TECHNOLOGY AND SECURITY POLICY

Moscow's Digital Offensive – Building Sovereignty in Cyberspace

Carolina Vendil Pallin and Mattias Hjelm

Summary

- Russia is pursuing a long-term policy that aims to build its cyber sovereignty.
- The law on a "sovereign internet" appeared in 2019, but the concrete plans were evident in 2014 and present among the security services as long-term aspirations even further back.
- The goals are strategic – to escape what Russia sees as U.S. dominance in the cyber sphere and to increase control over information flows within the "Russian segment of the internet".
- Russia has built up a capability to perform cyber operations over at least two decades, from relying on "mercenary" hackers and crude distributed denial of service attacks (DDoS) to employing its own specialists and utilising advanced malware.
- Russia's current bid for an international treaty on information security goes back to the late 1990s.
- Moscow aims to achieve a high degree of coordination for this policy across different government ministries, agencies and services as well as with parliament and the leading Russian internet companies.

Building sovereignty in cyberspace [1]

What the West perceives as a Russian digital offensive stems to a considerable degree from a deep-seated sense of insecurity in Moscow – both of being under attack and of lagging behind technologically. Russia's intelligence and security community, moreover, has been keenly aware of how the global internet infrastructure setup affects the intelligence balance of power. These concerns intensified after the Snowden leak exposed how advantageous the U.S. and its allies' position is when it comes to passive intelligence-gathering over the internet.[2]

From these basic premises for Russia's cyber strategy follows the conclusion that *the policy it pursues is long-term, coordinated and, therefore, difficult to influence.*

Information is potentially an existential security threat in what Moscow designates as "a Russian segment of the internet". This view dominated early within the military and security community inside Russia, but for many years the digital sphere in Russia remained relatively free. The Russian political leadership initially brought national mass media, especially television, under control, but largely neglected the internet as a catalyst for political protest and unrest. This changed with the Arab Spring and the demonstrations in Moscow in 2011–2012. From that point, the Russian government directed its attention towards not just strengthening but also enforcing legislation and other measures that would also allow it to control information on the internet. This, however, proved a far from easy task. Absent the possibility of controlling the global internet, the option left for Russian authorities was always to hammer out something approaching a territorially defined information space and claim Russian sovereignty. Russia has also developed its capability to conduct cyber operations and step by step built a coalition of likeminded countries around its bid on how to frame international information security.

Russia does not have a cyber portfolio

Anyone looking for a distinct cyber strategy in Russian official security documents will be disappointed. The upper house of parliament, the Federation Council, drafted a cyber strategy in 2011, but the Federal Security Service (FSB) opposed this initiative. No separate Russian cyber strategy was to exist, only an information security doctrine combining technical and psychological aspects. Consequently, there is no separate government authority dealing exclusively with cyber affairs, no military cyber domain and no cyber portfolio when the Russian government is involved in international talks: instead, there is an information space, an information security doctrine and a Russian position on international information security.

Cybersecurity and cyber operations are an integrated part of the larger Russian concepts of information security and information operations.[3] This is an important caveat when one embarks on any attempt to analyse Russia's position on cyber. Often the debate becomes blurred and at times even misleading. When Russia talks of international information security, it incorporates the need to protect

FOI Memo: 7521
Project no: B12527
Approved by: Anders Norén

April 2021

its own information space not only against hacker attacks but also against content that is illegal in Russia. This illegal content can be child pornography or terrorist propaganda, but it can also be political opposition websites or blacklisted reporting by human rights activists. Russia internationally promotes this position with vigour and consistency, as do China and a number of other authoritarian countries that have similar policy goals and cooperate with Russia within, for example, the United Nations (see below).

In practice, however, Russia determines that it also needs to divide the concept of information security into technical information security and psychological information security. This is certainly the case when Russia designs measures to develop its own technology as well as processes for countering information and communications technology (ICT) threats. For example, there is an ambitious and prioritised national project on "Digital Economy" and within it a sub-programme on "Digital Security", as well as an elaborate system for detecting, countering and eliminating ICT threats. It is also clear that Russia has developed its capability to engage in cyber operations (see below).

In Russia's Information Security Doctrine, the prioritised goals can be divided into four main areas:

1. to protect critical information infrastructure;
2. to reduce the country's dependence on imported technologies, including hardware, electronic components and software;
3. to control content in what Russia sees as its national segment of the internet;
4. to promote its view of information security internationally.

