Georgia Tech School of Public Policy

Sovereign Runet: What Does it Mean?

Ilona Stadnik

SUMMARY

This case study of RUnet is based on the theoretical framework of cyberspace alignment to national borders introduced by Mueller (2017). He argues that instead of technical fragmentation of the Internet, there are attempts to align the control of cyberspace with national borders. There are three main methods to implement such an alignment: national securitization, territorialization of information flows, and efforts to structure control of critical Internet resources along national lines. This theoretical and methodological frame is useful to study various ongoing process in Russia towards the Internet and explain what is happening with RUnet and how close it is now to become a truly "sovereign network."

The first part of this study describes national securitization in detail. It consists of four components: (1) emergence of cybersecurity as a national security issue in the Russian doctrinal documents; (2) centralization of threat intelligence in a form of GOSSOPKA program and creation of the National Coordination Center for Computer Incidents; (3) reliance on nationally produced technologies promoted by a state program of import substitution in software development and application; (4) establishment or reassertion of legal authority for network kill switch. The study shows that each of four components take place in the Russian policy with varying levels of completeness and success.

The second part of the study deals with territorialization of information flows that includes external content filtering, data localization laws and geo-blocking. Russia has a comprehensive mix of all components; however, it doesn't look similar to the Chinese Golden Shield. On the contrary, there is a gradual process of territorializing data and information, elaboration of laws regulating the blocking of websites with unlawful content and filtering of search engine results.

The third part of the study, devoted to the alignment of critical Internet resources to national borders, is the most interesting because of its implications for Internet fragmentation. Mueller explained it as a partition of the global domain name and IP address spaces along national lines to provide nation-states with greater leverage over the governance of the Internet in their territory. The case of RUnet offers an opportunity to track the development of legislation that deals with critical Internet infrastructure and attempts to create a system that allows RUnet to work independently form Internet in case of emergency or external shutdown.

The case study provides evidence for the Mueller's theory and illustrates the nationalization of Internet governance in Russia. But the most important aspect that threatens the Internet with fragmentation is unpacking now in a form of a recent legislation about the new logic of routing policies and attempts to make RUnet independent from procedures that the Internet Corporation for Assigned Names and Numbers uses to maintain the global network. If eventually there will be a technical solution to make RUnet independent, Russia will create a dangerous precedent for Internet fragmentation.

Keywords: RUnet, sovereignization, Internet governance, fragmentation, alignment

INTRODUCTION

The Russian government is well-known for its perpetual claims about dividing the Internet into "national segments" so that it can try to impose the logic of sovereignty on them. The "sovereign" segment refers in particular to "RUnet."

Historically, RUnet was the title for the web resources and services inside Russia's Country Code Top Level Domains, namely *.SU*[1], *.RU,* and later, the *.рф* and other Cyrillic domains; it also referred to online resources in the Russian language, regardless of the domain used. However, Russian legislators gradually began to use RUnet to mean a geographically defined network space located within the state's boundaries and subject to its authority. Recent years have seen numerous attempts by the Russian legislators and national security agencies to make the Russian networks independent from the global Internet in order to maintain their security and stability from external challenges.

Asserting sovereignty over the so-called national segment of the Internet is a real trend nowadays and happens predominantly in authoritarian countries. By the catchy term of "sovereignization," mass media, think-tanks and politicians mean various Internet governance practices of states ranging from expansive filtering and blocking of unwanted websites and services to the real infrastructural isolation of the local networks from the global Internet. In the meantime, there is a widespread impression that eventually the Internet will be fragmented by sovereign states to ensure their ability to protect and regulate the new domain of citizen interaction.

While Mueller argues that actual technical fragmentation of the Internet is unlikely, he claims that what is really happening is an attempt to *align* control of cyberspace with their national borders while preserving the benefits from using the global network. He suggested three main methods to implement the alignment: national securitization, territorialization of information flows, and efforts to structure control of critical Internet resources along national lines. We will use Mueller's framework of alignment to explain what is happening with RUnet and how close it is now to become a "sovereign network."

National securitization

National securitization consists of four parts, according to the alignment framework. The first is to make cybersecurity a national security issue; the second is to centralize and nationalize threat intelligence; the third is to attempt to nationalize technical standards and rely more on nationally produced technologies; the last is to develop a kill switch capability.[2] We see each of these at work in Russia, but with varying levels of completeness and success.

Reframing Cybersecurity

The process of securitization starts with reframing cybersecurity as a national security issue, together with recognition of cyberspace as a military domain. Securitization means that "societal dependencies on information technologies and networks create vulnerabilities that could pose an existential threat to the state itself."[3]

In Russia, cybersecurity as a term is not common in official language; instead, information security is used. According to the 2016 *Doctrine on information security*,[4] the information security of Russia means "the station of security of an individual, the society and the state from internal and external information threats at which are provided: implementation of the constitutional rights and freedoms of an individual and the citizen; good quality of living for citizens; sovereignty, territorial integrity and sustainable social and economic development of the Russian Federation;

[1] The domain .SU previously served for USSR organizations. At the moment, it is positioned as a domain for organizations working in the post-Soviet space.

[2] Milton Mueller. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace.* London: Polity (2017) p. 37.

[3] Ibid.

[4] This document is a strategic planning in the field of national security of Russia, and the Doctrine develops the provisions of the National Security Strategy of Russia published in 2015.

defense and security of the state."[5] The Russian national interests in the information field are now "objectively significant *needs* of an individual, the society and the state *in ensuring their security* and sustainable development in the area of information."[6] More specifically, national interests include a number of responsibilities of the state and other actors, divided in five areas and consolidated around content security, cybersecurity of information infrastructure, advancement of technological potential, and international information security based on the principle of sovereignty[7]. Also, the Doctrine catalogues the main threats to information security. Among these are: unlawful cross-border content flows, exposure of national critical infrastructure to attacks, use of ICT to influence the psychology of the population and to destabilize the political system, dependency on foreign ICT hardware and software, and improper distribution and control over critical Internet resources.

