Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West

Author(s): M Ristolainen

Source: *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), pp. 113-131

Published by: Peregrine Technical Solutions

Stable URL: https://www.jstor.org/stable/10.2307/26504121

Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West

M Ristolainen

Information Technology Division, Cyber Defence
Finnish Defence Research Agency,
Riihimäki, Finland

E-mail: mari.ristolainen@mil.fi

Abstract: *Russia aims to create an independent state information system that ensures the network's overall stability by controlling the Internet routing architecture inside Russia. A tightly regulated and secure 'information space' will not only ensure stronger defence against external attacks, but also increase offensive capabilities. This paper asks if the Western perspective that observes cyberspace and cyber security from an 'open' and 'shared' viewpoint is missing something. The author argues that understanding the new Russian threats to cyber security requires an acknowledgement of the essential differences between Russia and the West.*

Keywords: *Digital Sovereignty, Cyberspace Governance, Information Space Governance, Cyber security, Russia, RuNet*

Introduction

From an idealistic Western mindset, the Internet is governed with a strong emphasis on connection, sharing, openness, and freedom—reflecting the worldviews of the computer scientists who developed it. The Internet was designed to share information, and it is threatened by censorship and control. Moreover, the entire cyberspace has been envisioned as a space where borders and states are no longer able to adapt in the so-called Westphalian state system (Tuukkanen 2013; Nocetti 2015a). 'Digital sovereignty' is neither possible nor desired in the cyber security model of 'open, safe, and secure' cyberspace. Nevertheless, the overall aim of the West is to build a more secure cyberspace—"all with[in] the context of maintaining the free and open nature of the internet" (HM Government 2016, p. 35) and with deeper international cooperation (Limnéll 2016, p. 50; EU concept 2016). Opposing the Western vision, Russia has engaged with cyberspace by adapting the idea of 'digital sovereignty' through the development of Internet censorship and control (see, for instance, Ashmanov 2013; Streltsov & Pilyugin 2016). RuNet—the Russian segment of the Internet—is considered an extension of existing territory in the Russian 'information space' and a promoter of a 'digital Westphalia' (Nocetti 2015a, p. 117) or 'cyber Westphalia' (Demchak & Dombrowski 2014). Over the recent years, RuNet has become a platform for the Russian state to use its power by developing laws and technical solutions that challenge the global open Internet.

During the summer of 2016, when NATO recognised cyberspace as a military domain, Russia almost simultaneously declared that RuNet would be disconnected from the global Internet by 2020 (a system designated as 'RuNet 2020'). The contemporary global interpretation of cyber and information security stresses a tendency towards militarisation and declares that the cyber arms race has begun (see, for example, Zinovieva 2016; Limnéll 2016; NATO Cyber Defence 2016; EU concept 2016; HM Government 2016). It seems that both Western and Russian cyberspace and/or information space is becoming a new space within which states may act and reassert traditional notions of sovereignty—yet through contradictory 'open' and 'closed' approaches.

Cyberspace experienced within one state can radically differ from the cyberspace experienced within another. In the Russian approach, cyberspace is used by 'other countries' and hostile forces for the destabilisation of Russia (*Doktrina* 2000; *Doktrina* 2016). This kind of 'besieged fortress' (*osazhdennaia krepost*') mentality has characterised Russian thinking for decades (see, for example, Heller 1988, pp. 108-109; Trenin 2016, pp. 19, 36-39) and led, for instance, to Stalin's purges, the rise of the KGB, and the nuclear arms race. It follows repeatedly the very same fear-based template—the enemy is plotting to encircle Russia, to invade, and overthrow the Russian political system—on land, sea, air, space, and now in cyberspace. In this paper, the author proposes to look beyond Russia's self-victimisation and try to see what is being done behind the 'external enemy' discourse. It seems that many Western scholars view RuNet as pure propaganda and do not seriously consider the possibility that the Russian segment of the Internet could be disconnected from the global Internet. Moreover, RuNet is not considered by Western scholars as a threat to cyber security or even an instrument of deterrence. This paper addresses questions about whether RuNet 2020 should be taken seriously and whether observing cyberspace from a Western 'open' and 'shared' viewpoint causes scholars to miss something fundamental about cyber security. The primary aim of this paper is to identify the essential contradictions in the views about 'digital sovereignty' and cyber security between Russia and the West. Another objective is to try to comprehend the Russian way of thinking so the West can prepare for RuNet 2020.

First, this paper introduces Russian concepts, such as 'information space', 'information counter struggle', and 'digital sovereignty' and discusses their role in the Russian approach to cyber/information security. Second, it provides a short introduction to RuNet. Third, it discusses the measures that have either been completed or aimed at to gradually isolate RuNet from the global Internet. Finally, this paper provides a glance ahead at the global cyberspace of 2020—with or without RuNet.

This article includes a survey of the literature pertaining to the Russian view of cyber security and information space. In the conceptual part of this paper, primary sources include the Russian Federation's information security doctrines, strategies, projects, and ministries' statements. Secondary sources include Russian academic research, ICT specialists' commentary, and academic educational material. Supporting material includes Western commentary on Russian cyber/information terminology. The list of measures that aim to isolate RuNet is composed mainly of official press releases from the Russian Federation's ministries, academic studies, newspaper articles, and online materials from Russian news agencies. As an information or research source, Russian state-controlled media is challenging, and the information given should be treated cautiously. However, it is the best current and open-source information accessible. Additionally, since the original pieces are written in Russian, the material may be meant for the 'RuNet audience'

rather than for international propaganda purposes. The author has also used supporting material from Western news agencies and academic studies. Critical reading and researcher positioning are important considerations for anyone using this type of data for a survey as it is always a subjective account of what is relevant. Therefore, this paper serves as an opening for discussing 'situation awareness' in cyberspace and aims to suggest current, important themes for future cyber security studies that are written from or simply include a Russian studies perspective.

Counter Struggle and Sovereignty as Building Blocks of Security

The lack of common definitions for cyber terminology not only creates difficulties in mutual understanding, but it also reflects a deeper problem—fundamental differences in views about cyber security (see, for example, Giles 2016; Jaitner & Mattsson 2015). In this section of the paper, selected concepts that reflect Russian view about information security are explained in detail.

