Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet

Epifanova, Alena

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

German Council on Foreign Relations

No. 2
January 2020

DGAP ANALYSIS

Deciphering Russia's "Sovereign Internet Law"

Tightening Control and Accelerating the Splinternet

Alena Epifanova
is program officer at the Robert Bosch Center for Central and Eastern Europe, Russia, and Central Asia

KEY FACTS

In November 2019, Vladimir Putin's regime introduced new regulations that create a legal framework for centralized state management of the internet within Russia's borders. Although full implementation will be extremely difficult, this framework will likely lead to tighter state control over society and additional complications for domestic and foreign companies. The regulations are expected to accelerate the fragmentation of the global internet and to increase Russian reliance on Chinese technology.

- Germany and the EU should assess the risks and long-term implications of Russia's new internet legislation for European companies and civil society actors.
- EU institutions, particularly the European Commission with its geopolitical focus and ambitions, need to consider devising mechanisms to protect the companies and civil society actors of EU member states from disadvantages created by Russia's new regulations.
- Germany and the EU should actively promote the advantages of the global internet and involve major stakeholders, civil society actors, and business entities in a broad discussion on how to sustain and enhance its future.

THE NEW "SOVEREIGN INTERNET LAW"

New regulations on the internet in Russia, most of which came into force on November 1, 2019 and others of which are due to follow in January 2021, have attracted international attention and been described publicly as Russia's "sovereign internet law." In fact, there was no such new law, but rather a series of amendments to the existing federal laws "On Communication" and "On Information, Information Technologies, and Information Protection."

CONTENTS

Officially, the amendments aim to protect the internet within Russia from external threats. In fact, they provide the crucial legal framework for creating a centralized management system of the internet by the state authority – theoretically enabling the isolation of Russia's network from the global internet. These three amendments have particularly far reaching implications:

- *The compulsory installation of technical equipment for counteracting threats*
- *Centralized management of telecommunication networks in case of a threat and a control mechanism for connection lines crossing the border of Russia*
- *The implementation of a Russian national Domain Name System (DNS)*

RUSSIA'S GOALS

With these three key amendments, Russia is trying to achieve at least three different goals. First, it aims to create a mechanism for effective surveillance of the internet within its borders. To this end, the amendment concerning the installation of "technical equipment for counteracting threats," allows for greater state control of information and the prevention of its dissemination if needed. Consequently, implementation of the new legislation may give the Russian government the opportunity to curtail opposition activity on social media sites, helping it to prevent protests such as those in 2011 through 2013 ahead of elections to Russia's parliament, the State Duma, scheduled for 2021 and the presidential election scheduled for 2024. Even if this amendment is technically difficult to implement, as will be explained below, the law itself is a part of the Putin regime's continuing intimidation strategy and it will impact Russian society.

Second, the state aims to become the key regulator of the internet in Russia. The recent amendment allowing the state to create centralized control over the internet infrastructure by introducing the cross-border control of connection lines and the rerouting of traffic is an attempt to enable the isolation of a national network from the global internet – for which the state can open and close "digital borders" and determine the flow of information within them as it sees fit. While total state control of Russia's internet will remain impossible so long as the country is connected to the world via the existing infrastructure of the global internet, the passing of this amendment by Putin's regime was an attempt to present its control of telecommunication lines, networks, and traffic as a fait accompli.

Third, Russia intends to expand the state-centered model of the internet at the international level. The amendment aiming to create the infrastructure for a national Domain Name System (DNS) could, if achieved as planned in January 2021, create a Russian segment of the internet – parallel to and probably not compatible with the existing one. With this move, Russia is not seeking to isolate itself from the rest of world, but rather to create a precedent, which other states aspiring to sovereignty over their seg-

ments of the internet could follow. Presumably, Russia will need to cooperate even more closely with China than it has already to develop the technology to achieve its goals and coordinate its internet policy at the international level. In the long term, such cooperation could lead to the fracturing of the global internet and a shift of stakeholders and powers.

RISKS TO OTHERS

Although some implications of the three amendments are still unclear and some regulations and requirements are not yet in place, the new legislation already carries concrete risks, which concern not only Russia itself, but also Germany and other European countries that cooperate with Russia and own companies operating within it.

