measures in response to cyber and information attacks through increasing political consequences. At the political level, increasing attribution and effectively communicating such attacks to the public will assist in improving societal resilience. The EU is an excellent partner for NATO in this regard, having adopted a new sanctions-regime specifically for cyber-attacks.[133]

- **Foster a whole-of-government approach and the involvement of wider society.** The complex nature of the information environment requires many actors beyond NATO to effectively protect it. Private businesses and civil society must be closely engaged on building resilience against hybrid threats. Protecting the integrity of NATO member states is a whole of society effort, as every person and idea can be exploited, with adversaries aiming to influence the attitudes and behaviours of target populations. Therefore, beyond these recommendations, the importance of an informed and critical population that is immune to disinformation and will have reason to trust its political leaders with the protection of society in the event of cyber and informational attacks cannot be understated.

- **Impressing on Russia the futility of creating a closed information space:** Although Russia has undergone immense effort to create an insulated and disconnected information space, this might not be an all-encompassing solution to their strategic and tactical deficits. NATO allies and partners should resist Russia's portrayal of a closed information space as invulnerable, a remnant of Soviet-era thinking. The West's open information space may at times be vulnerable, but the freedoms provided by it inherently contribute to stability and foster adaptable societies that progress to meet the needs of the 21st century. Control of the information space might provide short-term gains, but history shows that a regime's survival in the long-term is questionable when information is repressed and manipulated. Russia's efforts to disconnect its information space from the rest of the world will not prevent its citizens from pursuing information – it is a double edged-sword that may sow more instability than security.

Endnotes

1 For more explanation on the similarities of the concepts, please see: Kukkola J. (2020), Digital Soviet Union. The Russian national segment of Internet as a closed national network shaped by strategic cultural ideas, p.184

2 Russian Federation. Information confrontation, Dictionary of Terms, Russian Ministry of Defence. http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary; V. Veprintsev, A. Manoylo, A. Petrenko, D. Frolov. (2015). Операции информациомнно-психологической войны, Горячая линия – Телеком, pp. 347-348.

3 Information warfare is however often used when referring to adversarial aggression in the information space, Lauder M.A. (2019), Gunshots by Computers, p. 6

4 Kukkola J., Ristolainen M., Nikkarila J-P (2017). Game Changer: Structural transformation of cyberspace, p. 119.

5 V. Veprintsev, A. Manoylo, A. Petrenko, D. Frolov. (2015). Операции информациомнно-психологической войны, Горячая линия – Телеком, pp. 347-348.

6 Kukkola J., Digital Soviet Union., p.107.

7 Russian Federation. (2016). Doctrine of Information Security of the Russian Federation, The Ministry of Foreign Affairs of the Russian Federation; J. Kukkola, M. Ristolainen, J-P. Nikkarila, Game Changer, p. 10. & N. Popescu, S. Secrieru. (2018). Hacks, leaks and disruptions – Russian cyber strategies, EUISS, pp. 17.

8 J. Kukkola, Digital Soviet Union.

9 Russian Federation. (2016). Doctrine of Information Security of the Russian Federation, the Ministry of Foreign Affairs of the Russian Federation.

10 Russian Federation (2011). Conceptual Views on the Activities of the Russian Federation Armed Forces in the Information Space, Russian Ministry of Defence

11 O.Fridman speaking at IISS webinar 'Russia's Use of Cyber Coercion', 3 December 2020

12 O.Fridman speaking at IISS webinar 'Russia's Use of Cyber Coercion', 3 December 2020

13 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, pp. 11-12; Kukkola J., Ristolainen M., Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', Journal of Information Warfare, Vol. 17, No. 2 (2018), 83-100.

14 Giles K. (2016), Handbook of Russian Information Warfare, p. 10.; K. Giles and W. Hagestad II. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English, NATO CCDCOE.

15 Russian Federation. (2011). Conceptual Views on the Activities of the Russian Federation Armed Forces in the Information Space; Mshvidobadze K. (2011). The Battlefield On Your Laptop, RFE. & Giles and Hagestad II, *Divided by a common language*.

16 U.S. Cyber Command. (2018). Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command, pp. 2-10.

17 Olsen J., Creveld M. (2011). The Evolution of Operational Art: From Napoleon to the Present. Oxford University Press, pp. 88-89.