The Russian understanding of cyberspace is more comprehensive than in the West, which may explain why the Russian terms for cyberspace are 'information space' (*informatsionnaia sfera*) and 'information environment' (*informatsionnoe prostranstvo*). Information space can be defined as a sphere of human activity related to creating, rendering, and using information, Information and Communication Technology (ICT) infrastructure, and information itself (see, for example, *Doktrina* 2000; *Doktrina* 2016). Russian information space includes all mass media, not only information and computer technology platforms (Makarenko & Chucklyaev 2014, p. 14; Kabanov 2014, p. 7). The Russian perspective highlights not only the technical wholeness of information, but also the cognitive wholeness of information (Jaitner & Mattsson 2015, p. 40). Additionally, Russia's operational thinking divides information warfare into digital-technological (electronic warfare) and cognitive-psychological operations (Panarin & Panarina 2003, pp. 244-245; Makarenko & Chucklyaev 2014, pp. 16-17). Moreover, instead of the Western term 'cybersecurity', Russia uses 'information security', a much broader notion and directly connected to the Russian state security (Adamsky 2015, 28-29; Makarenko & Chucklyaev 2014, p. 18). Jaitner and Mattesson (2015, p. 40) argue that the use of non-Western terminology in Russian military strategies and doctrines is done deliberately. Furthermore, Kukkola, Ristolainen & Nikkarila (2017) claim that Russia is able to control the 'cyber domain' with its own and peculiar concepts. Conceptual control forms one line of effort through which Russia is pursuing its objectives in the 'cyber domain'. Likewise, Darczewska (2016, p. 10) suggests that the Russian conceptualisation has been intentionally developed in opposition to the Western cyber concepts in order to create a certain kind of 'terminological newspeak' through which it is—in Orwellian style—impossible to discuss because there are no concepts for it.

One example of such terminological newspeak could be Russian *informatsionnoe protivoborstvo* (see, for example, *Doktrina* 2000; *Doktrina* 2016) that is repeatedly and "deliberately" incorrectly translated into English as 'information warfare' (Franke 2015, p. 10). In Russian *protivoborstvo* does not mean 'warfare', rather its literal translation would be 'counter struggle', 'counteraction' or 'countermeasure'. The verb *protivoborstvovat* can be found in common dictionaries and is translated as 'to oppose' or 'to fight against' (New Comprehensive Russian—English Dictionary 2004 s.v. *protivoborstvovat*'). In English, however, the verb 'to counteract' is defined rather similarly as 'to act against or in opposition to' or 'to oppose' (Oxford English Dictionary 2016 s.v. counteract).

Initially Russian information-theoretical thinking divides *informatsionnoe protivoborstvo* into four stages: (1) 'peaceful coexistence' (*mirnoe sosushchestvovanie*), (2) 'conflict of interests' or 'natural rivalry' (*stolknovenie interesov*/*estestvennoe sopernichestvo*), (3) 'armed confrontation' (*vooruzhennaia konfrontatsiia*), and (4) 'war' (*voina*) (Manoilo 2003, pp. 276-277; Panarin & Panarina 2003, pp. 20-21). Thus, re-conceptualisation might be appropriate; and an improved translation for ambiguous *informatsionnoe protivoborstvo* could be, for instance, 'information counter struggle' or 'information countermeasure'. Unfortunately, the incorrect counter struggle-to-war translation misses the intentionally created rhetorical game—as noted earlier—that Russia has been 'under attack' for decades (the 'besieged fortress' mentality). And for instance, in a cyber conflict situation Russia simply uses *informatsionnoe protivoborstvo* (i.e. 'countermeasures') as a 'defensive response' to the eternal (Western) external enemy. In the recent *Russia military power report* (The United States Defense Intelligence Agency 2017, p. 38) *informatsionnoe protivoborstvo* is translated as 'information confrontation', and the explanation catches the essence of *protivoborstvo* even better: information confrontation

> is a holistic concept for ensuring information superiority, during peacetime and wartime. This concept includes control of the information content as well as the technical means for disseminating that content. Cyber operations are part of Russia's attempts to control the information environment. (The United States Defense Intelligence Agency 2017, p. 38).

According to Thomas (2016, p. 574), simply overlapping Western concepts onto Russian thinking does not always work. A better approach would be "to ponder how new concepts fit into Russia's current military thought process" that requires more intimate knowledge of Russia's overall theoretical and planning process (Thomas 2016, p. 574). For instance, when analysing 'information counter struggle' in the context of the basic principles of war and the tenets of military operations (for instance, initiative, agility, depth, synchronisation, and versatility) that are concepts recognised by modern Russian military thought, Kukkola & Ristolainen (2017) suggest that initiative has already been taken by challenging cyber with information. This enables Russia to define what is included in the 'information struggle'. The concept of a continuous counter struggle allows reacting faster as well as seizing and holding the initiative. Russia can act more versatilely since 'information space' is more extensive than 'cyberspace'. It can meet diverse mission requirements by using both cyber (technical) and information means in various ways. 'Agility' means that Russia is using multiple means and vectors to achieve the same end result and changing its tactics flexibly depending on the situation. Because 'counter struggle' is already ongoing during peace time, Russia is able to synchronise its information operations in time and potentially achieve the desired effects at the decisive point. By framing cyber as information, Russia is, on the one hand, able to operate in the full depth of its adversary's defences using cyber operations without sanctions and, on the other hand, able to legitimise a nationally governed network approach (Kukkola & Ristolainen 2017).

Furthermore, 'digital sovereignty' as a concept has been part of the Russian 'information space' discussion and research starting from 2012 (Dubov 2014, p. 125; Nocetti 2015a, p. 113). One of the main visionaries behind the concept of 'digital sovereignty' is an innovator of RuNet and IT expert Igor Ashmanov, who has been envisioning 'digital sovereignty' as the right and ability of the national government to independently determine geopolitical national interests in the digital environment. When Ashmanov (2013) speaks about 'digital sovereignty', he divides it into

'electronic sovereignty', which contains 'cyber warfare sustainability', and 'information sovereignty', which contains 'information warfare sustainability'. By Ashmanov's definition, 'electronic sovereignty' represents a sustainable infrastructure protecting from viruses, attacks, breakings, leakages, bookmarks, data theft, and spam, whereas 'information sovereignty' is an independent control of information (filtering, blocking, distributing) and a resistance to information attacks (detection, prevention, counter-attack). According to Ashmanov, components of ideal 'digital sovereignty' are autonomous hardware and software platforms (PC and network) and autonomous or controlled mobile platforms, autonomous Internet infrastructure, autonomous mass media structure and TV, autonomous system and means for propaganda and information warfare, and sophisticated ideology and appropriate laws (Ashmanov 2013).

In a 2016 article, Anatoly Streltsov and Pavel Pilyugin explain their view on the main components of 'digital sovereignty' and give the technical parameters of how to maintain a nationally-governed network. To begin with, Streltsov and Pilyugin (2016, p. 25-30) compare 'digital sovereignty' with traditional state sovereignty, see the Internet as a federation of networks, and apply simple border theory based on topography in cyberspace. Furthermore, they explain how there are certain rules of how national borders are to be protected and how different subjects (vehicles, goods, people, and animals) can cross national borders. Streltsov and Pilyugin (2016, p. 28-29) suggest that 'digital sovereignty' requires delineating cyberspace, that is, the formation of 'digital state borders' (*tsifrovaia granitsa*). Similarly, border crossings should be organised through 'digital border crossing points' where the in/out coming (that is, cross-border) traffic can be monitored. Moreover, they introduce the concept of 'digital customs' (*tsifrovaia tamozhnia*). 'Digital customs' would not check all the 'information packets' passing through the 'digital border', but digital customs would have a right to monitor the "legitimacy of the information flow" (Streltsov & Pilyugin 2016, p. 28; Kukkola, Nikkarila & Ristolainen 2017).