The now compulsory "technical equipment for counteracting threats" will, for example, also be able to prioritize traffic. It can delay the flow of certain types of network packets while prioritizing others, giving them better performance. In practical terms, users of particular websites and services could experience slow access or unavailability. Such prioritization could compromise network neutrality and lead to discrimination against companies not protected by the Russian state.

The fact that neither technical requirements nor certification for this new equipment exist also means that network failures are likelier to happen. Companies operating in Russia could, in turn, suffer collateral damage caused by the new equipment with limited possibilities for recouping losses.

In addition, the likelier prospect of the so-called "splinternet," where segments of the internet are controlled and regulated by different states and actors, could lead to incompatibility among technical, regulatory, and operational standards – thus impeding cross-border cooperation and the interoperability of the global internet.

CENTRALIZING STATE CONTROL OVER THE DECENTRALIZED INTERNET

Russia has a long-standing information and internet policy through which it has already attempted to control the internet in previous years, as was also described in a recent DGAP paper by Andrei Soldatov[1] (see Infobox on page 4). But, in current practice, the state authorities apply the restrictive internet laws that already exist in Russia[2] selectively for two reasons. First, due to the lack of technical capability, some of the laws cannot be implemented. [3] Secondly, certain internet services and applications are so popular that the state does not block them in order to avoid public discontent.[4]

Generally speaking, in order to gain more influence over a domestic internet, state authorities can implement centralized and decentralized control mechanisms. Which one to choose is mainly defined by the network infrastructure and the amount of control countries possess over their networks.[5] China, for example, opts for centralized control; the country brought internet service providers (ISPs) under its yoke early on and traffic is guided through "choke points," network nodes through which data travels when entering or exiting a country's internal network. Countries such as the United Kingdom, India, and Russia currently have much less control over their networks and domestic ISPs. In their case, a decentralized approach is favorable. Authorities roll out new laws and policy measures and oblige ISPs to comply.[6] Up to this point, Russia was "the largest and most aggressive" country pursuing decentralized control,[7] as demonstrated by the laws enacted since 2012 regulating the internet. The new amendments introduced in 2019 aim to give Russian authorities more centralized powers. Roskomnadzor – the Federal Service for Supervision of Communications, Information Technology, and Mass Media – and the central point for control over communication networks and facilities as well as personal data in Russia,[8] wants to monitor traffic at its source, without having an ISP in between or internet services that do not comply with new regulations.[9]

1 Andrei Soldatov, "Security First, Technology Second: Putin Tightens his Grip on Russia's Internet – With China's Help," DGAP Kompakt, Nr. 3, March 2019, <https://dgap.org/system/files/article_pdfs/2019-03-dgapkompakt.pdf > (accessed January 6, 2020).

2 For more on the legislation restricting the internet see the Reporter Without Borders' report "Taking Control? Internet Censorship And Surveillance In Russia," November 2019, < https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/Russiareport_20191128.pdf> (accessed January 6, 2020).

3 "Even without an Internet 'nuclear option,' Russian intelligence has been using an existing law to try to access RuNet user data for months. Here's how"; Meduza, April 23, 2019, <https://meduza.io/en/cards/even-without-an-internet-nuclear-option-russian-intelligence-has-been-using-an-existing-law-to-try-to-access-runet-user-data-for-months-here-s-how> (accessed January 6, 2020).

4 Yana Belyaeva, "Will YouTube, Facebook, and Instagram be banned in Russia?" [in Russian], Deutsche Welle, September 24, 2019, <https://www.dw.com/ru/забанят-ли-в-россии-youtube-facebook-и-instagram/a-50544905> (accessed January 6, 2020).

5 Reethika Ramesh et al., "Decentralized Control: A Case Study of Russia," University of Michigan, November 6, 2019, pp. 2–3, <https://news.umich.edu/how-russias-online-censorship-could-jeopardize-internet-freedom-worldwide/> (accessed January 6, 2020).

6 Ibid., p. 3.

7 Ibid., p. 2.

8 "Powers of Roskomnadzor," Roskomnadzor, January 29, 2013, <http://eng.rkn.gov.ru/about/powers_of_roskomnadzor/> (accessed January 6, 2020).