18 Lambeth B. (1993). Desert Storm and Its Meaning: The View from Moscow, RAND, p. 73.

19 Thomas T., Russian Views of Information-Based Warfare, p. 30.

20 Giles K. (2016). Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power, Chatham House, pp. 28-29.; Popescu N., Secrieru S. (2018). Hacks, leaks and disruptions – Russian cyber strategies, EUISS, pp. 5, 15-16.; Blank S. *Cyber War and Information War a la Russe*, p. 84.; Soldatov A. With its cyber troops the Russian military has become political, Raam op Rusland. 31 October, 2018.

21 Iasiello E. (2017). Russia's Improved Information Operations: Form Georgia to Crimea, Army War College, pp. 52-54.

22 Giles K. (2016), Russia's 'New' Tools for Confronting the West, p. 29.

23 Giles K.(2016), Russia's 'New' Tools for Confronting the West, pp. 29-31.; Soldatov A. With its cyber troops the Russian military has become political

24 Giles K. (2019). Moscow Rules: What Drives Russia to Confront the West, Chatham House, Brookings Institution, pp. 35-38.

25 The term 'Colour Revolutions' is used to describe non-violent protests to overthrow the autocratic regimes in the countries of former Soviet Union, such as Georgian Rose Revolution (2003), the Ukrainian Orange Revolution (2004) and the Kyrgyzstani Tulip Revolution (2005). Some sources use the term 'Colour revolutions' also to refer to similar protest movements in Asia and Balkans.

26 Fridman O., The Russian perspective on Information Warfare, Defence Strategic Communications, Vol 2, 2017, pp. 75-76.

27 Giles K., Handbook of Russian Information Warfare, p. 41.

28 Russian Federation (2016), Doctrine of Information Security of the Russian Federation

29 Blank S., Cyber War and Information War a la Russe, p. 84.; Russian Federation (2000). National Security Concept of the

Russian Federation, The Ministry of Foreign Affairs of the Russian Federation.

30 Fink Loukianova A. (2017). The Evolving Russian Concept of Strategic Deterrence: Risks and Responses, Arms Control Association; See also: Kofman M., Fink A., Edmonds J. Russian Strategy for Escalation Management: Evolution of Key Concepts. April 2020, CNA

31 Bruusgaard V. (2016). Russian Strategic Deterrence, Global Politics and Strategy, pp. 9-10.; Fink Loukianova A. (2017). The Evolving Russian Concept of Strategic Deterrence: Risks and Responses, Arms Control Association;

32 Lauder M.A (2019), Gunshots by computers, p. 16.; Meakins J. (2018). Living in (Digital) Denial: Russia's Approach to Cyber Deterrence, European Leadership Network, p. 7.

33 Bruusgaard V., Russian Strategic Deterrence, pp. 14-19.; Forsström P (2019). Venäjän sotilasstrategia muutoksessa: Tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen, National Defence University, p. 183.

34 J. Kukkola, M. Ristolainen, J-P. Nikkarila, Game Changer, p. 21, 23.

35 Giles K., Handbook of Russian Information Warfare, pp. 16-18.

36 Kincaid C. (09.04.2014), How Putin Uses KGB-style "Active Measures", Accuracy in Media; Jaitner M, Mattsson P. (2015), Russian Information Warfare of 2014, NATO CCD COE, p. 39.

37 United States Department of State. (1981). Soviet "Active Measures": Forgery, Disinformation, Political Operations.

38 Rasmussen R. C. (2015)."Cutting Through the Fog: Reflexive Control and Russian STRATCOM in Ukraine." Center for International Maritime Security.

39 Thomas T. (1996). Russian Views of Information-Based Warfare, Airpower Journal, pp. 31-32.

40 Keating K. (1981). Maskirovka: The Soviet System of Camouflage, U.S. Army Russian Institute, p. 4.; Beaumont R. (1982). Maskirovka: Soviet Camouflage Concealment and Deception, The Texas Engineering Experiment Station, pp. 1-3.; Lauder M.A, Gunshots by computers, p. 45.

41 Lauder M.A, Gunshots by computers, p. 45.

42 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, pp. 5, 93.