In the Russian way of thinking, 'cyber' seems to be recognised as a geopolitical (or 'geodigital') territory, and the intention is to delineate its 'digital borders'. Thus, 'digital sovereignty' appears to be a logical concept for defining and safeguarding the borders of the Russian 'information space' and for ensuring 'information security'. According to Ashmanov (2013), the U.S. is the only country in the world that is 'digitally sovereign'. In the Russian approach, the Internet is a by-product of the dominant American culture and, therefore, poses a threat to the Russian cultural integrity and independence. The global Internet is dependent on popular applications and services that are provided by U.S.-based companies and, therefore, poses a threat to Russian technological integrity and autonomy (see, for example, *Doktrina* 2016). Moreover, the Internet is dominated by the English language and, therefore, the Russian segment of the Internet—RuNet—has emerged as an alternative social universe that celebrates Russian cultural and intellectual tradition.

RuNet—From an Alternative Social Universe to a Model of Secure Environment

RuNet, is a relatively closed, online environment that is based on the Russian language. RuNet is not only in the Russian language, but it is also based on the 'Russian way' of doing things (for example, sovereignty, independence from the West, the 'restoration' of the 'digital sovereignty' mentality). RuNet is a self-contained environment with well-developed and highly popular research engines (*Yandex*, *Rambler*), social network sites (*Vkontakte*, *Odnoklassniki*, *LiveJournal*, *Moi Mir*), and free e-mail services (mail.ru). RuNet has been generally defined as

> a totality of information, communications and activities which occur on the Internet, mostly in the Russian language, no matter where resources and users are physically located, and which are somehow linked to Russian culture and Russian cultural identity. (Gorny 2009, p. 27)

At the beginning, RuNet developed largely free from state influence (Gorny 2009). However, for the past few years, the Russian government has been significantly tightening the control of Russian information space. The increasing activity of the government makes RuNet not only 'more Russian' but also more state-affiliated—the state controls the Internet within its borders and censors or suppresses the information circulated in the Russian information space. Today RuNet offers new perspectives for governing the country. It also offers a 'sphere-of-influence' or 'near-abroad' type of channel in digital form which aims to influence Russian-speaking minority populations in Finland and elsewhere. Furthermore, the increasing 'closed, safe, and secure' rhetoric encourages Russian Internet users to stay within the framework of the 'national web', and this shaping of the information space gives rise to its natural and self-attained isolation. In a global context, RuNet could be seen as a certain kind of prototype for development of 'digital sovereignty'. It diminishes the value of Western 'free and open' Internet, facilitates further digital Balkanisation, and encourages the emergence of other 'sovereign Internets'. Consequently, RuNet has evolved from an alternative social universe to a state-controlled 'safe and secure' digital environment that manifests 'digital sovereignty'.

Russian Measures towards 'Digital Sovereignty'

In May 2016, the Russian Ministry of Communications (*Minkomsvyaz*) circulated in the Russian press new additions to the State Program 'Information Society' (*Minkomsvyaz* 2014) that ensures the protection of the critical Russian Internet infrastructure. The updated program would include plans to eliminate the dependence of RuNet from external networks and to ensure that RuNet would be fully controlled by the state. *Minkomsvyaz* declared that that by 2020, ninety-nine percent of Russian Internet traffic would be transmitted within the country and that a 'back-up copy' of ninety-nine percent of the 'critical infrastructure' within Russia would be created. At that point, 'critical infrastructure' was not defined (*Minkomsvyaz* 2016).

In keeping with the 2015 National Security Strategy's concerns regarding international influence in the field of information security (*Strategiia* 2015), the Information Security Doctrine signed by Vladimir Putin in December 2016 openly aims "to deploy a national system of managing the Russian segment of the internet" (*Doktrina* 2016). The Strategy on the Development of an Information Society in the Russian Federation for 2017-2030 (*Strategiia* 2017) signed in May 2017, follows the Doctrine and takes a top-to-bottom approach to building an information society in Russia. According to the strategy, this means identifying objects of information infrastructure, establishing centralised government-controlled monitoring of networks, using national cryptography, replacing imported technology, using Russian software and services, storing data inside Russia and transporting it using national Internet Service Providers (ISP), and integrating government—including defence networks. The strategy states clearly that the Russian segment of the Internet has to be nationally controlled, independent, self-sufficient, protected from outside interference, and under sovereign jurisdictions (*Strategiia* 2017; Kukkola, Nikkarila & Ristolainen 2017.) As a practical realisation of the Strategy, a State Program 'Digital Economy of the Russian Federation', signed in July 28, 2017 presents a 'road-map' tasking that Russia will be digitally

sovereign by 2020 and that Russia will be one of the world-leading countries in the field of information security by 2024 (*Tsifrovaia ekonomika* 2017).

Over the past years there have been factual measures that resonate well with the recent Doctrine, Strategy and State Programs (*Minkomsvyaz* 2016; *Doktrina* 2016; *Strategiia* 2017; *Tsifrovaia ekonomika* 2017). These measures either have been done or aim to gradually isolate RuNet from the global Internet infrastructure. Thus, the following discussion presents a list of Russian linguistic, cultural, legislative, economic, military and technical measures that show how Russia is intentionally pursuing 'digital sovereignty'.

Language, culture, and spirituality

Today, Russian is the second most-used language in the Internet, and RuNet users are the largest group of Internet users in Europe (Zinovieva 2016, p. 22). For years Russians had been demanding that the Internet Corporation for Assigned Names and Numbers (ICANN) break the English language dominance of the Internet. The Cyrillic domain battle was aimed at raising the status of Russian as a global language and expanding Internet use among Russian speakers unfamiliar with Latin characters (Gorham 2014, p.190). The first Internet domains using the Cyrillic script were launched in May 2010 after Russia was officially assigned the '*рф*' (.rf, for Russian Federation) domain. Currently Russia has three different domain types: .ru, .su, and *.рф* (.su stands for Soviet Union). At the same time, national domains in Arabic were also given to Egypt, the United Arab Emirates, and Saudi Arabia.

According to the Information Security Doctrine (*Doktrina* 2016), "increased information influence on the population of Russia, mainly on the young generation, aimed at erosion of traditional Russian spiritual and moral values" poses a serious threat to Russian information security. A project called 'Clean Internet', which was endorsed by *Minkomsvyaz* in 2012, is an example of the shaping of the Russian information space and its natural and self-attained isolation. Within this project a voluntary association 'Safe Internet League', which celebrates the 'closed, safe, and secure' rhetoric, was established (Soldatov & Borogan 2015, p. 298). According to its website (http://www.ligainternet.ru/), the Safe Internet League is the largest and most reputable Russian organisation fighting dangerous web content. Its volunteers monitor the Internet for violations on behalf of law enforcement. In the league's view, violations include child pornography, pornography accessible to children, promotion of drug and alcohol abuse, as well as violent or 'extremist' content. Despite the prominent role assigned to countering child pornography, the league's actual focus is social media. In many opinions, the league is actually law enforcement's monitoring attempt to match social media's expansion (Carr 2011, pp. 240-241; Gorham 2014, pp. 189-190; Soldatov & Borogan 2015, pp. 201-202).