9 "VPN services refuse to comply with Roskomnadzor's requirements" [in Russian], Roskomsvoboda, March 29, 2019, <https://roskomsvoboda.org/46149/> (accessed January 6, 2020).

Apparently, Russia is now attempting to catch up with what China quickly implemented in the early days of the internet: centralized and effective control mechanisms at the root of the network.

RUSSIA'S INFORMATION AND INTERNET POLICY

One of the first laws was passed in reaction to a series of mass protests in 2011 through 2013. The protests were against manipulation of the parliamentary election and the so-called rokirovka – the position swap between then President Dmitri Medvedev and Prime Minister Vladimir Putin. The opposition made wide use of the internet to bring people to the streets. As a reaction from the state, in 2012, a law on a unified register of banned websites came into force.[10] The register initially included sites containing child pornography and drugs. But less than two years later, in 2014, it was amended to include websites promoting rioting or containing extremist content or participation in mass public events.[11]

Since 2015, all domestic and foreign internet companies are obliged to ensure the recording, systematization, accumulation, and storage of the personal data of Russian citizens on servers physically located within Russia.[12]

In 2016, Yarovaya's Law (named after Irina Yarovaya, a member of the party United Russia in the State Duma and co-author of the legislation) came into force. Since then, telecommunication companies have been required to store the content of text messages, phone conversations, images, and videos for six months, as well as their metadata for three years within Russian territory. They must provide this information to security services upon request.[13]

IMPLICATIONS OF THREE KEY AMENDMENTS

Below the implications of three key amendments included in the new regulations are explained in detail.

1. The Compulsory Installation of Technical Equipment for Counteracting Threats

This amendment requires all internet service providers to install "technical equipment for counteracting threats to stability, security, and the functional integrity of the internet on the territory of the Russian Federation" (TSPU) on their networks.[14] The legislation does not specify which technical equipment should be used. Although, at this writing, there has still been no official decree on this equipment and its technical requirements, the articles of this amendment state that Roskomnadzor will provide it to ISPs free of charge.[15] The technology will apparently be installed nationwide by a single company called "Data – Processing and Automation Center"[16] and controlled by Roskomnadzor.

The past attempt by the Russian state to block Telegram,[17] a cloud-based messaging app, provides a good example of how the regime is attempting to use this amendment to prevent unrestricted communication that could be utilized to coordinate social unrest and opposition movements.[18] Telegram claims to allow the secure exchange of information through end-to-end encryption, which makes communication possible without intelligence services being able to read it. In 2018, according to the founder of the company Pavel Durov, Telegram had over 15 million users in Russia.[19]

In its attempt to block Telegram, Roskomnadzor tried to ban the IP addresses of Telegram servers without success.[20] In order to finally ban the service[21] and prevent undisclosed

10 Resolution of the Government of the Russian Federation No. 1101 dated October 26, 2012 (Moscow) "On the Unified Automated Information System 'Unified Register of Domain Names, Indexes of Pages of Websites in the Information and Telecommunication Network 'Internet' and Network Addresses that Allow Identification of Websites in the Information and Telecommunication Network 'Internet' containing information the dissemination of which is prohibited in the Russian Federation'" [in Russian], Rossiyskaya Gazeta, October 29, 2012, <https://rg.ru/2012/10/29/reestr-dok.html> (accessed January 6, 2020).

11 "On the entry into force of amendments to the Federal Law 'On Information, Information Technologies, and Information Protection'" [in Russian], Roskomnadzor, January 31, 2014, <https://rkn.gov.ru/news/rsoc/news23647.htm> (accessed January 6, 2020).

12 "Processing and storage of personal data in the Russian Federation. Changes from September 1, 2015" [in Russian], Ministry of Digital Development, Communications and Mass Media of the Russian Federation, February 12, 2016, <https://digital.gov.ru/en/personaldata/> (accessed January 6, 2020).

13 "Federal law No. 374-FZ dated July 6, 2016 about making changes to the federal law 'on counterterrorism' and certain legislative acts of the Russian Federation in terms of establishing additional countermeasures to terrorism and public security" [in Russian], Rossiyskaya Gazeta, July 8, 2016, <https://rg.ru/2016/07/08/antiterror-dok.html> (accessed January 6, 2020).