43 Kukkola J., Ristolainen M, Nikkarila J-P, Game Changer, pp. 11-12. & Pynnöniemi K. Kari M., Russia's New Information Security Doctrine

44 Kukkola J., Ristolainen M, Nikkarila J-P, Game Changer, p. 11.; Barandiy M. (2018). Ideology and Information Attacks: How the Kremlin Builds its Informational Sovereignty; Ashmanov I. (2013). Информационний суверенитет России: новая реальност. Россия навсегда;

45 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, pp. vii, 12.

46 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, p. 13.

47 Kukkola J. Digital Soviet Union. p. 321.

48 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, pp. xiii, 20.; Lavikainen J, Pynnöniemi K. and Saari S, Voiman Venäjä, Puolustusministeriö p. 66.; Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, p. vii.; Kukkola J. Digital Soviet Union.

49 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, p. xi.

50 Kukkola J. Digital Soviet Union.; Kukkola J. The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry, pp.16 – 21; in: Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCD COE, 2021.

51 Polyakova A and Meserole C. (2019). Exporting Digital Authoritarianism: the Russian and Chinese Models. Brookings Institution.

52 Cimpanu C, Some of Russia's surveillance tech leaked data for more than a year, ZDNet 30 Aug 2019,; J A Lewis, Reference Note on Russian Communications Surveillance, Center for Strategic and International Studies, 18 Apr 2014

53 Kukkola J. Digital Soviet Union, p.351

54 Kukkola J. Digital Soviet Union, p.328

55 Fundamentals of the State Policy in the Field of Ensuring the Safety of the Population of the Russian Federation and the Protection of Critical and Potentially Dangerous Objects from Natural Threats, Man-made and Terrorist Acts for the Period up to 2020

56 Turovskiy D. Moscow's cyber-defense: How the Russian government plans to protect the country from the coming cyberwar. Meduza, 19 July, 2017

57 Kukkola J. Digital Soviet Union, p. 349

58 Kukkola J. Digital Soviet Union, p. 346

59 Polyakova A and Meserole C. (2019). Exporting Digital Authoritarianism: the Russian and Chinese Models. Brookings Institution.

60 'RUNET: The Growth of the Authoritarian Internet,' Swedish Center for Russian Studies (2018), p. 3-29, no. 10.

61 This report understands 'state actors' as governmental institutions and its subordinate structures (f.e. intelligence agencies). The 'proxies' are used to describe all non-governmental actors that are receiving direct or indirect tasks from the state or working for the state interests.

62 Galeotti M.. (2016). 'Putin's Hydra: Inside Russia's Intelligence Services', ECFR, p. 12-13. & Lauder M.A, Gunshots by computers, p. 40 - 43.

63 Galeotti M., Putin's Hydra, pp. 4-8.

64 For more information on institutions involved in securing of Russia's information space see. J.Kukkola (2020), Digital Soviet Union.

65 Välisluureamet, International Security and Estonia, p. 54.; Connell M, Vogler S., Russia's Approach to Cyber Warfare, p. 7.; Galeotti M. (2016), Putin's Hydra, p. 2.; Defense Intelligence Agency (2017). Russia Military Power: Building a Military to Support Great Power Aspirations, p. 72.

66 Välisluureamet, International Security and Estonia, pp. 48-49.; Paganini P.(2017). The Snake APT Group is preparing its offensive against high-profile Mac users, Security Affairs, 5 May, 2017

67 Greenberg A. The SolarWinds Hackers Shared Tricks With a Notorious Russian Spy Group. Wired. 11 January, 2021

68 Lilly.B, Cheravitch J., The Past, Present and Future of Russia's Cyber Strategy and Forces, in: 12th International Conference on Cyber Conflict, NATO CCDCOE Publications, 2020., pp.139-141

69 Lilly.B, Cheravitch J. The Past, Present and Future of Russia's Cyber Strategy and Forces, pp.142-146.

70 Rid. T. (2020) Active Measures: The Secret History of Disinformation and Political Warfare. Profile Books, pp.364-365

71 Garret M. Graff, Indicting 12 Russian Hackers Could Be Mueller's Biggest Move Yet, Wired, 13 July, 2018 https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear/

72 COUNCIL IMPLEMENTING REGULATION (EU) 2020/1536, 22 October, 2020

73 Recorder Future. (2015). Cyber Berkut Graduates From DDoS Stunts to Purveyor of Cyber Attack Tools.; E. Kovacs. (2014). Three NATO Websites Disrupted by Ukrainian Hackers of Cyber Berkut, Softpedia.; J. Haines. (2015). Russia's Use of Disinformation in the Ukraine Conflict, FPRI.