Legislation for surveillance, control, and isolation

Russia has intensively ratified new laws that meet the objectives of both the Information Security Doctrine (*Doktrina* 2016) and the Strategy on the Development of an Information Society (*Strategiia* 2017). Between 2012 and 2014, the Russian government passed several laws that aimed at gaining a complete control over RuNet (see, for instance, Nocetti 2015b; Vargas-Leon 2016, p. 175) and, some of these laws were tightened in the period 2015-2017. These laws, for instance, allow the Federal Service for Supervision of Communications, Information Technology and Mass Media (*Roskomnadzor*) to block and to censor harmful information and websites deemed extremist

or a threat to public order. They also demand that owners and operators of websites store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action and keep this content for six months. The laws limit anonymous money transfers and donations on the Internet and require all web-based writers (bloggers, social media accounts) with posts that exceed 3,000 page views to register with the government. They control the dissemination or re-dissemination (tweeting and retweeting) of 'extremist materials' and require Internet companies (including Google, Twitter, and Facebook) to locate servers handling Russian Internet traffic inside the country and to store their users' data on these locally-based servers for a minimum of six months. In addition, the laws prohibit anonymous access to the Internet in public spaces; hold media, news services, and search engines liable for all the content in their publications (for instance, links, reposts, and automatically-created links). Moreover, these laws forbid owners of Virtual Private Network (VPN) services and Internet anonymisers from providing access to websites banned in Russia. The most famous of these laws, the so-called counter-terrorism law, known as the '*Yarovaya* package', will take effect in 2018 (Soldatov & Borogan 2015, pp. 215-216,263-264; Vargas-Leon 2016, 176; *TASS* 2017).

In 2016, *Minkomsvyaz* initiated a law-drafting project preliminarily called 'About the autonomous system of the Internet' (Golitsyna & Prokolenko 2016). This project consists of two different proposals to update laws called 'On communications' (*Minkomsvyaz* 2016) and 'On information, information technologies, and on information security' (*Zakonoproekt* 2017) that are literally related to the technical isolation of RuNet. In October 2016, *Minkomsvyaz* released a draft bill that defines basic Internet infrastructure concepts such as 'autonomous system' and 'infrastructure of the Russian national segment of the Internet' and national .ru and *.рф* zone domain name registry from the Russian point of view. The Russian national segment of the Internet is defined as the infrastructure that enables the assigning and functioning of country-code domain names (domain names that end in .ru and *.рф*), systems that can manage the flows of Internet traffic, and other fundamental Internet communication hardware (*Minkomsvyaz* 2016). The draft bill mandates state control of RuNet's entire 'critical infrastructure', including the national .ru and *.рф* domains, Internet traffic eXchange points (IXPs), as well as autonomous systems and networks belonging to various corporations and individuals. That is, the draft bill mandates that all domains in the .ru zone be hosted in Russia and all IXPs belong exclusively to Russian companies (for example, Rostelekom, which is under State control). For the first time, 'critical infrastructure' is defined in detail in this draft bill. This information is reminiscent of earlier statements by *Minkomsvyaz* that claimed Russia needed its own reserve systems should its Internet segment be cut off from the rest of the world if, for instance, Russia were to face a national emergency, such as military action or serious protests (*Minkomsvyaz* 2016; Golitsyna & Prokolenko 2016; Vargas-Leon 2016, p. 175). At the time this article was written (August 2017), the law proposed by *Minkomsvyaz* was not yet approved.

Updates on the law 'On information, information technologies and on information security' were executed by the Federal Security Service of the Russian Federation (FSB) in December 2016 (*Zakonoproekt* 2017). The new bill titled "On the Security of Critical Information Infrastructure of the Russian Federation" was approved at first reading in the state Duma in January 2017. It mandates forming a special registry of all companies and agencies that control elements of critical information infrastructure. It was signed by Vladimir Putin in June 2017, and it will take effect in the beginning of 2018. Russian critical information infrastructure as defined in this law includes,

for example, information systems and telecommunication networks belonging to government agencies; automated control systems for technological processes in the defence industry; as well as spheres of healthcare, transportation, communications, financial institutions, energy, and fuel. Nuclear and aerospace industries, as well as a number of other areas, are also included (*Zakonoproekt* 2017).

Taking all of the legislation for surveillance, control, and isolation into account, it seems that a new official state registry of IP addresses for RuNet might appear shortly and that all of RuNet's 'critical infrastructure' will fall under the complete control of the Russian state authors.

Domestic software

Russia's Information Security Doctrine (*Doktrina* 2016) calls for eliminating the dependence of domestic industries on foreign information technologies and ensuring information security by developing effective Russian technologies. In 2011, the intent was to develop a national Operating System (OS) that would reduce the Russian dependency on Microsoft Windows. Yet the project was called off in 2012 when Nikolai Nikiforov was appointed as the head of the Ministry of Communications. Since then, Nikiforov has repeatedly stated that Russia does not need a national OS. Rather he would promote a Brazil, Russia, India, China, and South Africa (BRICS) OS (Gaidar Forum 2016). Nevertheless, in September 2016, it was reported that the city of Moscow would replace Microsoft programs with domestic software on thousands of computers. Furthermore, the state media company *Rossiya Segodnya* and Moscow's regional government switched from Oracle database systems to open-source software (PostgreSQL) maintained by local programmers (Khrennikov 2016; Kostyleva 2016).

In October 2016, the Russian 'military internet' (*voennyi internet*) was declared fully operational. Officially, the system is called 'Closed segment for data transmission' (*zakrytyi segment peredachi dannykh*), and all of the computers connected to it rely on domestic components and software (Zykov & Ramm 2016). One thing that makes this military internet interesting is that it is supposed to have an email system for transferring highly classified information, including 'top secret' documents, which would make it the fastest way to transfer information in a combat situation. This closed military internet is a response to the concern that the information security of the Russian armed forces and other state institutions is threatened by foreign intelligence agencies (*Doktrina* 2016). There already exists a network for governmental authorities called RSNet (Russian State Internet). To function, RSNet needs to meet the requirements of the GIS State Internet System (*Gosudarstvennaia Informatsionnaia Sistema*): that it is an administrative and legally-controlled concept for secure transmission and processing of data (*Prikaz* 2016.) Theoretically, networks such as the 'closed military internet' and RSNet might serve as testing grounds for domestic hardware and software solutions that could provide independence from the West.

The need for domestic solutions in the economic sphere is also underlined in *Doktrina* 2016, Russia's information security doctrine. The necessity for having a Russian domestic Society for Worldwide Interbank Financial Telecommunication (SWIFT) code and a national payment system became more acute after sanctions were imposed against Russia following the Crimea takeover and war in Eastern Ukraine in 2014. In January 2016, it was reported that about a half of the Russian banks had turned into using the domestic equivalent to SWIFT (Alekseevskikh 2016). A

national payment system would enable independence from the West and could be used together with new allies, for instance, the BRICS countries.