Militarization of cyberspace

According to Mueller, creation of military "Cyber Commands" is also a part of national securitization because it this is how states develop capabilities to engage in cyber conflict and defend themselves. Militarization of cyberspace is against Russian stance at the international level – on the contrary, Russia promotes the idea of peaceful use of ICT and responsible state behavior, while preventing the possibility of cyberconflict. In 1998 Russia was the first at the United Nations to raise the concern about the possible use of ICT in inter-state conflicts and pushed the adoption of the resolution that called states to promote the consideration of existing and potential threats in the field of information security. [8] Interestingly, back in 2011 there was a framework document named "*Conceptual views on the activity of the Russian Armed Forces in the information space*".[9] It stated that the Armed Forces should adhere to "deterrence and prevention of conflicts in the information environment, conduct conflict resolution if it occurred through negotiations, reconciliation, appeal to the UN Security Council or to regional bodies or agreements, or other peaceful means." In the context of escalation of a conflict in the information space and its transition to the crisis phase, the Armed Forces can "*use the right to individual or collective self-defense using any chosen methods and means that do not contradict the universally recognized norms and principles of international law*". The major part of the document is devoted to several principles the Armed Forces should observe in the information space, among others: the principle of *legality* (act in accordance with the Russian and international law); the principle of *complexity* (use all available forces and means in information space (intelligence, operational camouflage, electronic warfare, communication, hidden and automated control, information work of the Staff); the principle of *cooperation* (establish an international legal regime governing the military activities of states in the global information space on the basis of international law and regional mechanisms of collective defense).

However, despite the peaceful international rhetoric, the first public mention about the Russian cyber command goes back to 2012, when Russian Vice-Prime Minister Rogozin voiced the necessity to create a division similar to the United States Cyber Command[10]. But only in February 2017 was it officially announced that now Russia has its own "*information operations troops*"[11]. In between these dates there was an active work of creating "scientific troops" – the Army recruited young professionals in the field of ICT to serve like traditional soldiers or as a civil staff in research centers affiliated with the Ministry of Defense (MoD). Also, there was a "big hunt" during 2013 on software developers among

---

[5] Doctrine on information security. (2016). Part I. https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

[6] Ibid.

[7] Doctrine on information security. (2016). Part II, paragraph 8.

[8] A/RES/53/70 "Developments in the field of information and telecommunications in the context of international security". The UN General Assembly, 53rd session. http://undocs.org/A/RES/53/70

[9] Conceptual views on the activity of the Russian Armed Forces in the information space. (2011). Ministry of Defense. http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

[10] В российской армии может появиться киберкомандование, заявил Рогозин. [In the Russian army may appear cyber command, said Rogozin]. (2012, March 21) RIA Novosti. Retrieved from: https://ria.ru/20120321/601798789.html

[11] В Минобороны РФ создали войска информационных операций. [The Ministry of Defense created the troops of information operations]. (2017, February 22) Interfax. Retrieved from: https://www.interfax.ru/russia/551054

graduates who could perform some work for the MoD that can be counted as military service for students[12]. In May 2014 anonymous sources in the MoD claimed that troops of information operations were formed in the Armed Forces to protect the Russian military systems of control and communications from cyberattacks[13]. Nevertheless, representatives of the Russian Parliament denied any presence of "cyber troops" in the Armed Forces structure, though pointed that the state had faced with the task of protecting its own information and all countries that claim to be superpowers conduct R&D in this field. From 2014 to 2016 the MoD never spoke publicly about the structure of information troops, their size or number of employees. At the same time, publications about their achievements appeared in sources close to MoD, and many vacancies that could be linked to information troops were published on career portals. In need were employees familiar with the use of exploits and reverse engineering. Social networks promoted among youth the attractive idea of scientific troops and their technologically (and intellectually) advanced position over traditional forces. Ultimately, in January 2017 the newspaper Kommersant reported that according to the draft of a Zecurion Analytics study (a Russian cybersecurity firm) that Kommersant had in disposal, Russia is ranked in the top five countries in terms of the number and financing of cyber troops – $300 million per year for around 1000 employees[14]. However, the published report didn't mention Russian capabilities at all and it dated after the publication in Kommersant[15]. A month later the Minister of Defense Shoigu disclosed the creation of information troops that substituted the former counter propaganda bureau of the Soviet Union[16]. Details about this new division in MoD are classified, but small pieces of information in mass media signals that their purpose is to repel cyberattacks on Russian military networks and "expose foreign sabotage in electronic, paper and television media" according to the Deputy Chairman of the Federation Council Committee on defense and security.

Nationalization of threat intelligence

The next step for securitization is nationalization and centralization of threat intelligence reporting and sharing capabilities**,** together with development of national CERTs. In this field Russia also has a continuous history in law-making and practical steps.

In January 2013, President Putin signed a Directive creating a system of detection, prevention and elimination of consequences of computer attacks on information resources (GOSSOPKA), under the supervision of Federal Security Service (known as FSB)[17]. The purpose of this massive state initiative was to create a system of information sharing between the most significant organizations and entities in the country on ongoing cyberattacks and thus elaborate a preventive protection. However, the implementation of the directive was not immediate: FSB worked on specific documents and recommendations about the structure of the system and the technical requirements of the equipment for detection, prevention and elimination of computer attacks on critical information resources. The first "pilot" centers of GOSSOPKA started to emerge in some federal government agencies around 2015.

At the same time, FSB struggled to pass the law on critical information infrastructure (CII) that would define its objects, classify their significance, and integrate GOSSOPKA into the logic of ensuring the security of CII. Only in July 2017 did

---

[12] Сергей Шойгу объявил о «большой охоте» на молодых программистов. [Sergei Shoigu announced a "big hunt" for young programmers]. (2013, April 07) CNews. Retrieved from: http://www.cnews.ru/news/top/sergej_shojgu_obyavil_o_bolshoj_ohote

[13] Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций. [Source in the Ministry of Defense: in the Armed forces of the Russian Federation created troops of information operations]. (2014, May 12) TASS. Retreived from: https://tass.ru/politika/1179830

[14] В интернет ввели кибервойска. Аналитики оценили количество хакеров на госслужбе. [Cybertroops were sent to the Internet. Analysts estimated the number of hackers in the civil service] (2017, January 10) Kommersant. Retrieved from: https://www.kommersant.ru/doc/3187320

[15] Zecurion Analytics (2017, January 13) Кибервойны 2017: баланс сил в мире. [Cyberwars 2017: balance of power in the world]. Retrieved from: http://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf

[16] Шойгу рассказал о российских войсках информационных операций. [Shoigu told about the Russian information operations troops] (2017, February 22) RBC. Retrieved from: https://www.rbc.ru/politics/22/02/2017/58ad78cd9a794757f3c80ece

[17] Указ Президента Российской Федерации от 15 января 2013 г. №31 [Decree of the President of the Russian Federation dated 2013 January 15, №31] Retrieved from: https://rg.ru/2013/01/18/komp-ataki-site-dok.html

the Parliament pass law FZ-187 on the security of Russia's critical information infrastructure[18]. The law provided a definition of objects (i.e., physical objects that comprise critical infrastructure), and subjects (i.e., owners of objects) and their responsibilities in relation to the law. The law also created a registry of CII objects. CII objects include information systems, information and telecommunication networks, and the automated control systems of CII owners[19]. CII owners can include state institutions, Russian legal entities/individual entrepreneurs that interact with the above-mentioned systems and networks in all sectors of the economy, energy, production and defense. The law prescribes the subjects to categorize[20] the CII objects in order to define their significance and prioritize their security, to insure the integration of CII objects into GOSSOPKA, and finally, to take organizational and technical measures to ensure the security of CII. Also, the law defined GOSSOPKA as a system that consists of geographically distributed centers of various scales that exchange information about cyberattacks. Such centers are required to be created in all companies and public agencies that own CII. In addition, the law contains amendments (published in a separate FZ-194) to the Criminal Code that establishes criminal liability for wrongful/illegal acts against CII objects[21].

By the end of 2017 the President signed a second Directive aimed at enhancing the system[22]. It gave the FSB executive control over GOSSOPKA in accordance with FZ-187 and endowed the FSB with tasks to monitor the degree of information security in the country, to ensure interaction between owners of information resources of Russia, telecom operators and other entities responsible for licensed info-security activities, and to develop guidelines to detect computer attacks and prevent them in future based on the information gathered by GOSSOPKA. However, FZ-187 contained too many unresolved issues in the text to make its full implementation possible. Gradually, from December 2017 to July 2018, the FSB, the Federal service for technical and export control, and the Government issued orders and regulations to make it possible for subjects to comply with the law.

But the most important development in centralization of threat intelligence was the last three orders by FSB issued in July 2018. They establish the National Coordination Center for Computer Incidents (NCCCI), defined the list of information required to be submitted to GOSSOPKA[23] and regulate the way the Russian CII subjects can exchange information about computer incidents[24]. The rules cover both exchanges among CII subjects and foreign partners in incident response, such as foreign CERTs. Also, it offers analytical support to detection and response to computer incidents. The powers of NCCCI are significant. All international incident response interactions must only go through NCCCI (except where there are special cooperation agreements, but even then NCCCI must be notified). It can refuse

---

[18] Federal law dated 26.07.2017 №187-FZ. Retrieved from: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.247740626598083 7#07294351284912781

[19] The process of defining CII is not comple yet. There is a covert struggle of telecom operators and Internet exchange points to escape the categorization of their infrastructure as critical to avoid the high costs of compliance with FZ-187.

[20] Telecom operators and banks delay implementation of the law on CII. The process of categorization is a hard task for telecom sector. They try to categorize objects as many small and insignificant, while supervising body tries to combine elements of infrastructure into larger and more significant objects. Banks, in addition to the new FZ-187 have to comply with regulation of the Russian Central Bank.
See more: Нестрашные хакеры: почему не работает закон о критической инфраструктуре. [Informidable hackers: why doesn't work the law on the critical infrastructure]. (2019, February 01) RBC. Retrieved from: https://www.rbc.ru/technology_and_media/01/02/2019/5c53222e9a794766142b2a41?from=center_2

[21] Преступление и наказание для владельцев критической информационной инфраструктуры РФ. [Crime and punishment for owners of critical information infrastructure of the Russian Federation] (2018, January 10). Habr (blog). Retrieved from: https://habr.com/ru/post/346372/

[22] Указ Президента Российской Федерации от 22.12.2017 г. № 620. [Decree of the President of the Russian Federation dated 2017 December 22, №620]. Retrieved from: http://www.kremlin.ru/acts/bank/42623

[23] Приказ Федеральной службы безопасности Российской Федерации от 06.09.2018 № 52108. [Order of the Federal Security Service dated 09.06.2018 № 52108]. Retrieved from: http://publication.pravo.gov.ru/Document/View/0001201809100002?index=0

[24] Приказ Федеральной службы безопасности Российской Федерации от 06.09.2018 № 52107. [Order of the Federal Security Service dated 09.06.2018 № 52107]. Retrieved from: http://publication.pravo.gov.ru/Document/View/0001201809100003?index=0

to share information about incidents with foreign counterparts if such information is deemed to threaten the national security of Russia.

GOSSOPKA is tasked to provide information on methods and means to respond to computer incidents to the subjects of CII through NCCCI. The latter was created within the Center for information security and special communication of FSB. Also, NCCCI is now adopting the functions and infrastructure of the GOV-CERT which was also established in 2012 by FSB for incident response in government networks of Russia. It is worth mentioning that in the mid of 2017, while FSB orders were still under elaboration, Sberbank (the largest state-owned bank and leading giant in cybersecurity) stepped up with its own vision of the national cybersecurity center[25]. The center would be curating all existing institutions in the field of information security of the country, including RU-CERT, GOV-CERT, FinCERT and GOSSOPKA. The overall idea was criticized by cybersecurity experts, because the creation of a national center by a bank (though huge and innovative in cybersecurity as Sberank) is utopia, as well as the scale for incident response. However, this case illustrates that there was an urgent necessity to create a unified body responsible to coordinate national cybersecurity.