74 Maurer T. (2015). Cyber Proxies and the Crisis in Ukraine, CCDCOE, p. 85. & A. Greenberg. (2017). 'Everything We Know About Russia's Election-Hacking', Wired.

75 Defense Intelligence Agency, Russia Military Power, p. 39-40

76 Maurer T, Cyber Proxies and the Crisis in Ukraine, p. 81.

77 Greenberg A. US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit Wired, 19 October 2020

78 Press release by the US Department of Justice, 19 October, 2020

79 Nakashima E. and Timberg C. Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, The Washington Post, 14 December, 2020

80 Välisluureamet, International Security and Estonia, p. 56

81 Weedon J. (2015). Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine, CCDCOE, pp. 69-70.

82 Nakashima E. and Timberg C. Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, The Washington Post, 14 December, 2020

83 Greenberg A. The SolarWinds Hackers Shared Tricks With a Notorious Russian Spy Group. Wired. 11 January, 2021.

84 Connell, Vogler, Russia's Approach to Cyber Warfare, pp. 7-8.

85 Connell, Vogler, Russia's Approach to Cyber Warfare, pp. 7-8.; Soldatov A. and Borogan I., Russia's Approach to Cyber: The Best Defence is a Good Offence in :Hacks, Leaks and Disruptions: Russian Cyber Strategies.2018, p.17

86 Beckhusen R.. The Russian Military Creates Its Own Cyber Troops, War is Boring. 28 May, 2015.

87 Lauder M.A (2019), Gunshots by computers, p. 43; Pernik P.(2018), Hacking for influence, p. 9.

88 Maurer T. (2018). Cyber Mercenaries: The State, Hackers, and Power, pp. 94-95.

89 Connell, Vogler, Russia's Approach to Cyber Warfare, pp. 10-11. & Välisluureamet. (2019). 'International Security and Estonia', pp. 50-53.

90 Maurer T., Hinck G., Russia's Cyber Strategy.

91 Chen A., The Agency, The New York Times Magazine, June 2, 2015

92 T. Rid. Active Meassures: The Secret History of Disinformation and Political Warfare. Profile Books, 2020, p. 409.

93 For more information see: NATO StratCom COE. The Black Market of Social Media Manipulation. Riga, November 2018.

94 Statement by the US Assistant Attorney General for National Security John Demers in the indictment against GRU hackers. See: Press release by the US Department of Justice, 19 October, 2020

95 Cheravitch J., Lilly B.(2021), Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond, In: Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCD COE, p.45

96 Lauder M.A. (2019), Gunshots by computers, pp. 35, 40.; Maurer T., Hinck G. (2018). Russia's Cyber Strategy, ISPI.

97 Weedon J., Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine in K. Geers (ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015, pp. 67-77, https://ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf

98 Croft A, Apps P. NATO websites hit in cyber-attack linked to Crimea tension, 16 March 2014

99 Koval N., 'Revolution Hacking'. In K.Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCDCOE Publications, Tallinn 2015. Pp. 56-58.