For obvious reasons, the doctrine only lists threats to Russian information security and the measures planned to counter these. However, there is ample evidence that Russia also engages in offensive measures. The most obvious example is the increased incidence of cyber operations attributed to Russia, but Russia also has a plan on how to shape the global digital landscape more to its taste and then, not least, in its immediate neighbourhood. And, again, the focus is on shaping the information space as a whole to Russia's advantage. Digital measures are only a part of this overall goal.

Russia's sovereign internet

Russia's illegal annexation of Crimea resulted in condemnation and sanctions from the U.S. and the European Union. With the downing of the Malaysian airliner MH17 over Ukraine, a new round of sanctions increased concerns in Moscow about Russia's dependence on the global internet infrastructure. There had been no threats or even hints about cutting Russia off from this infrastructure. Inside Russia's political system, however, forces that had been championing measures to create a so-called "internet kill switch", since the late 1990s, and the drafting of the 2000 Information Security Doctrine,[4] seized on the opportunity to further this agenda. At a national Security Council meeting on 1 October 2014, Vladimir Putin outlined many of the main themes that would dominate the 2016 Information Security Doctrine. He especially mentioned the need for Russia to build a 'sovereign internet' that, if necessary, would be independent of the global internet infrastructure.

This proved easier said than done. Only in 2019 did draft legislation appear. At that point, the idea had become both to create a kill switch and to introduce additional means for sifting and blocking unwanted content traffic on Russian territory. This signified that all internet providers on Russian territory would be obligated to install equipment by 2021 to block what the government defines as illegal information from reaching internet users. The law also introduces stricter government control over internet infrastructure – most importantly concerning internet exchange points, cables that cross its national borders and routing rules. The government agency for supervising communication and media, Roskomnadzor, will play a key role in supervising which routes internet traffic should take inside Russia. A centre under Roskomnadzor will take over and direct traffic on Russian territory in case of an emergency or threat. In addition to this, Russia intends to make sure it has the necessary infrastructure for its internet to function even when operators are unable or unwilling to connect to the global internet infrastructure; this would be a Russian 'domain name system', with DNS servers on Russian soil. Government authorities are also obliged to conduct cyber exercises each year. [5]

Somewhat ironically, Russia's broad definition of information security and its ambition to control content has led it to focus on the technical aspects, the cyber aspects. The law on a sovereign internet was not a sudden whim but rather a step further in Russia's long-term strategy to increase control and surveillance. This now takes place through everything from registries of forbidden websites, so-called blacklists, and laws making it mandatory to store user data on Russian soil, to demands on companies such

as Yandex to hand over encryption keys to Russia's security services.[6]

Encryption has been a continuing concern for Russian authorities wanting to control information flows inside the country. In September 2020, Russia's Ministry for Digital Development suggested legislation that would ban encryption that prevents identification of webpages.[7] One of Russia's main concerns was probably its previous inability to block websites efficiently. Its experience from trying to block the Telegram messaging service in 2018 no doubt contributed to this. Roskomnadzor, Russia's government agency for supervising communication, ended up preventing access to millions of webpages, as Telegram's founder, Pavel Durov, hid the messaging service on IP addresses in Amazon Web Services and Google Cloud. In the end, Telegram continued to function relatively well, while the blocking activity crippled other internet services.[8] To add insult to injury, the number of Telegram users in Russia in 2018 increased, rather than the opposite.

New digital solutions, thus, often thwart Russia's control measures. For example, protocols that hide which DNS an internet user directs a request to have become increasingly normal; DNS over HTTPS, or DNS over TLS, encrypts this information. One of Russia's four planned cyber exercises during 2020 aimed to examine whether it was possible to block traffic that used these protocols. In the end, no exercise took place, because of the pandemic.[9]

Russian cyber operations – implausible deniability

Russia denies any involvement in cyber operations abroad. Its official response to all allegations of Russian hacking is that Russia does not meddle in the internal affairs of other countries. The accompanying text to the draft legislation on a sovereign internet even maintained that a reason for its necessity was the U.S. National Cyber Strategy from 2018, which accuses Russia of reckless cyberattacks. 'Under these conditions defence measures are necessary in order to ensure the long-term and reliable work of the Internet in Russia.'[10]