To summarize, it has taken Russia 5 years to set up and elaborate the necessary legal basis for a government-led threat intelligence collection, sharing and reporting system under the supervision of the Federal Security Service. Still, the situation with Russian CERTs seems to deviate from this goal. There are at least five CERTS for different purposes and sectors, which are not yet nationalized or centralized and probably will continue to function as they do now:

- RU-CERT was created by the Russian Institute for Public Networks (a research institute for the development of computer networks for scientific and educational organizations, and basic elements of Russian Internet infrastructure). According to its website, RU-CERT provides assistance to Russian and foreign legal entities, LEAs and individuals in identifying, preventing and suppressing illegal activities related to network resources located on the territory of the Russian Federation. It also collects, stores and processes statistical data related to the spread of malware and network attacks in the Russian Federation. RU-CERT claims to be a full-member and contact point for Russia in Forum of Incident Response and Security Teams (FIRST) since 2001. However, its efficiency is under a question: working hours are "10:00-18:00 Moscow time, except weekends and official holidays;" the only publication on the website, a report on phishing attacks, dates back to 2017. It is hard to say how effective they are in incident response.
- CERT-GIB is a leader among private emergency response teams by Group-IB – the Russian leading information security vendor with antifraud and anti-APT solutions and threat Intelligence. CERT-GIB helps everyone 24/7 with DDoS attacks, distribution of malicious software, fraudulent web-resources, botnet-related incidents, phishing and attacks on e-banking and electronic payment systems. CERT-GIB officially collaborates with the Coordination Center of the .RU top level domain and blocks dangerous websites in the .ru, .su and .рф domains. It is also a member of FIRST, Association of European Security and Incident Response Teams and a partner of the International Multilateral Partnership Against Cyber Threats (IMPACT).
- GOV-CERT.RU was established by the FSB to protect Russian governmental networks. It coordinates state authorities, local authorities and LEAs on identifying, preventing and eliminating consequences of computer incidents concerning state information and telecommunication networks. Now its functions are taken over by NCCI, though its website and a form for reporting an incident are still available. The working hours are 09:00-18:00 Moscow time except weekends and official holidays, which also seems to contradict the logic of an incident response team.
- FinCERT was created in 2015 by the Russian Central Bank to collect information on cyberattacks in the financial sector and exchange it with law enforcement authorities, banks and financial institutions, as well as issue

[25] Киберспецслужба: Сбербанк предложил создать штаб борьбы с хакерами. [Cyber special service: Sberbank suggested to create a special HQ to struggle with hackers]. (2017, September 01) RBC. Retrieved from: https://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15

guidelines for the safe transfer of funds. FinCERT positions itself as an industry center of GOSSOPKA because it deals exclusively with incidents in financial and credit sector.

- KASPERSKY LAB ICS CERT Kaspersky's Industrial Control Systems Cyber Emergency Response Team was launched in 2016 for coordination of manufacturers of automation systems, owners and operators of industrial facilities, information security researchers for protection of industrial enterprises and critical infrastructure facilities. The project is still alive, though it lost a bit of relevance after adoption of FZ-187 about CII. Kaspersky tried to adapt it for deployment of GOSSOPKA centers on CII objects, but was not successful yet.

Other private sector actors are also active in incident information sharing. Bi.Zone (a daughter enterprise of Sberbank that serves as an external information security division) and Association of Russian Banks launched a new platform for information sharing between credit companies in 2019. In fact, it duplicates the work performed by FINCERT. Also, Bi.Zone plans to help medium-sized enterprises obliged to connect to GOSSOPKA by reducing the costs, according to the national program "Digital Economy"[26]. In 2018, Rostelekom acquired Solar Security, which operates in the field of targeted monitoring and operational management of information security. Thus, the Russian telecom giant plans to create a national cyber security operator of Russia on the basis of Solar Security products[27]. Among others, it aims to create information security management centers (SOC), and corporate and departmental centers of GOSSOPKA in accordance with FZ-187. Finally, there are plans to create a special CERT for the telecom industry. These plans are not defined yet, as it involves a big investment in a contractor for deploying the center.

To sum up, public CERTS seem to be not so willing to engage in 24/7 work, in comparison to their private sector counterparts. A separate story is FinCERT, but it is a well-designed structure confined to the financial sector. NCCCI still have to prove its efficiency because it exists a bit more than 6 months as of this writing. Private CERTs are more client-oriented, and cope with its task. Meanwhile, all CII objects should have special centers integrated to GOSSOPKA, that in fact serves as nation-wide CERT under the auspice of FSB. Deployment of its centers is a complicated and costly task, so we can see the major players of the industry doing mergers and acquisitions to grab a piece of the market of ready-made solutions for the creation of GOSSOPKA centers, because there are a lot of operators and owners of CII objects that are not all technically and financially able to implement the FZ-187 on their own.

National standards and technologies

Reliance on national standards and technologies also helps with securitization process. Import substitution has become a buzz word for the Russian government since 2014 after events in Ukraine and Crimea were followed by a cascade of anti-Russian sanctions. This spurred debates about high levels of dependence on foreign software and hardware, especially for governmental needs. Another reason to think about import substitution in IT sector were the Snowden revelations in 2013 which showed the US National Security Agency's ability to use vulnerabilities and backdoors for espionage purposes.

After a long discussion with the industry in 2015 the government issued a Decree "On the establishment of a ban on the admission of software originating from foreign countries for the purposes of procurement for state and municipal needs." This policy is also reflected in the Doctrine on Information Security which was published in 2016. Among other threats the document mentions "a high level of dependence of the domestic industry on foreign information technologies in terms of the electronic component base, software, computer equipment and means of communication, which makes the socio-economic development of the Russian Federation dependent on the geopolitical interests of foreign countries". So, one of the declared aims is to reduce "to the minimum possible level of influence the negative factors caused by insufficient level of development of domestic IT and electronics industry,"

[26] Малый бизнес хотят защитить от кибератак через «дочку» Сбербанка. [They want to protect small businesses from cyberattacks through the "daughter"of Sberbank]. (2018, October 17) Vedomosti. Retrieved from: https://www.vedomosti.ru/technology/news/2018/10/17/783864-malii-biznes-kiberatak

[27] «Ростелеком» купил Solar Security, чтобы стать «национальным оператором кибербезопасности России». ['Rostelecom' bought Solar Security to become a "national provider of cyber security in Russia"]. (2018, May 22). D-Russia. Retrieved from: http://d-russia.ru/rostelekom-kupil-solar-security-chtoby-stat-natsionalnym-operatorom-kiberbezopasnosti-rossii.html

and to enhance development and production of domestic tools for ensuring information security, while increasing the scope and quality of rendering services in the field of information security.