The BRICS cable and new non-Western allies

Together, the BRICS countries aim to challenge American hegemony in global affairs. In 2013, BRICS countries decided to build their own internet infrastructure—'hidden from the NSA'—to enhance cyber security and to create a parallel cyber universe. They announced they would connect the BRICS countries with a new high-capacity underwater cable going from Brazil, around the Cape of Good Hope, northeast up to India, along the Chinese coast, and up to Vladivostok in eastern Russia. The length of the fibre-optic cable would be more than 33 thousand kilometres, making it one of the most ambitious underwater telecom projects ever attempted. The main goal of the project is to create sovereign data access, bypassing all parts of internet infrastructure located outside of BRICS countries. Russia sees BRICS as an influential global actor with 'its own voice' on cyber security issues (Nocetti 2015a, p. 124; Gupta 2016). In 2015, Russia and China signed a 'nonaggression pact' for cyberspace (Kulikova 2015) that well reflects the atmosphere in which Russia is seeking to strengthen, equalise, and stabilise strategic partnerships among 'non-contentious' countries in the field of information security, and to create new allies to challenge the so-called 'post-Western world order' (Lavrov 2017). Allies of these 'non-contentious' countries could be found, for instance, among the framework of the Collective Security Treaty Organization (CSTO) or the Commonwealth of Independent States (CIS) (Nikkarila & Ristolainen 2017).

RuNet as a 'back-up-copy'—Technical puzzles of 2016

Oliphant (2015) reported that the Russian authorities (*Minkomsvyaz*, *Roskomnadzor*, Ministry of Defense, FSB, and *Rostelekom*) trained to disconnect RuNet from the global infrastructure in 2014. Again, according to Oliphant, during the exercise, *Roskomnadzor* ordered communications hubs run by the main Russian internet providers to block traffic to foreign communications channels by using a traffic control system called Deep Packet Inspection (DPI). However, the experiment failed because thousands of smaller service providers, over which *Roskomnadzor* had little control, continued to pass information out of the country (Oliphant 2015).

Russian officials originally initiated the idea of creating and maintaining a 'back-up-copy' of RuNet in 2014 (Sukharevskaia 2016; Sukharevskaia & Iuzbekova 2016; Nazarov 2016). Along with the additions to the 'information society' state program launched in June 2016, more detailed technical plans for disconnecting RuNet from the global Internet by 2020 were also announced. According to the Russian news agencies, an autonomous non-commercial organisation Moscow Internet eXchange (MSK-IX), which owns, along with *Rostelekom*, the largest internet traffic exchange point in Russia, started to study the formation of 'back-ups' of the RuNet (Sukharevskaia 2016; Sukharevskaia & Iuzbekova 2016; Nazarov 2016). The terms for 'back-up' mostly used in Russian are '*rezervnaia*' (reserve), *'kopiia'* (spare or back-up), '*dubl*' (from the English word 'double'), and more rarely '*zerkalo*' (a mirror). Since, as noted earlier, the aim is to exclude foreign ownership of Russian IXP's (*Minkomsvyaz* 2016), the term 'back-up' might refer to state ownership and regulation of the entire critical infrastructure.

According to Alexey Platonov, head of MSK-IX, the first phase of the project will include macroscopic studies of the internet that will be identified as 'walking' traffic and interaction between autonomous systems (Sukharevskaia 2016). The study will be the basis of a unified

system that will combine the databases of the Dutch RIPE (French for 'European IP Networks') Network Control Center (NCC) (which is responsible for distributing IP addresses between telecommunications operators, including Russian) and other registries and databases of route information of the internet (that is, the intention is to make an analogue of RIPE) (Sukharevskaia 2016). Each operator independently determines the policy for routing traffic. Companies do not share this information with each other, but manifest their routes in the routing database—the Internet Routing Registry, which is also under the control of the RIPE NCC (Sukharevskaia & Iuzbekova 2016).

Minkomsvyaz also intends to create its own set register of traffic exchange points and to oblige operators to use only registered points. It will propose to owners of these points that they build reserve channels of communication funded from the state budget. Only operators who have licenses for cross-border data communication can organise international communication channels. Such international communication is not under control of the *Sistema Operativno-Rozysknykh Meropriiatii* (SORM), the technical specification for lawful interception interfaces of telecommunications and telephone networks operating in Russia, which must be installed by each Russian operator (Sukharevskaia 2016; Sukharevskaia & Iuzbekova 2016). In other words, the national operators (that is, providers) would be able to organise the traffic, but they would be under the control and supervision of the state. According to Streltsov & Pilyugin (2016, p. 29), all of this could be organised with existing technology by using Border Gateway Protocol (BGP), a standardised exterior gateway protocol designed to exchange routing and reachability information among Autonomous Systems (AS) on the Internet. Together with an innovative use of Software-Defined Networking (SDN) technology, individual states would be able to form their own policies and international agreements for the 'digital border crossing'. Moreover, Streltsov and Pilyugin (2016, p. 30) suggest that anonymity on the internet can be erased by different nationally controlled register mechanisms of IP-addresses and domains, and the state-owned provider of cross-border traffic implements the authentication of any entity interacting with a global network.

Published technical details of RuNet are still scarce. Nevertheless, all of the discussed technical measures aim to control the internet routing architecture inside Russia and to prepare for maintaining operational capabilities outside of the global Internet. The most alarming fact is that disconnection can most likely be executed with existing technology and protocols, which makes the process rather fast and relatively inexpensive to complete; the 'RuNet 2020' timeframe might actually be realistic.

Discussion—A Global Cyberspace of 2020 with or without RuNet

The aim of this paper has been to illustrate to the Western audience the nature of Russian information space, 'information counter struggle', and 'digital sovereignty' *and* to explain the Russian way of thinking about information security and/or cyber security. As shown in this paper, the Western idealism of the Internet as 'open, safe, and secure' has been seriously challenged by the Russian alarmism that seeks a 'closed, safe, and secure' internet. Western scholars have largely underestimated the mental, legal, and technical measures Russia has taken to create RuNet. Indeed, RuNet is still not considered a threat to cyber security or even an instrument of deterrence by the West. Observing Russia from a Western perspective or with a reliance on Western concepts obscures both the strength of Russia's desire to restore information sovereignty and its progress toward the goal of digital sovereignty. The Russian challenge to the U.S.-dominated/-led world

order is real, serious, and long term (Trenin 2016, p. 19). It may be tempting to perceive the Russian government's internet policy as backwards and authoritarian; however, Russia has officially endorsed the concept of disconnecting the Russian segment of the internet from the global Internet. The intent is to control the internet routing architecture inside Russia and to maintain operational capabilities outside of the global Internet. Consequently, the isolation of RuNet would have at least three alarming and potentially serious cyber security outcomes: (1) weaponization of information (Pomerantsev & Weiss 2014), (2) fragmentation of the global Internet, and (3) intensification of cyber deterrence. The first two outcomes have already essentially come to fruition.

An isolated RuNet will make confronting Russia's weaponization of information even more difficult. Coordinated information operations that target both a domestic audience and the 'near abroad' audience will be used to convince Russians that they are under attack and that greater censorship of RuNet is justified. These operations will create a 'besieged-fortress' mentality. For security purposes, RuNet will keep opposition information out and Russian data in. Moreover, information warfare targeted outside of RuNet will be easier to conduct, and the recruitment of free-will agitators (information fighters) will occur almost naturally. Since the U.S. presidential election of 2016, there has been a growing concern about Russia's intention to exert covert influence over peoples and governments.