Attribution of cyber operations is complex and seldom absolute but rather a question of degree and political considerations.[11] This is one of the reasons why IT-security reports often make the attribution in terms of, for example, 'a Russia-affiliated attacker' or 'a Russia-based cyber actor'. Nevertheless, both target countries and IT-security firms have now attributed cyberattacks either to Russia, or referred to them as "Russia-sponsored", especially after the 2016 U.S. election. This is the result of extensive cyber forensics efforts complemented by intelligence sources. Also, Washington took the lead when it decided to adopt a policy of going public with its capacity to track down who is behind a cyber operation and to "name and shame" the countries responsible, following an increase in Chinese, North Korean and Russian attacks. In July 2020, the European Union sanctioned Russian military officers for cyberattacks for the first time.[12]

Experts believe Russia to be among the top five countries when it comes to cyber operation capabilities.[13] Russian intelligence services' first encounter with information gathered through hacking probably dates back to the Soviet era, when German hackers contacted the KGB to sell their exploits.[14] In the Russian Information Security Doctrine from 2000, Russia still called for a ban on the use of ICT for military means. Since then, a number of cyber operations have been attributed either to Russia, or Russia-affiliated – from the distributed denial-of-service (DDos) attacks against Estonia in connection with the moving of a Soviet war memorial, the Bronze Soldier, in 2007, to the hacking of about 250 American federal agencies and businesses through an update of SolarWinds' software, in 2020.

The attacks have become more sophisticated over time. Most likely, the Russian security and intelligences services began by relying on the enlistment of external hackers and purchased ready-to-use spyware. In time, they also went on to build their own dedicated units for cyber operations and pursued a policy of recruiting bright young IT specialists at hacker competitions, for example. In some cases, the hackers behind the cyberattacks are probably only affiliated with Russian authorities. However, there is an increasing amount of evidence that there are regular intelligence units, which conduct cyber operations. For example, the U.S. Mueller Report firmly attributed the attack against the Democratic Party in 2014 to the Military Intelligence Directorate (GRU), down to identifying the specific GRU unit.[15]

Russia is also the victim of cyberattacks and convinced that it is the target of coordinated and continuous information warfare. Its build-up of cyber warfare capabilities has taken place over decades in part as a response to this threat perception. There is some evidence of infighting between different branches of the intelligence and security services and there is not, of course, any published cyber

operations strategy. Russia's overall track record when it comes to cyber operations, however, is evidence that the offensive component of Russian cyber strategy is long-term as well as coordinated at the strategic level.

Russian Diplomacy and Cyber

Russia's position on international regulation of cyberspace is also far from new. Russia proposed a resolution in the United Nations as early as 1998.[16] The General Assembly adopted a modified version of that resolution the following year.[17] Russia's initiative became the starting point for a UN dialogue process on potential norms and confidence-building mechanisms in cyberspace. From the very beginning, there was a significant difference in the approach to information security between Russia and the Shanghai Cooperation Organization (SCO) countries on one side and Western liberal democracies on the other.[18] Despite conceptual disagreements, the dialogue led to the creation of a UN Group of Governmental Experts (UN GGE), which subsequently turned into the main international vehicle for discussions on rules of behaviour for states in cyberspace and resulting in a number of consensus reports. However, the apparent failure of the UN GGE in 2016–2017 again highlighted the irreconcilable differences between the two camps. The stalemate probably made Russia explore other ways of pushing forward its agenda, even as the planning for the 2019–2021 UN GGE was underway.

Since 2014, Russia has signed over 30 ICT deals bilaterally and with regional organisations.[19] This is consistent with the objective stated in Russia's 2016 Information Security Doctrine to expand Russia's international cooperation. Russia, together with China and Central Asian states that agreed with Russia's policy suggestions, also submitted an SCO International Code of Conduct for Information Security to the UN General Assembly in 2011 and again in revised form in 2015.[20] The code is in many ways a global application of Russia's (and China's) aspirations for state sovereignty and territoriality in the digital space. Among Western countries, the concern is that this could become a way of legitimising censorship and state control over the internet. Russia's longstanding objectives are national security and regime stability and its endeavours within the international information security framework demonstrate a remarkable continuity in this regard.