In accordance with the Decree, Ministry of Communications and Digital Development (MoC) started to maintain a registry of Russian software[28]. Since January 1, 2016 the registry has more than 5000 items that cover operating systems, cloud storage, office software and database toolkits. Interestingly, one of the owner categories has "Russian commercial organization with foreign persons in the chain of ownership" that fully illustrates the real problems of import substitution in software development. It was assumed that import substitution in IT should concern not only the public sector, but also ordinary users. However, the quality of the first versions of Russian analogues of popular software made these products uncompetitive in the market. As a result, civil servants have to be the first to start using the Russian software. On July 26, 2016, the Government adopted a 3-year plan for the transition of government agencies in all state bodies to Russian software by gradually replacing imported products. Items from the register have advantage over other software in public procurements.

The process of software substitution imposes painful costs: for some items state bodies still have licenses for foreign software, and domestic analogues are very inconvenient to use. Sometimes public servants still use foreign software even after their agency bought the Russian programs during public procurements. Ultimately, by the end of 2018 Expert Council on software under the MoC announced its plans to exclude from its register any software products of foreign origin. These changes need to be made in favor of customers, which are already or prospectively under sanctions, so they can have the opportunity to work entirely on Russian technologies[29]. Such decision leads to high costs for software developers whose products based on foreign or open source (about 30% of total) are already in the register – they will have about 6 months to upgrade their products to meet the criteria.

Kill switches

The final part of securitization is establishment or reassertion of legal authority for network kill switches. A kill switch for RUnet still does not exist, at least officially. The story with kill switches started in 2014. The Government discourse differs from Mueller's understanding of domestic shutdowns but is actually more consistent with the alignment thesis. The Russian approach was (and still is) about an *external* kill switch for RUnet; it is conceived as a response to security and resilience threats to the Internet in Russia by "unfriendly" states. Upon the request of the President, the MoC conducted special cyber drills in summer 2014 the official aim of which was to "assess the security and stability of the national segment of the network, the degree of its connection with the global infrastructure"[30]. The drills were supposed to "assess potential vulnerabilities, determine the level of readiness for joint work of industry, operators and situational centers of the federal executive authorities in case of negative targeted impact." They involved the Ministry of Defense, the FSB, the Federal security service, Ministry of Internal Affairs, Rostelecom, the Coordination Center for TLD .RU/.РФ, the Internet Technical Center (which supports the DNS infrastructure for Russia and interaction with accredited registrars) and MSK-IX. Apparently, they tested the probability of a complete Internet shutdown orchestrated from outside the country. A year later the media reported about the contents of the report prepared by MoC after the cyber drills[31]. Among other things, the report claimed that: RUnet is vulnerable to external threats; there is a need for greater state regulation of the key organizations responsible for Internet operations in Russia; there is a need for creation of backup DNS servers and IP addresses. In 2015 and part of 2016 the Russian government actively criticized the Internet Corporation for Assigned Names and Numbers (ICANN), the California nonprofit responsible for

[28] Unified register of Russian software for electronic computing machines and databases https://reestr.minsvyaz.ru/reestr/

[29] Российский софт отключают от заграницы. Требования к отечественному ПО ужесточают в деталях. [Russian software is disconnected from abroad. Requirements for domestic software is tightened in the details]. (2018, December 12) Kommersant. Retrieved from: https://www.kommersant.ru/doc/3827670

[30] Ministry of Communications (2014, July 28). Press release: Ministry of Communications, FSB, and Ministry of Defense conducted cyber drills on protection of the Russian segment of the Internet. Retrieved from: https://digital.gov.ru/ru/events/31441/

[31] Министр связи предложит правительству взять рунет под контроль. [Minister of communications will propose to the government to take the RUnet under control]. (2015, March 26) Vedomosti. Retreived from: https://www.vedomosti.ru/technology/articles/2015/03/26/ministr-svyazi-predlozhit-gosudarstvu-vzyat-runet-pod-kontrol

the global governance of the DNS root and the allocation of IP addresses to regional registries. At this time ICANN was still in the throes of a stewardship transition process that ended the supervision of the U.S. Department of Commerce. Russia called for internationalization instead, preferring transition of ICANN functions to ITU.

In 2017 there was another cyber drills involving a broader list of government agencies and telecom operators[32]. This drills also tested the resilience of RUnet. In particular, MSK-IX tested the stability of the RUnet in case on one of the root DNS servers will delete information about the Russian top-level domain .RU. Sources close to MSK-IX noted that the results of the drills were almost the same as in 2014: "In Russia there is a system of duplicate root DNS which are able to maintain the normal operation of the RUnet for a long time in the case of some manipulation of the root DNS, but the security authorities are still concerned that the root DNS is managed by foreign organizations"[33]. In 2016 the MoC introduced the first bill that dealt with critical Internet infrastructure in Russia and aimed at protecting RUnet from external shutdown. The bill has stalled, especially because it overlapped with some provisions of FZ-187 on CII that was also under consideration that time. Thereby, the regulation of technical side of the RUnet remains an unresolved task. By the end of 2018 members of the Federation Council introduced a new bill on "national" Internet that can be viewed as an attempt to establish the legal kill switch for RUnet, though motivation is still the same: to be able to monitor the network and protect it from external threats and possible shutdowns. Both bills will be analyzed in the third part of the paper below.

However, there is a fresh case of a local shutdown of mobile Internet in Ingushetia Republic during the protests caused by the revision of the administrative border with neighboring Republic of Chechnya[34]. The shutdown happened at the end of September and into October. Access to 3G and 4G service was denied by the main telecom operators. In November Roskomnadzor replied to complaints that operators hadn't violated the laws because they acted in compliance with the requirement of law enforcement agencies[35].

The current state of affairs shows that there is no general kill switch for RUnet. The government admits that such radical measures will only harm the national economy and disrupt daily operations in various sectors. On the contrary, the government is concerned with external threats and shutdowns. That's why it works on the new laws to protect RUnet form aggression, though the methods are strange and seems to weaken the resilience of network because of interference into traffic routing and attempts to impose a centralized control point for monitoring and response. Despite this, there is (and probably there were cases in the past) an example of local mobile Internet shutdown conducted for the national security interests.