Furthermore, RuNet might serve as an example and encourage the emergence of other 'sovereign internets' to push global cyberspace towards fragmentation. There are already several examples of aims to de-Westernise, maintain control over internet users, and control the spread of information (for instance, the Great firewall of China, Halal internet of Iran, Pakistan's intranet, BRICS internet, and data localisation requirements). De-Westernising and digital Balkanisation would fundamentally influence cyber security.

Information space is still relatively new to the Russian military. However, Russia is intently developing both defensive and offensive capability to operate in the cyber realm. It seems that Russia is preparing itself for a confrontation in a hostile environment (see, for instance, *Doktrina* 2016; *Strategiia* 2017). Clearly, Russia has integrated offensive cyber capabilities, including Distributed Denial of Service (DDoS) attacks, malware, and advanced information warfare (for example, troops for 'informational operations') into its military arsenal (The U.S. Defense Intelligence Agency 2017, pp. 38-40). Consequently, RuNet would increase not only defensive capabilities, but also offensive capabilities. The Russian military's manoeuvrability, firepower, and protection in cyberspace would be at a relatively higher level than the expected enemy's (Nikkarila & Ristolainen 2017; Kukkola, Nikkarila & Ristolainen 2017; Kukkola, Ristolainen & Nikkarila 2017).

The arms race in cyberspace is certainly accelerating. We in the West should no longer ask 'if' an attack on our network will be successful, but 'where' and 'how' such an attack will occur (see, for instance, EU concept 2016). However, perhaps this is what Russia wants us to contemplate when it is by itself focused on building resilience on a national level and aiming towards digital sovereignty. The 'RuNet 2020' project indicates that Russia is not only striving for 'cyber weapons' or 'cyber-attack capabilities', but also for 'resilience' and 'recovery plans'. In this arms

race, Russia is leading and as a result, Russia might be writing a new chapter in the theory of cyber deterrence.

There is still a great deal of confusion about how deterrence would work in the cyber domain. The new Russian Information Doctrine states that strategic deterrence and preventing military conflicts are among the main methods of ensuring information security (*Doktrina* 2016). Nevertheless, the wisdom of applying classical Cold War deterrence theory to cyber warfare is disputable (see, for instance, Nye 2017; Bendiek & Metzger 2015; Davis 2014; Lindsay 2015; Stevens 2012; Elliot 2011; Libicki 2009). Moreover, the Russian concept of 'strategic deterrence' (*strategicheskoe sderzhivanie*) is broader than the direct Western equivalent. The Russian concept contains defensive, nuclear, non-nuclear, and non-military tools of deterrence (Bruusgaard 2016, pp. 7-8; Adamsky 2017, p. 3). Simply put, the success of deterrence comes down to one side's ability to convince another side that there is no point in attacking. If the Russians are able to develop an independent and resilient network that can absorb an attack, limit its impact as much as possible, and be quickly restored to full operational capability, it could inaugurate a new form of cyber deterrence that may be referred to as 'deterrence by denial' (Elliot 2011, p. 38). 'Deterrence by denial' in the RuNet context would mean persuading an enemy not to attack because that attack will be defeated. This idea could fall under the non-military deterrence component of the Russian strategic deterrence concept (Bruusgaard 2016, p. 14-15). Moreover, when Russia's own system is independent of the global network, Russia could deter attacks both technically and kinetically.

In the Western mindset, 'deterrence by denial' has been recognised as an 'answer to cyberattack' (Elliot 2011, p. 38). However, it has been considered too difficult to achieve "without major technical advances and significant new policies" (Elliot 2011, p. 39). As shown in this paper, Russia has developed and is developing domestic hard- and software, has pursued alternative technical solutions, and has ratified new laws and policies. In the Russian understanding, a technically independent and legally supported RuNet will be a safe and reliable digital infrastructure. Thus, 'RuNet 2020' could be considered a Russian 'disaster recovery plan' and 'business continuity plan', the likes of which other EU countries have only recently started to consider and plan for (EU concept, 2016).

Once RuNet is technically successful, Russia will raise the level of cyber resilience to a new level—it will be claiming 'digital sovereignty', and the era of the global Internet may be passing. It is clear that Russia will pursue its own 'digital sovereignty' through a combination of propaganda, psychological operations, and manipulation of information. Before this occurs, the West should improve its understanding of the context within which Russia makes its assessments. The West should study Russia's planning processes, then thoroughly re-conceptualise and re-analyse the Russian concept of 'information space'. Certainly, the West should acknowledge that 'RuNet 2020' should be taken seriously.

Acknowledgements

The author wishes to acknowledge the support and guidance received from colleagues Captain Juha Kukkola (National Defence University) and First Lieutenant (Eng.) Juha-Pekka Nikkarila (Finnish Defence Research Agency) during the writing and re-writing of this article.

References

Adamsky, D 2015, *Cross-Domain coercion: The current Russian art of strategy*, Proliferation papers 54, Ifri Security Studies Center, Brussels, BE.

——2017, 'From Moscow with coercion: Russian deterrence theory and strategic culture', *Journal of Strategic Studies*, 24 July 2017, pp. 1-28.

Alekseevskikh, A 2016, '*Rossiiskie banki zashchitilis' ot otkliuchenii iz Briusselia*' (Russian banks protect themselves against outages from Brussels), *Izvestiia*, 11 January, viewed 2 November 2016, <http://izvestia.ru/news/601876>.

Ashmanov, I 2013, '*Doklad: Informatsionnyi suverenitet. Sovremennaia real'nost*' (Presentation at iForum 24 April, Information sovereignty, contemporary reality), *Rossiia navsegda*, viewed 17 October 2016, <http://rossiyanavsegda.ru/read/948/>.

Bendiek, A & Metzger, T 2015, 'Deterrence theory in the cyber-century', Working Paper, Research Division EU/Europe *Stiftung Wissenschaft und Politic*, German Institute for International and Security Affairs, viewed 15 November 2016, <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf>.

Bruusgaard, K 2016, 'Russian strategic deterrence', *Survival*, vol. 58, no. 4, pp. 7-26.

Carr, J 2011, *Inside cyber warfare: Mapping the cyber underworld*, O'Reilly Media, Inc., Sebastopol, CA, U.S.A.

Darczewska, J 2014, 'The anatomy of Russian information warfare: The Crimean operation, a case study', *Point of View*, no. 42, Centre for Eastern Studies, viewed 1 October 2016, <https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf>.

Davis, PK 2014, 'Toward theory for dissuasion (or deterrence) by denial: Using simple cognitive models of the adversary to inform strategy', *RAND Working Papers WR-1027*, January, viewed 1 December 2016, <http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf>.

Demchak, C & Dombrowski, P 2014, 'Cyber Westphalia: Asserting state prerogatives in cyberspace', *Georgetown Journal of International Affairs*, no. 20, pp. 29-38.