14 Article 46, Federal Law No. 90-FZ dated May 1, 2019 "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies, and Information Protection'" [in Russian], Official Internet Portal for Legal Information, May 1, 2019, <http://publication.pravo.gov.ru/Document/View/0001201905010025?index=2&rangeSize=1> (accessed January 6, 2020).

15 Ibid., article 65[1]

16 Maria Kolomychenko, "Nokia's former head in Russia will implement 'sovereign Runet' systems" [in Russian], RBK, September 26, 2019, <https://www.rbc.ru/technology_and_media/26/09/2019/5d8b4c1c9a7947d3c58f9a48> (accessed January 6, 2020).

17 "Russia will check the means to block Telegram on users in Tyumen – sources" [in Russian], Reuters, September 13, 2019, <https://ru.reuters.com/article/topNews/idRUKCN1VY1U1-ORUTP> (accessed January 6, 2020).

18 Ilya Khrennikov, Stepan Kravchenko, "Putin Wants His Own Internet," Bloomberg, March 5, 2019, <https://www.bloomberg.com/news/articles/2019-03-05/vladimir-putin-wants-his-own-internet> (accessed January 6, 2020).

19 Post by Pavel Durov on the social network platform "VK," April 16, 2018, <https://vk.com/wall1_2296940> (accessed January 6, 2020).

20 Mikhail Zelensky, "Russia is trying to block Telegram, but it's failing. Why?", Meduza, April 17, 2018, <https://meduza.io/en/cards/russia-is-trying-to-block-telegram-but-it-s-failing-why> (accessed January 6, 2020).

21 See note 16: Kolomychenko, "Nokia's former head in Russia will implement 'sovereign Runet' systems."

communication, Russian authorities might use, among others, a technology commonly referred to as Deep Packet Inspection (DPI). This new amendment obliges ISPs to accept and cooperate in the installation process of DPI systems or a similar technology.

DEEP PACKET INSPECTION

The main technical components of DPI systems are so-called black boxes, which are installed at the hubs of internet providers to analyze both data packets and the content of communications. They enable the monitoring, filtering, and slowdown of requests as well as the blocking of specific content. The black boxes can also determine to which service or application each data packet is attributed. Although DPI systems have been used in Russia since 2012, when legislation creating an internet blacklist was enacted,[22] ISPs have yet to introduce them widely because of their high cost, which they had to bear themselves.

Anonymous sources have told the BBC that DPI systems, which have already been tested on the networks of all major mobile network operators in the Ural region,[23] are indeed Roskomnadzor's choice.[24] While it can therefore be assumed that the implementation of the TSPU amendment will be based, at least in part, on the use of Deep Packet Inspection technology – the exact specifications, capabilities, and effectiveness of which are unknown – it might also include other hardware and software solutions, which are also unknown at this time.

Even Encrypted Connections Might Be Blocked

If Roskomnadzor widely implements DPI systems or similar technologies, they might be used to block undesired traffic and severely censor the Russian web. One might think that DPI systems cannot identify, and therefore block, packets of encrypted connections such as HyperText Transfer Protocol Secure (HTTPS),[25] which is widely used on the World Wide Web.[26] Unfortunately, this is not entirely the case. Because data packets – even those sent via an encrypted connection – are always sent to a certain destination, they must always carry an address that is visible. This information cannot be encrypted because an ISP would otherwise not know to which address it is supposed to send the user's request. For example, an ISP will know that a user is requesting data from YouTube, the size of the request, and its length. But, thanks to encryption, it will not know which specific video the user is watching.

For Russian authorities, the package destination might be indicator enough to block requests from undesired websites. One possible solution would be for a user to hide the address of the packet he or she wishes to send by redirecting it through a Virtual Private Network (VPN). In this case, the user doesn't communicate directly with the ISP but through one or several entities in between. This makes the destination of the request only visible to the VPN service provider but not the ISP. But, since Russian authorities are also trying to use DPI systems or similar technologies to shut down VPN services, this workaround may sooner or later cease to be a viable option.