In 2018, the UN General Assembly adopted two new resolutions in the field of cybersecurity. Russia initiated both of these. The first resolution created an openended working group (OEWG) to run parallel with the already existing UN GGE. The resolution calls for 'rules, norms and principles' of responsible state behaviour in cyberspace.(21) Unlike the GGE's twenty-five handpicked member states, the OEWG is open to all interested UN member states. Russia aims to position itself as a defender of the rules-based international order as well as committed to multilateral solutions to international challenges. In one of its statements on the draft final document, Russia even referred to the OEWG as a 'cyber General Assembly'.(22) The OEWG reached a compromise in a report in March 2021. The report endorsed the language and recommendations of the GGE process, but the human rights element was weaker. In addition, the concluding paragraph mentioned that proposals had been put forward on 'additional legally binding obligations'.(23)

Russia launched a second resolution, adopted in the Third Committee of the General Assembly, about cybercrime prevention as an alternative to the Budapest Convention. Russia argues that the document is of a technical nature and intended to help combat illegal activity on the internet.[21] However, the resolution's wording is vague and could just as easily legitimise authoritarian surveillance and limit freedom of expression on the internet. Among the countries that sponsored Russia's resolution on cybercrime are Belarus, China, Iran, North Korea, Venezuela and Syria.[22]

These two resolutions constituted a success in Moscow's long-term efforts to adjust the international normative environment more to its preferences. Russia promotes an alternative to the Western vision of global internet governance, where the core prerequisite is state sovereignty.[23] Together with countries like China, it seeks to constrain what it sees as the prevailing U.S. hegemony in cyberspace. Ideally, it would like to transfer power from institutions such as ICANN (Internet Corporation for Assigned Names and Numbers) to the UN level, where states would negotiate and decide on global internet governance.

Both resolutions are the result of a painstaking process, where Russia has been building alliances with like-minded countries. A strategy of using regional organisations – not least the ones where Russia had a leading role – was evident by 2011 and formalised in official documents from at least 2013.[24] Russia's measures for internet control are attractive

to countries with hybrid and authoritarian regimes, including those within the Commonwealth of Independent States (CIS).[25] In line with this, the meetings of the Collective Security Treaty Organization (CSTO) shifted focus to cyber-related threats after the Arab Spring.[26] Inside BRICS, consisting of Brazil, Russia, India, China and South Africa, Russia has pushed through agreements in the information security sphere.[27] The most comprehensive cooperation is arguably within the framework of the SCO.[28]

Russia has also made a bid to contribute to international standards on encryption. The International Organization for Standardization (ISO) has already approved one standard developed by the FSB's Centre for Information Protection and Special Communications. Another proposed algorithm, however, is pending approval from ISO, after experts warned that it possibly contained a flaw in one of its components that could undermine the security of encrypted material. A debate quickly ensued as to whether the flaw was intentional or not. Russia denied such allegations.[29]

In parallel, Russia has gradually strengthened its bureaucracy to coordinate efforts on the international level. When Russia drafted its letter proposing a cyber arms control agreement in 1998, these questions were probably within the remit of the military and security elites.[30] Russia adopted its first Information Security Doctrine in 2000. An important person behind it was the first deputy secretary of the Russian Security Council, Vladislav Sherstiuk, who came from the Soviet security service (KGB). In 2003, Sherstiuk went on to create the Institute of Information Security, tasked with promoting Russia's vision for a future international treaty on information security.

Russian diplomat Andrei Krutskikh chaired both the first and the second GGE in the UN General Assembly. In 2014, Russia appointed Ambassador Krutskikh its Special Representative for International Cooperation on Information Security. From January 2020, he is also the head of a new department inside the Russian Ministry of Foreign Affairs, the Department of International Information Security. There is, moreover, a separate directorate for information technologies, created in 2012, inside the Presidential Administration. This directorate was reorganised in 2018 and is probably one of the main vehicles behind the 2019 legislation on a sovereign internet.[31]

It is too early to say exactly how these organisational changes will influence Russia's activity in the sphere of international information security. The fact that Russia has established a new MFA department indicates that these issues have moved up on the Kremlin's agenda. Krutskikh is likely to have the support of stronger in-house expertise when defending Russia's position – adding to his own long-term experience on these matters.[32]

Russian cyber dilemmas

Russia's policy may be long-term and coordinated, but this does not mean that there are no challenges ahead. Sovereignty is something of a domestic policy mantra, but hammering out just what it means to be sovereign on the internet is quite another matter than simply stating it. One dilemma that Russia faces when it comes to its legislation on a sovereign internet is that technology tends to develop faster than legislation. In other words, additional legislative and other initiatives will probably have to follow on after the law on a sovereign internet; and perhaps often one step behind technology developments, as is the case with new encryption solutions.