Territorialization of information flows

Territorialization of information flows covers external content filtering, data localization laws and geo-blocking. Russia has a comprehensive mix of all components; however, it doesn't resemble the famous Chinese Golden Shield. On the contrary, it was a gradual process of territorializing data and information, elaboration of laws regulating the blocking of websites with unlawful content and filtering of search engine results.

---

[32] Ministry of Communications. (2017, December 19). Press release: Ministry of communications held exercises to improve information security, integrity and stability of the unified telecommunication network of the Russian Federation. Retrieved from: https://digital.gov.ru/ru/events/37727/

[33] В Минсвязи проверили возможность перехвата SMS и отключения зоны .RU от интернета. [Ministry of Communications tested the possibility of intercepting SMS and disable the zone .RU from the Internet]. (2017, December 26) Roskomsvoboda. Retrieved from: https://roskomsvoboda.org/34751/

[34] Жители Ингушетии пожаловались в Роскомнадзор из-за отключения интернета во время митинга. [Residents of Ingushetia complained to Roskomnadzor because of the Internet disconnection during the rally]. (2018, October 24). Novaya Gazeta. Retrieved from: https://www.novayagazeta.ru/news/2018/10/24/146212-zhiteli-ingushetii-pozhalovalis-v-roskomnadzor-iz-za-otklyucheniya-interneta-vo-vremya-mitinga

[35] Ингушскую связь накрывали погонами. Отключение мобильного интернета во время митингов объяснили просьбой правоохранителей. [Ingush communication was covered with shoulder straps. Disabled mobile Internet during rallies was explained by the request of LEAs]. (2018, November 15). Kommersant. Retrieved from: https://www.kommersant.ru/doc/3799649

Content filtering

The first filtering practice started in 2012 after adoption of the law FZ-139 that established a special registry of domain names, URLs and network addresses of websites on the Internet containing information prohibited by law. The registry is run by Roskomnadzor, a federal supervising body in the field of communication, IT and mass communications. Prohibited information under the federal law FZ-139 includes child pornography, and information promoting drugs and suicide. Later, federal law FZ-398 added calls for mass riots, extremist activities, and participation in mass public events that violate the established procedure as a basis for blocking by the decision of the General Procuracy. Finally, FZ-187, called the Anti-piracy Act, allows for blocking sites containing unlicensed content, at the request of the rights owner. Web resources are added to the registry either after the court decision or several federal executive agencies may request Roskomnadzor to block web resources before the court decision if it contains unlawful information defined by the laws mentioned above.

According to these 2012 rules, when a site with prohibited information is found, Roskomnadzor must determine the hosting provider for this site and send the provider a notification about the need to remove the prohibited information. If the site owner or hosting provider does not delete the information within three days, the site is entered in the registry. The registry must be updated daily at 9:00 and 21:00 Moscow time. The network operator is obliged to restrict access to the sites from the registry within 24 hours from the date of update. Interestingly, Internet providers are free to decide how technically they will execute the decisions of Roskomnadzor for blocking and filtering. But there was a problem to supervise the due execution and punishment of operators who continued to provide access to the blocked resources.

In 2015 Roskomnadzor started to elaborate a special system called "Revizor" to check the operator's compliance to block the banned Internet resources[36]. This is hardware and software complex, which automatically checks whether an operator blocks sites from the register of prohibited sites and if not, it is qualified as administrative violation and can lead to a fine for operator. By 2017 the system covered 95% of all operators.

The national program "Digital economy" signed by the Prime Minister Medvedev in summer 2017 contains a provision to prototype a national system of Internet traffic filtering for children using information resources by 2019[37]. The League of Safe Internet (a Government NGO organized in 2011 to lobby for Internet censorship for the sake of child protection) was one of the main advocates of this system. Its head, Denis Davydov, shared the two possible options of its realization in the program: traffic filtering can be made only in educational institutions, or it can be spread to all users of RUnet[38]. In other words, this is introduction of "white lists" for the safety of children. He said that "the system could work as follows – citizens will be able to visit sites from the "white list", and if they need to get access to unfiltered content, they will to write an application to the Internet provider or remove the corresponding" tick " in their personal account." The League of Safe Internet has its own "whitelist" of sites, which contains more than 1 million resources. It also developed two filtration systems. The first is a browser add-on that shows only trusted sites from the white list. The second — hardware and software complex, which is installed on the operator's side. The League has already tested this system in several regions of Russia.

In summer 2018 the Russian lawmakers passed a law that imposes fines for the operators of the search engines if they refuse to connect to the federal state information system containing a list of prohibited Internet resources in order to

---

[36] Сетевой «Ревизор»: как работает система контроля за запрещенным контентом. [Network "Revizor": how works the system of control over the prohibited content]. (2017, September 07). RBC. Retrieved from: https://www.rbc.ru/technology_and_media/07/09/2017/59b00e269a79475c24ccf090

[37] National program "Digital Economy of the Russian Federation". (2017, July). The Russian Government. Retrieved from: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

[38] В России появится национальная система фильтрации интернета. Для россиян подготовят «белые списки» доверенных сайтов. [Russia will have a national Internet filtering system. For Russians will be prepared "white lists" of trusted sites]. (2017, August 02). Izvestiya. Retrieved from: https://iz.ru/627080/natcionalnaia-sistema-filtratcii-internet-trafika-poiavitsia-v-rossii

automatically filter search results[39]. In October it came into force and Roskomnadzor sent the requirement to connect to the system to Google, Yandex, Sputnik, and Mail.Ru. According to Roskomnadzor, by the end of October, these operators, excluding Google, made a connection to the system and comply with the requirements of the legislation. In December 2018 Roskomnadzor imposed a 500 thousand ruble fine on Google for noncompliance[40]. The company paid the fine a month later[41], but Roskomnadzor said it is considering the option to change the law and add the possibility to ban the search engine in case of noncompliance. Recently, Google began to remove from the search results links to sites from the Roskomnadzor blacklist.[42] Despite the search engine hasn't connected to the federal state information system to perform the filtering in automatic way, Google employees have started to clean the search results from prohibited information manually. The decision to exclude links from search results is made by people after analyzing the reasons for removal, and not a robot, as in Russian search engines. Nevertheless, by the time of the writing, there is no official acknowledgement form the Google of such a practice. Instead, there is an opinion that Google benefits from its silence – neither deny nor admit – because it lets Roskmnadzor to speak that it successfully made the last search engine giant to start complying with the law, and at the same time Goggle avoids reputational risks for officially participating in internet censorship.[43]