Doktrina 2000, *Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* (Information security doctrine of the Russian Federation), 9 September, viewed 31 October 2016, <http://www.scrf.gov.ru/documents/6/5.html>.

Doktrina 2016, *Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* (Information security doctrine of the Russian Federation), 5 December, viewed 5 December 2016, <http://static.kremlin.ru/media/acts/files/0001201612060002.pdf>.

Dubov, D 2014, '*Kibermogushchestvo kak bazis obespecheniia "tsifrovogo" suvereniteta v sovremennom mire: kliuchevie podkhody*'. (Cyberpower as a fundamental concept for digital sovereignty in the contemporary world: Key aspects), *Oborona i bezopasnost'*, vol. 4, no. 25, pp. 123-35.

Elliot, D 2011, 'Deterring strategic cyberattack', *IEEE Security and Privacy*, September/October 2011, pp. 36-40.

EU concept 2016, *EU concept on cyber defence for EU-led military operations and missions*, 22 November 2016, Brussels, Belgium.

Franke, U 2015, *War by non-military means: understanding Russian information warfare, FOI-R-4065-SE*, Swedish Defence Research Agency, viewed 18 October 2016, <https://pdfs.semanticscholar.org/2869/71ba9762da1d039d0d40a27c94e0ec8d31ac.pdf>.

Gaidar Forum 2016, '*Polnaia videozapis' repli*ki Nikolaia Nikiforofa *na Gaidarovskom Forume* 2016', (Full video clip of Nikolai Nikiforov's statement at the Gaidar Forum 2016), 16 January, viewed 22 October 2016, <https://vk.com/video292653561_171817033>.

Giles, K 2016, *Handbook of Russian information warfare*, Fellowship monograph 9, Research Division, NATO Defence College, November, viewed 19 December 2016, <http://www.ndc.nato.int/news/news.php?icode=995>.

Golitsyna, A & Prokolenko, A 2016, '*Chnovniki khotiat podchinit' sebe ves' rossiiskii internet*', (Officials want to supress under their control the entire Russian Internet), *Vedomosti*, 27 May, viewed 2 November 2016, <http://www.vedomosti.ru/technology/articles/2016/05/27/642739-chinovniki-hotyat-internetom>.

Gorham, M 2014, *After Newspeak: Language, culture and politics in Russia from Gorbachev to Putin*, Cornell University Press, New York, NY, U.S.A.

Gorny, E 2009, *A creative history of the Russian Internet*, Studies in Internet Creativity, VDM Verlag Dr. Muller, Berlin, Germany.

Gupta, A 2016, 'Cold War-style 'cyber arms race' between US and Russia: Reality or rhetoric?', *Center for Air Power Studies (CAPS)*, vol. 98, no. 16, viewed 2 November 2016, <http://capsindia.org.managewebsiteportal.com/files/documents/CAPS_Infocus_AG_19.pdf>.

Heller, M 1988, *Cogs in the wheel: The formation of Soviet man*, Collins Harvill, London, UK.

HM Government (UK), 'National strategy 2016-2021', viewed 1 August 2017, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>.

Jaitner, M & Mattsson, P 2015, 'Russian information warfare of 2014', *Proceedings of the 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 2015, eds. M Maybaum & A Osula, NATO CCD COE Publications, Tallinn, Estonia, pp. 39-52.

Kabanov, Y 2014, *Information (cyber-) security discourses and policies in the European Union and Russia: A comparative analysis*, Working papers, vol. 1/2014, Centre for German and European Studies (CGES), Bielefield/St. Petersburg, viewed 31 November 2016, <http://www.zdes.spbu.ru/assets/files/wp/2014/WP_2014_1%20%20Kabanov.compressed.pdf>.

Khrennikov, I 2016, 'Moscow drops Microsoft on Putin's call for self-sufficiency', *Bloomberg Technology*, 27 September, viewed 30 September 2016, <https://www.bloomberg.com/news/articles/2016-09-27/moscow-drops-microsoft-outlook-as-putin-urges-self-sufficiency>.

Kostyleva, T 2016, '*Uchastniki IT-rynka ob importozameshchenii softa: zakon slishkom miagkhii, o rezul'tatakh govorit' rano*' (Participants of the IT-development on the software substitution: The law is too soft, it is too early to speak about results), *Digital Russia*, 23 September, viewed 30 September 2016, <http://d-russia.ru/uchastniki-it-rynka-ob-importozameshhenii-softa-zakon-slishkom-myagkij-o-rezultatax-govorit-rano.html>.

Kukkola, J, Nikkarila, J-P & Ristolainen, M 2017, 'Asymmetric frontlines of cyber battlefields', Forthcoming in *Proceedings of the 22nd International Command and Control Research and Technology Symposium (ICCRTS)*, Los Angeles, CA, U.S.A.

——, Ristolainen, M & Nikkarila, J-P 2017, 'Confrontation with closed network nation: Open network society's choices and consequences', *Proceedings of the Military Communications (MILCOM) 2017*, Baltimore, Maryland, U.S.A.

——& Ristolainen, M 2017, 'Russian conceptual control of the cyber domain: The five basic principles of war', Poster in the *16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.

Kulikova, A 2015, 'China-Russia cyber-security pact: Should the US be concerned?' *Russia Direct*, 15 May, viewed 30 September 2016, <http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned>.

Lavrov, S 2017, 'Foreign Minister Sergey Lavrov's address and answers to questions at the 53rd Munich Security Conference', 18 February, The Ministry of Foreign Affairs of the Russian Federation, viewed 19 March 2016, <http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2648249>.

Libicki, M 2009, *Cyberdeterrence and cyberwar*, RAND, Santa Monica, CA, U.S.A.

Limnéll, J 2016, 'The cyber arms race is accelerating—what are the consequences?', *Journal of Cyber Policy*, vol. 1, no. 1, pp. 50-60.

Lindsay, J 2015, 'Tipping the scales: The attribution problem and feasibility of deterrence against cyberattack', *Journal of Cybersecurity*, vol. 1, no. 1, pp. 53-67.

Makarenko, S & Chucklyaev, I 2014, '*Termonologicheskii basis v oblasti informatsionnogo protivoborstva*' (The terminological basis of the informational conflict area), *Voprosy kiberbezopasnosti*, vol. 1/2014, pp. 13-21.

Minkomsvyaz 2014, '*Gosudarstvennaia programma: "Informatsionnoe obshchestvo" (2011-2020 gody)'*, (State program Information Society [2011-2020]), 27 August, viewed 18 October 2016, <http://minsvyaz.ru/ru/activity/programs/1/>.

——2016, *Federal'nyi zakon "O vnesenii izmenenii v Federal'nyi zakon "O sviazi" (Proekt)* (Federal Law, On the changes to the Federal Law, On communications), October 11, viewed 22 October 2016, <http://regulation.gov.ru/projects#npa=58851>.

Manoilo, A 2003, *Gosudarstvennaia informatsionnaia politika v osobykh usloviiakh* (State Information Policy in Special Circumstances), MIFI, Moscow, Russia.