Russia's capacity to conduct cyber operations has increased, while its policy of denial has remained the same. This might have served Russia well to start with, but there could be a problem of "diminishing returns", as the targets of cyberattacks come to understand what is going on and start to devise a unified and calibrated response.[33] Russia is already facing a tougher environment for conducting its cyber operations and policy of denial; the U.S. response to Putin's overture on restarting bilateral talks on information security in September 2020 bears testimony to this, irrespective of whether Russia's proposal was grounded in a genuine wish to start talks or not. A leading Russian IT security firm, Kaspersky Lab, has seen its market in the U.S. diminish after allegations that it had close links to the FSB, and the Russian encryption algorithm will probably have to undergo rigorous tests and examinations before, if at all, getting a stamp of approval.

A number of cyberattacks have demonstrated how potent they are in combination with psychological operations that use the information the hackers obtained. This has made other states than Russia sensitive to how intimately connected cyber issues are with psychological information attacks. Cyber operations are also in the West increasingly becoming a way of referring to something broader than just attacks against ICT systems. The agenda has shifted since it became clear how vulnerable many democracies are to cyber-based information operations. However, although the international environment may

have become more conducive to Russia's diplomatic cyber agenda, Russia has at the same time undermined its position as a reliable partner with which to negotiate and close agreements. Few Western countries will be interested in reaching agreements that cannot be verified and enforced. Russia's activity in this field has underlined the importance of understanding what Russia brings to the table and why.

Russia's main dilemma in the future, however, will be to stay in the technology race. Russia remains dependent on imports when it comes to certain electronic components, ICT equipment, programmes and operating systems. It is unlikely that Russia will overcome this dependence any time soon, or completely. So far, Russia has been using both Western and Chinese technology, but there will continue to be a tendency for Moscow to become more dependent on China as technological competition hardens, trade wars intensify and international tensions increase. In the end, Russia might not even actively choose China. Forces that it will be unable to influence will have made the choice for Moscow and sovereignty will remain a chimera. ■

Carolina Vendil Pallin is Deputy Research Director at FOI's Russia and Eurasia Studies Programme, www.foi.se/russia. *Mattias Hjelm* did an internship at FOI's Russia and Eurasia Studies Programme August 2020 – January 2021 before completing his MSc at the Swedish National Defence College.

Endnotes

1 The authors are grateful for comments from Keir Giles on an earlier draft of this paper. His suggestions led us to revise and develop some of the key points in the paper. He is not to blame in any way, however, for any remaining errors or transgressions. Thank you also to colleagues at FOI for helpful suggestions along the way.

2 Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Cambridge; Massachusetts, Harvard University Press, 2020.

3 Giles, Keir. *Handbook of Russian Information Warfare.* Fellowship Monograph, Research Division, NATO Defense College, no. 9 (November 2016). http://www.ndc.nato.int/news/news.php?icode=995. Accessed: 9 March 2020.

4 See Kukkola, Juha. *Digital Soviet Union: The Russian National Segment of the Internet as a Closed National Network Shaped by Strategic Cultural Ideas.* PhD Thesis. Helsinki, National Defence University, 2020: p. 153. https://www.doria.fi/handle/10024/177157. Accessed: 10 November 2020.

5 Federal law No. 90-FZ. 1 May 2020. https://rg.ru/2019/05/07/fz90-dok.html. Accessed: 20 November 2020.

6 Vendil Pallin, Carolina. 'Russian Information Security and Warfare'. In *Routledge Handbook of Russian Security*, Roger E. Kanet (ed.), 203–213. London: Routledge, 2019. See also, for example, Kolomychenko, Mariia. "FSB potrebovala kliuchi shifrovaniia perepiski polzovatelej u 'Yandeksa'". *RBK*. 4 June 2019. https://www.rbc.ru/technology_and_media/04/06/2019/5cf50e139a79474f8ab5494b. Accessed: 20 November 2020.