Data localization

Localization of personal data storage and processing (FZ-242) came into force in 2016 and the first victim became LinkedIn. The service is blocked in Russia due to its refusal to transfer the servers containing personal data of the Russian citizens to Russian territory[44]. The Law requires all companies that store and process the personal data of the Russian citizens, including foreign ones, to carry out their activities using databases located on the territory of Russia (storage and hosting facilities). If a foreign entity has already stored a database abroad, it should transfer it to Russia. The major giants like Microsoft, Samsung, Lenovo, Aliexpress, Ebay, PayPal, Uber, Booking.com instead of physically locating their databases started to use special cloud services to process personal data and waived the legal responsibility for complying with FZ-242. Leading social networks like Facebook and Twitter were in the process of negotiating the compliance with the law until the end of 2018. Roskomnadzor asked the companies to provide information about compliance with the data localization law. However, neither of the two succeed to provide a consistent report that describe how they comply or plan to comply with the law in future. As a result, Roscomnadzor started civil proceedings against Facebook and Twitter because they violated the law by failing to provide information about compliance.[45] According to FZ-242 companies who did not tell about the storage of personal data, face liability in a form of a fine under the article on the failure to provide information to state bodies. Roskomnadzor also has the right to block violators of data localization law as he did with LinkedIn.

---

[39] Federal law dated 06.27.2018. №155-FZ Retrieved from: http://publication.pravo.gov.ru/Document/View/0001201806270048?index=0&rangeSize=1

[40] Роскомнадзор оштрафовал Google и пообещал проверить Twitter и Facebook. [Roskomnadzor fined Google and promised to check Twitter and Facebook]. (2018, December 11). RBC. Retrieved from: https://www.rbc.ru/rbcfreenews/5c0f839d9a79478947d36454?from=materials_on_subject

[41] Google оплатил выписанный Роскомнадзором штраф 500 тысяч рублей. [Google paid a 500 thousand rubles fine issued by Roskomnadzor]. (2019, February 01), Kommersant. Retrieved from: https://www.kommersant.ru/doc/3869198

[42] Google начал удалять из результатов поиска ссылки на сайты, запрещенные в России. [Google began to remove links to sites prohibited in Russia from the search results]. (2019, February 06). Vedomosti. Retrieved from: https://www.vedomosti.ru/technology/articles/2019/02/06/793499-google

[43] Комментарий: Google начал цензурировать поисковую выдачу в России? [Commentary: has Google started censoring search results in Russia?] (2019, February 8). Deutsche Welle. Retrieved from: https://www.dw.com/ru/комментарий-google-начал-цензурировать-поисковую-выдачу-в-россии/a-47427466

[44] В России заблокировали LinkedIn. [Russia blocked LinkedIn]. (2016, November 17) Lenta.Ru. retrieved from: https://lenta.ru/news/2016/11/17/linkedin_block/

[45] Russia opens civil proceedings against Facebook and Twitter. (2019, January 21) CNBC. Retrieved from: https://www.cnbc.com/2019/01/21/russia-reportedly-opens-civil-proceedings-against-facebook-twitter.html

Alignment of critical Internet resources

The last and most intriguing method Mueller mentioned is to partition the global domain name and IP address spaces along national lines to provide nation-states with greater leverage over the governance of the Internet in their territory. Since 2016 in the Russian public discourse appeared ideas about independent national segment of Internet that works by duplicating DNS and numbering resources. The overall idea is to protect RUnet from external shutdown by hostile actors (implying the United States), as mentioned in the first section about Internet kill switches.

Going back to October 2014, there was a meeting of the Security Council that also discussed the outcomes of the first cyber drills mentioned above; and MoC got a request to address the challenges for the RUnet. This can explain the appearance of the bill introduced first time by MoC in November 2016 that described the basic elements of the critical infrastructure of the Internet in Russia and their regulation[46]. In 2016 and 2017, the MoC introduced several versions of a bill to amend the existing law on communications by adding definitions of the critical infrastructure of the Internet and its basic elements. These include Internet exchange points (IXPs), the national top-level domain registries, IP addresses and AS numbers. Also, the bill proposed to create the State Information System aimed to ensure the integrity, stability and security of the Russian national segment of the Internet, called "GIS Svyaz". The GIS Svyaz must include information about:

- Traffic exchange points, including telecom operators and organizers of information distribution
- Network addresses and information on individuals who own these network addresses
- Numbers of autonomous systems of the Internet, and also data on persons/entities to whom such identifiers are provided, and date of their providing
- Routing policies for Internet packets

Initially, telecom operators were merely advised to use GIS Svyaz. The draft dated August 2017, however, toughened the regulation and required them to use GIS Svyaz exclusively in their work and connect to the approved traffic exchange points. Also, the bill restricted foreign ownership of traffic exchange points. In other words, creation of GIS Svyaz partly duplicates the database of RIPE NCC, the regional Internet address registry for European and some Middle Eastern providers. The industry, and the key telecom operators strongly criticized the bill.[47] It got stuck because of the budgetary issues, too. According to different estimates, the creation of GIS Svyaz could cost more than 1 billion rubles. The last news on the bill was in January 2018, stating that MoC revised the bill and took into account all the objections by the telecom industry.[48] Anyway, the updated version wasn't published and was never submitted to State Duma. In contrast, by the end of 2018 a brand-new bill was introduced to the State Duma.[49]

The bill develops new rules and regulations for all major organizations responsible for Internet functioning in Russia. It requires network operators, to route the traffic through the exchange points listed in the special national registry and according to the rules defined by Roskomnadzor. In cases of "threats to the integrity, stability and security of the

---

[46] Draft law "On modification of the Federal law "On communication" and the Federal law " On information, information technologies for information protection". (2016). Retrieved from: https://regulation.gov.ru/projects#departments=31&okveds=33&StartDate=null&search=Интернет&npa=71277

[47] Expert Council under the Russian Government. (2016, November 21). Opinion of the working group on communications and IT. Retrieved from: https://open.gov.ru/upload/iblock/b30/b30cd6c520580c9c5f445cf8a5a9b5a8.pdf