NATO Cyber Defence 2016, 'NATO cyber defence fact sheet', July, Public Diplomacy Division (PDD)—Press & Media Section, viewed 22 October 2016, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf>.

Nazarov, D 2016, '*Rezervnaia kopiia: Mozhno li otkliuchit' rossiiskii internet ot global'noi seti*?', (Back-up-copy: Can the Russian segment of the Internet be disconnected from the global system?), *FurFur*, 1 September, viewed 4 October 2016, <http://www.furfur.me/furfur/freedom/freedom/218695-chto-takoe-rezervnaya-kopiya-interneta>.

Nikkarila, J-P & Ristolainen, M 2017, 'RuNet 2020—Deploying traditional elements of combat power in cyberspace?', *Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS)*, 15-16 May 2017, pp. 1-8.

Nocetti, J 2015a, 'Contest and conquest: Russia and global Internet governance', *International Affairs*, vol. 91, no. 1, pp. 111-30.

——2015b, 'Russia's "dictatorship-of-the-law" approach to Internet policy', *Internet Policy Review: Journal on Internet Regulation*, vol. 4, no. 4, pp. 1-19.

Nye, J 2017, 'Deterrence and dissuasion in cyberspace', *International Security*, vol. 41, no. 3, pp. 44-71.

Oliphant, R 2015, 'Russia 'tried to cut off' World Wide Web', *The Telegraph*, 15 October, viewed 19 October 2016, <http://www.telegraph.co.uk/news/worldnews/europe/russia/11934411/Russia-tried-to-cut-off-World-Wide-Web.html>.

Ormrod, D & Turnbull, B 2016, 'The cyber conceptual framework for developing military doctrine', *Defence Studies*, vol. 16, no. 3, pp. 270-98.

Panarin, I & Panarina, L 2003, *Informatsionnaia voina i mir. Informatsionnoe protivoportsvo v sovremennom mire* (Information war and peace: Information counter measures in the contemporary world), OLMA-PRESS, Moscow, Russia.

Pomerantsev, P & Weiss, M 2014, 'The menace of unreality: How the Kremlin weaponizes information, culture and money', *The Interpreter*, no. 11/2014, viewed 15 November 2016, <http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf>.

protivoborstvovat' 2004, *New Comprehensive Russian—English Dictionary*, eds., D Ermolovich & T Krasavina, Russkij Jazyk, Moscow, Russia.

Prikaz 2016, *Prikaz FSO Rossii ot 07.09.2016, no. 443 "Ob utverzhdenii Polozheniia o rossiiskom gosudarstvennom segmente informatsionnoe-telekommunikatsionnoi seti* "internet" (Order of FSO Russia 07.09.2016, no. 443 About approval of the condition on the Russian segment of the state information-telecommunication network*)*, viewed 15 December 2016, <http://www.gov.ru/main/rsnet/pr_fso_443_07092016.pdf>.

Rozhkov, RO 2016, '*Pervye litsa: Internet "liazhet" na sutki? Ia etogo voobshche ne ponimaiu" Gendirektor* TTSI Aleksei Platonov *ob osobennostiakh raboty interneta v Rossii*', (Leading faces: Internet "falls down" in 24 hours? I truly don't understand it, Aleksei Platonov CEO the Technican Centre of Internet speaks about the specialties of Internet in Russia), *Kommersant'*, 18 March.

Soldatov, A & Borogan, I 2015, *The Red Web: The struggle between Russia's digital dictators and the new online revolutionaries*, Public Affairs, New York, NY, U.S.A.

Stevens, T 2012, 'A cyberwar of ideas? Deterrence and norms in cyberspace', *Contemporary Security Policy*, vol. 33, no. 1, pp. 148-70.

Streltsov, A & Pilyugin, P 2016, '*K voprosu o tsifrovom suverenitete'* (About digital sovereignty), *Informatizatsiia i sviaz'*, no. 2/2016, pp. 25-30.

Strategiia 2015, *"Strategiia natsional'noi bezopasnosti Rossiiskoi Federatsii"* (Russian National Security Strategy), 31 December, viewed 8 March 2017, <http://static.kremlin.ru/media/acts/files/0001201512310038.pdf>.

——2017, *'Strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na* 2017-2013 *gody*' (The 2017-2030 Strategy for the Development of an Information Society in the Russian Federation), viewed 24 July 2017, <http://static.kremlin.ru/media/acts/files/0001201705100002.pdf>.

Sukharevskaia, A 2016, '*Zapasnoi Internet: Kto zaimetsia sozdaniem "reservnoi kopii"'* (Spare Internet: Who will establish the "back-up-copy"), *RBK: Ezhednevnaia delovaia gazeta*, 7 July 2016.

——& Iuzbekova, I. 2016, '*Tri voprosa o suverennom runete*', (Three questions about sovereign RuNet), *RBK: Ezhednevnaia delovaia gazeta*, 6 June.

TASS 2017, '*Regulirovanie interneta v Rossii*', (Internet regulation in Russia), *TASS*, viewed 9 August 2017, <http://tass.ru/regulirovanie-interneta-v-rossii>.

Thomas, T 2016, 'The evolution of Russian military thought: Integrating hybrid, new-generation, and new-type thinking', *Journal of Slavic Military Studies*, vol. 29, no 4, pp. 554-75.

'to counteract' 2016, *Oxford English Dictionary Online*, Oxford University Press, viewed 15 December 2016, <https://en.oxforddictionaries.com/definition/counteract>.

Trenin, D 2016, *Should we fear Russia?* Polity Press, Cambridge, UK.

Tsifrovaia ekonomika 2017, *Programma: 'Tsifrovaia ekonomika Rossiiskoi Federatsii'* (State project: Digital economy of Russian Federation), viewed 1 August 2017, <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf>.

Tuukkanen, T 2013, 'Sovereignty in the cyber domain', *The fog of cyber defence*, eds. J Rantapelkonen & M Salminen, National Defence University, Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection 10, Helsinki, Finland, pp. 37-45.

The United States Defense Intelligence Agency 2017, *United States Defense Intelligence Agency report: Building a military to support great power aspirations*, Defense Intelligence Agency, viewed 2 August 2017, <http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf>.

Vargas-Leon, P 2016, 'Tracking Internet shutdown practices: Democracies and hybrid regimes', *The turn to infrastructure in Internet governance*, eds. F Musiani, D Cogburn, L DeNardis & N Levinson, Information Technology and Global Governance, Palgrave Macmillan, New York, NY, U.S.A., pp. 167-88.

Zakonoproekt 2017, *Zakonoproekt No. 47571-7: 'O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii'* (Bill No. 47571-7: On the Security of Critical Infrastructure of the Russian Federation), viewed 28 February 2017, <http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C5851432580810054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement>.

Zinovieva, E 2016, '*Vozmoshnosti Rossii v global'nom informatsionnom obshchestve*' (Russia in the global information society), *Vestnik MGIMO universiteta/MGIMO Review of International Relations*, vol. 3, no. 48, pp. 17-29.

Zykov, V & Ramm, A 2016, '*V Rossii poiavilsia voennyi* internet', (A military Internet appeared in Russia), *Izvestiia*, 19 October.