7 Draft law on the website of the Ministry for Digital Development, https://regulation.gov.ru/projects#npa=108513. Accessed: 22 December 2020. See also Kolomychenko, Mariia. 'Ministerstvo tsifrovogo razvitiia khochet zapretit sovremennye protokoly shifrovaniia v Runete. Bezuslovno, blogodaria etomu v Rossii budet proshche blokirovat saity.' *Meduza*. 21 September 2020. https://meduza.io/feature/2020/09/21/ministerstvo-tsifrovogo-razvitiya-hochet-zapretit-sovremennye-protokoly-shifrovaniya-v-runete-togda-roskomnadzoru-budet-prosche-blokirovat-sayty. Accessed> 22 December 2020.

8 More specifically, Russia wants to block different anonymising services, such as virtual private network (VPN) and the security protocol DNS over TLS (domain name system, DNS, over transport layer security, TLS), which increase privacy and security. One of Russia's planned exercises on cybersecurity for 2020 aimed to check whether it was possible to block encryption through DNS over TLS, and DNS over HTTPS. However, by December 2020, none of the planned exercises had taken place, officially because of the pandemics, but there were also signs that the necessary equipment was not installed. See, for example, Demurina, Gaiana. 'Minkomsviaz perenesla ucheniia po 'suverennomu Runetu' iz-za koronavirusa'. *RBK*. 20 March 2020. https://www.rbc.ru/technology_and_media/20/03/2020/5e7456be9a7947247c8bf391. Accessed: 22 December 2020.

9 Ministry for Digital Development, No. 839, annex with planned exercises available at https://digital.gov.ru/uploaded/files/grafik-uchenij-k-prikazu-839.pdf. Accessed 12 January 2021. See also, Demurina, Gayana. 'Minkomsviaz perenesla ucheniia po "suverennomu Runetu" iz-za koronavirusa'. *RBK*. 20 March 2020. https://www.rbc.ru/technology_and_media/20/03/2020/5e7456be9a7947247c8bf391. Accessed: 12 January 2021.

10 State Duma of the Russian Federation. Draft Law No. 608767-7. https://sozd.duma.gov.ru/bill/608767-7. Accessed: 9 November 2020.

11 See, for example, Rid, Thomas and Buchanan, Ben. 'Attributing Cyber Attacks.' *Journal of Strategic Studies,* Vol. 38, no. 1: 4–37; Nye, Joseph S. 'Deterrence and Dissuasion in Cyberspace.' *International Security,* Vol. 41, no. 3 (Winter 2016/17): 44–71. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266. Accessed: 2 May 2019.

12 Council Implementing Regulation (EU) 2020/1125. 30 July 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX-:32020R1125&from=EN. Accessed: 2 December 2020. See also Giles, Keir & Hartman, Kim. '"Silent Battle" Goes Loud: Entering a New Era of State-Avowed Cyber Conflict'. In T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (eds) *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn, NATO CCD COE Publications, 2019. file:///C:/Users/carven/Downloads/Silent_Battle_Goes_Loud_Entering_a_New.pdf. Accessed: 11 February 2021.

13 Jensen, Benjamin, Valeriano, Brandon and Maness Ryan. 'Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist'. *Journal of Strategic Studies.* Vol. 42, no. 2, 2019: 212–234, 214. See also *Kibervoiny 2017: balans sil v mire*, Zecurion Analytics, January 2017. http://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf. Accessed: 22 March 2018. See also Voo, Julia, Hermani, Irfan, Jones, Simon et al. *National Cyber Power Index 2020.* Belfer Center for Science and International Affairs. September 2020. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf. Accessed: 2 December 2020.

14 Stoll, Clifford. 2005. *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage.* New York, Doubleday, Kindleedition.

15 The U.S. Department of Justice. *Report on the Investigation Into Russian Interference In The 2016 Election.* Special Counsel Robert S. Mueller. Washington, D.C. March 2019. https://www.justice.gov/storage/report.pdf. Accessed: 14 January 2021. See also, Turovskii, Daniil. 2019. Vtorzhenie: Kratraia istoriia russkich khakoerov. Moscow: Individum.

16 General Assembly. *Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General.* (30 September 1998) A/C.1/53/3, available from https://undocs.org/A/C.1/53/3. Accessed: 22 January 2021. See also, Giles, Keir & Monaghan, Andrew. Legality in Cyberspace: An Adversary View. Strategic Studies Institute & U.S. Army War College Press, March 2014. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1314&context=monographs. Accessed: 20 January 2021. Kukkola, *Digital Soviet Union,* p. 155.