[48] 23.01.2018
Минкомсвязь переработала поправки о пропуске трафика в сетях связи. [Ministry of Communications has worked on amendments for the routing of traffic in communication networks]. (2018, January 23) Rossiskaya Gazeta. Retrieved from: https://rg.ru/2018/01/23/minkomsviaz-pererabotala-popravki-o-propuske-trafika-v-setiah-sviazi.html

[49] The Bill № 608767-7 "On amendments to some legal acts of the Russian Federation". (2018, December). The State Duma. Retrieved from: http://sozd.duma.gov.ru/bill/608767-7
See more: Stadnik, I. (2018, December 23). Russia tries to double down on a "national" Internet. *Internet Governance Project* (blog). Retrieved from: https://www.internetgovernance.org/2018/12/23/russia-tries-to-double-down-on-a-national-internet/

Russian segment of the Internet," Roskomnadzor will "centrally manage the public communications network." The bill establishes a national Domain Name System: "In order to ensure the sustainable functioning of the Internet, a national system for obtaining information about domain names (or network addresses) is being created as a set of interrelated software and hardware designed to store and obtain information about network addresses in relation to domain names, including those included in the Russian national domain zone, as well as authorization for domain name resolution". Finally, the bill prescribes all network operators to install special technical means to counter threats in their networks. Interestingly, these means will serve a dual purpose: to protect Runet from external threats (which are not detailed in the bill) and to block the resources from the blacklist maintained by Roskomnadzor that is currently a responsibility of operators to execute content filtering with their own equipment and methods. The bill has very uncertain provisions about how all these technical novelties will become real. Anyway, the bill passed the preliminary reading in State Duma and despite it lacks a solid technical and financial explanations for its implementation. The bill got the support from the Government with reservations that it has to be revised, taking into account the comments made for the first reading scheduled in February 2019.[50] In particular, this applies to the list of threats to the integrity and stability of RUnet that legislators must specify.

Both legislative episodes show a strong commitment of the Russian government to keep finding ways to make RUnet independent form the system created around ICANN as far as possible.

Conclusions

The political intention to align the Internet with the national borders of Russia is proved to be right. Almost each method of alignment suggested by Mueller can be found in Russian developments over the past decade.

Firstly, securitization of cyber security has been finished with the publication of the updated Doctrine on information security. Despite that, internal militarization of cyberspace was denied until the last year. It can be partially explained by the "peaceful use of ICT" rhetoric translated by Russia on international level: the need to prevent international cyberspace from militarization that can cause conflicts, and elaboration of rules for responsible behavior of states. However, the revelation happened in 2017 when the Minister of defense talked publicly the new information operations troops. Probably it was a question of prestige - cyber command is a modern must-have for the superpower. Or, it has become unnecessary to hide the existence of such a kind of forces.

Secondly, deployment of the GOSSOPKA system, operated by FSB, is a good example of nationalization and centralization of threat intelligence reporting. Basically, the system accumulates all information about various computer incidents on government and state corporations' networks, develops measures to counter cyberattacks, and elaborate recommendations to eliminate or reduce the consequences associated with the actions of cybercriminals. Creation of the National Coordination Center for Computer Incidents that absorbed the functions of the GOV-CERT just adds to the necessary institutional landscape. Russia has several private and public CERTs for specific sectors. Private initiatives seem to be more active, but NCCCI still has to prove its efficiency. Also, we can witness in future a struggle for market between corporations with state participation to have the biggest share in providing ready solutions for CII organizations that can't afford creation of GOSSOPKA centers themselves.

Thirdly, there is no complete reliance on national technologies and standards regarding IT and security, because Russia started to reduce its reliance on imported software and hardware only after the sanctions went into effect. Creation of a special register for the Russian software doesn't help too much with transition of the government to the national technologies, not to speak of the whole population. There is a long way for the Russian hard and software developers to become competitive with foreign products. Notably, no one is talking about national standards for Internet protocols, because it is inexpedient to refuse from benefits of using the global network.

As for a kill switch for the RUnet, there has been several attempts to legalize a kill switch for Internet in Russia since

[50] Official opinion of the Government of the Russian Federation on the bill № 608767-7, (2019, February 01). The State Duma. Retrieved from: http://sozd.duma.gov.ru/bill/608767-7

2014, but this option was implicit. Industry and human rights activists paid attention to this covert aim, however, the official motivation of authorities to adopt laws on RUnet was explained by the need to protect RUnet from possible external shutdowns inspired by hostile states. Yet, lawmakers and lobbyists don't take into consideration that centralization of Internet governance in a technical way leads to a more vulnerable situation when there is only one command and control center for the whole RUnet. So, two recent bills try to define the critical internet infrastructure and align it to the national borders. They attempt to duplicate the DNS and make it national, duplicate the IP and ASN databases, intrude into traffic routing policies to minimize the crossing of state borders and block unwanted traffic from foreign sources. The time showed that adoption of such bills is not so easy, keeping in mind their ill-formulated provisions and weak technical justification. However, we must pay attention to the doubling effort of the last bill introduced recently, that signals about strong political will to finish the legal framework for government-led regulation of Internet operation in Russia. Finally, even either of the bills is adopted, it won't mean that their implementation starts immediately. The law on CII, and other examples concerning the telecom industry show that it takes an additional 2-3 years for execution, because such laws are mostly frameworks and require additional orders and decrees that clarify procedures, set responsibilities of federal executive bodies in order to be implemented. If eventually legislators find a technical solution to make RUnet really sovereign and independent but still connected to the global network, it will create a dangerous precedent for Internet fragmentation.

Finally, territorialization of information flows continues in a full swing. From year to year we see a trend to a tougher regulation in connection to traffic filtering and blocking of websites in Russia. The means to execute filtering and check compliance to laws are multiplying and resemble the Chinese great firewall more and more. In the meantime, Roskomnadzor, supervising body in the field of communications, still has no ability to compel foreign Internet services to execute full-fledged content filtering, or data localization, except issuing fines and threating with total blocking on the Russian territory.

For the Russian government it is very tempting to align the Internet with its sovereign authority. But it is not a one-year story. Some parts are done, but the most important and technical are still under consideration. And hopefully, the voice of wisdom will prevail over the political will to do it.