100 Press release by the US Department of Justice, 19 October, 2020

101 Your Guide to Russia's Infrastructure Hacking Teams, Wired, 7 Dec 2017

102 Zetter K., The Ukrainian Power Grid Was Hacked Again, Motherboard Tech by Vice, 10 Jan 2017,
103 Lauder M.A., Gunshots by computers, p. 39.
104 S.Jewkes, O.Vukmanovic, Suspected Russia-backed hackers target Baltic energy networks, 11 May 2017, Reuters
105 E.Nakashima. Russian military was behind NotPetya cyberattack in Ukraine CIA concludes. 12 January, 2018, The Washington Post
106 A.Greenberg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History, 22 August, 2018, Wired.
107 A.Greenberg. The US Blames Russia's GRU for Sweeping Cyberattacks in Georgia, Wired, 20 February 2020
108 E.Tiik, K.Kaska, L.Vihul, International Cyber Incidents: Legal Considerations, NATO CCD COE, 2010, pp.69-71; P.Pernik. The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine, in: Hacks, leaks and disruptions: Russia's cyber strategies, EU ISS, October 2018, pp.59 - 60
109 Cimpanu C., Largest cyber-attack in Georgia's history linked to hacked web hosting provider, 28 Oct 2019; Lindsey N., Massive Web Defacement Attack in Georgia Raises New Concerns About Politically Motivated Cyber Attacks, 6 Nov 2019,
110 U.S., U.K. Blame Russia For 2019 Cyberattack On Georgian Websites, 21 February, 2020. RFE/RL's Georgian Service
111 Georgia Hit by Massive Cyber Attack. 28 October 2019, BBC
112 For more details on Russia's interference in 2016 US presidential election, see: Report on the Investigation Into Russian Interference In The 2016 Presidential Election, US Department of Justice, March, 2019.
113 Vilmer J.B.J. The "#Macron leaks" operation: a post-mortem, The Atlantic Council, 20 June, 2019
114 Lilly B. Bringing order through CHAOS: a framework for understanding Russian cyber operations and disinformation during the 2020 U.S. elections and beyond, CyberWire, 2 November, 2020
115 D.Tomovic, M. Zivanovic. Russia's Fancy Bear Hacks Its Way into Montenegro. BIRN, 5 March 2018.
116 O.Jonsson. The Next Front: The Western Balkans, in: Hacks, leaks and disruptions: Russia's cyber strategies, EU ISS, October 2018, p.87
117 D.Tomovic, M. Zivanovic. Russia's Fancy Bear Hacks Its Way into Montenegro. BIRN, 5 March 2018.
118 D.Tomovic, M. Zivanovic. Russia's Fancy Bear Hacks Its Way into Montenegro. BIRN, 5 March 2018.; O.Jonsson. The Next Front: The Western Balkans, in: Hacks, leaks and disruptions: Russia's cyber strategies, EU ISS, October 2018, p.88
119 For more information see: Threat Research: 'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned With Russian Security Interests, FireEye, 29 June 2020
120 For more information see: Russian Narratives on NATO's Deployment, https://medium.com/dfrlab/russian-narratives-on-natos-deployment-616e19c3d194
'**#BalticBrief:** Enhanced Anti-NATO Narratives Target Enhanced Forward Presence', https://medium.com/dfrlab/balticbrief-enhanced-anti-nato-narratives-target-enhanced-forward-presence-fdf2272a8992
121 Threat Research: 'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned With Russian Security Interests, FireEye, 29 June 2020.
122 More details on operation 'Secondary Infektion' can be found here: https://secondaryinfektion.org/
123 For more details see: N. Aleksejeva. Fact-checker's identity stolen to spread disinfo about NATO and COVID-19, **DRF Lab. 29 April, 2020**
124 Pernik Piret. Hacking for Influence – Foreign Influence Activities and Cyber Attacks. February 2018, ICDS Estonia, p.15
125 Pernik, Hacking for Influence, p. 13.
126 J. Lewis. (2017). Fighting the Wrong Enemy, aka the Stalemate in Cybersecurity, the Cipher Brief.
127 Ven Bruusgaard, Russian Strategic Deterrence, pp. 17-18.
128 Pernik, Hacking for Influence, p. 13. & Ministère des Armées, Eléments publics de doctrine militaire de lutte informatique OFFENSIVE.
129 A. Greenberg. A brief history of Russian hackers evolving false flags. Wired, 21 December, 2019,
130 U.S. Cyber Command. (2018). Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command, pp. 2-10.; Taillat S. (2019). Signaling, Victory, and Strategy in France's Military Cyber Doctrine, War on the Rocks.
131 Doffman Z. Cyber Warfare: Army Deploys 'Social Media Warfare' Division To Fight Russia, Forbes. August, 2019.
132 Kukkola J. (2020): Digital Soviet Union.
133 Goebel N. EU to punish cyberattackers with sanctions. Deutsche Welle, 17 May, 2019.

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org