17 General Assembly Resolution 53/70, *Developments in the field of information and telecommunications in the context of international security.* (4 January 1999) A/RES/53/70, available from https://undocs.org/A/RES/53/70.

18 For a thorough examination of this, see Giles, Keir. 'Russia's Public Stance on Cyberspace Issues' in Czosseck, C., Ottis, R. & Ziolkowski, K. (eds). *4th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications, 2012: 63–75 and Giles, Keir & Hagestad, William III. 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in Podins, K., Stinissen, J. & Maybaum, M. (eds). *5th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE Publications 2013. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6568390 Accessed: 12 November 2018.

19 Bugayova, Nataliya. *Putin's Offset: The Kremlin's Geopolitical Adaptations since 2014.*Washington D.C: The Institute for the Study of War. 2020.

20 In 2011, China, Tajikistan and Uzbekistan were co-signers; in 2015, Kazakhstan and Kyrgyzstan had joined the initiative. See General Assembly documents: A/66/359. 14 September 2011. https://undocs.org/A/66/359 Accessed: 15 February 2021; A/69/723. 13 January 2015. https://undocs.org/A/69/723 Accessed: 15 February 2021.

21 The Polish Institute of International Affairs. *Russia on the Global Regulation of Cyberspace.* 18 December 2018. https://pism.pl/publications/Russia_on_the_Global_Regulation_of_Cyberspace Accessed: 17 November 2020.

22 General Assembly, *Countering the use of information and communication technologies for criminal purposes.* A/C.3/73/L.9/rev.1. 2 November 2018. https://undocs.org/A/C.3/73/L.9/Rev.1 Accessed: 15 February 2021.

23 General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Substantive Report*. (10 March 2021) A/AC.290/2021/CRP.2, available from https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

24 *Bases for the State Policy of the Russian Federation in the Area of International Information Security for the Period until 2020* [in Russian]. Adopted through Presidential Order No. Pr-1753. 24 June 2013. http://www.scrf.gov.ru/security/information/document114/ Accessed: 27 November 2020: §11. See also §11 and §15 in *Information Security Doctrine of the Russian Federation* [in Russian] approved by Decree of the President No. 646, 5 December 2016. http://www.scrf.gov.ru/security/information/document5/ Accessed: 17 November 2020.

25 Weber, Valentin. *The Worldwide Web of Chinese and Russian Information Controls.* Washington D.C: Open Technology Fund. 2019. https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf Accessed: 17 November 2020. See also Kurowska, Xymena. 'What does Russia Want in Cyber Diplomacy?' in *Governing Cyberspace,* Dennis Broeders & Bibi van der Berg (ed.). London: Rowman & Littlefield. 2020. 85-106: 95.

26 Nocetti, Julien. 'Contest and conquest: Russia and global internet governance'. *International Affairs*. Vol. 91, no. 1, 2015: 111-130. DOI: 10, 1111/1468-2346.12189. Accessed: 5 November 2020.

27 VII BRICS Summit: 2015 Ufa declaration. 9 July 2015. http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html. Accessed: 17 November 2020.

28 Kurowska 'What Does Russia Want in Cyberspace', 98.

29 Cox, Joseph. 'Experts Doubts Russian Claims That Cryptographic Flaw Was a Coincidence'. *VICE*. 8 May 2019. https://www.vice.com/en/article/43j3wm/experts-doubt-russian-encryption-standard-cryptography-backdoor-streebog-kuznyechik Accessed: 13 January 2021.

30 Kukkola, *Digital Soviet Union,* pp. 160ff, 202ff.

31 Novyj, Vladislav. 'Kurator rubilnika Runeta.' *Forbes.* 12 February 2020. https://www.forbes.ru/tehnologii/393021-kurator-rubilnika-runeta-chto-izvestnoo-kandidate-na-post-glavy-roskomnadzora. Accessed: 10 March 2020.

32 TASS. 'Novyy departament MID Rossii zaymetsya mezhdunarodnoy informatsionnoy bezopasnost'yu'. 29 December 2019. https://tass.ru/politika/7442537 Accessed: 7 January 2021.

33 Freedman, Lawrence. 2013. *Strategy: A History*. New York: Oxford University Press: 23.