Another workaround in current use is a technique called "domain fronting," with which a request gets redirected on the same server after a HTTPS connection has been established. This technique, among others, was used by Telegram to bypass Roskomnadzor's IP bans. However, this workaround, too, is becoming more difficult to implement as companies such as Amazon or Google, which operate servers also used for domain fronting, seek to end this practice.[27]

Traffic Speeds May Be Prioritized and Discriminated

DPI or similar technologies can also be used to prioritize and discriminate traffic. Prioritizing traffic could have far-reaching consequences for net neutrality, especially if it is carried out by a state authority. Roskomnadzor could slow down the traffic speed

22 Andrei Soldatov, Irina Borogan, "The Kremlin's New Internet Surveillance Plan Goes Live Today," Wired, November 1, 2012, <https://www.wired.com/2012/11/russia-surveillance/> (accessed January 6, 2020).

23 See note 16: Kolomychenko, "Nokia's former head in Russia will implement 'sovereign Runet' systems"; and note 17: "Russia will check the means to block Telegram on users in Tyumen – sources."

24 Andrey Zakharov, Svetlana Reyter, "Roskomnadzor will introduce a new Telegram blocking technology for 20 billion rubles" [in Russian], BBC, December 18, 2018. <https://www.bbc.com/russian/features-46596673> (accessed January 6, 2020).

25 David Naylor et al., "The Cost of the 'S' in HTTPS," Proceedings of the 10th ACM International Conference on emerging Networking Experiments and Technologies CoNEXT, December 14, 2014, pp. 133–140, <https://core.ac.uk/download/pdf/76526401.pdf> (accessed January 6, 2020).

26 "HTTPS encryption on the web" [in German], Google transparency report, <https://transparencyreport.google.com/https/overview> (accessed January 6, 2020).

27 Hakan Tanriverdi, "A decision by Google and Amazon, which will delight censors" [in German], Sueddeutsche Zeitung, May 2, 2018, <https://www.sueddeutsche.de/digital/it-sicherheit-eine-entscheidung-von-google-und-amazon-die-zensoren-freuen-wird-1.3965101> (accessed January 6, 2020).

of all unknown or undesired connections and prioritize trusted connections of entities that comply with the fixed rules.[28]

European telecommunication operators may have confirmed that such prioritization and discrimination of traffic works. Larger ISPs – including Deutsche Telekom – are suspected of using DPI for commercial purposes in order to control traffic speeds to block intensive forms of consumption (for example streaming) that are not included in a user's contract.[29] And if ISPs can slow down connections, Roskomnadzor could do the same in order to put enormous pressure on companies that do not comply with its fixed rules. If a state authority massively slows down some connections, targeted companies could face issues that threaten their businesses. These could include seeing a marked decrease in their user base as customers dissatisfied with the inconvenience of substantially slower services are pushed toward alternatives.

If this amendment is fully implemented, bypassing DPI services and accessing restricted areas of the internet will be very difficult except for highly skilled users, leading to an "asymmetry of blocking effectiveness."[30] Since it must be assumed that IT specialists can circumvent DPI systems, the amendment's official goal – repulsing threats – is not entirely plausible. In other words, it is likelier that the primary target of wide implementation of DPI is Russia's ordinary users, whose internet use will assuredly be restricted. Private companies might also be targeted to cause them economic disadvantages.

2. Centralized Management of Telecommunication Networks in Case of a Threat and a Control Mechanism for Connection Lines Crossing the Border of Russia

This new amendment states that the media regulator Roskomnadzor can take over the centralized management of the network[31] in case of a "threat." The three main threats are defined in a government decree on the "centralized management of a public communications network,"[32] which is currently still in its development phase and has not yet entered into force. These threats are:

1. *to the integrity of the network, for example when no connection can be established between users;*
2. *to the stability of the network, for example when equipment does not work correctly or is disabled due to natural or man-made disasters;*
3. *to the safety of the functioning of the network, for example when hackers attack the network and ISPs cannot resist the attack, or when ISPs themselves cause disruption.*[33]

If any of these threats materialize, Russian ISPs will have to comply with the rules fixed by Roskomnadzor, which then prohibit the routing of telecommunication messages through communication networks located outside of the territory of the Russian Federation.[34] In addition, when two autonomous systems wish to communicate with each other, they will have to do so through traffic exchange and connection points[35] monitored by Roskomnadzor. The agency can ask any ISP or person running an autonomous system to "change the routes of telecommunication messages" and guide those messages through "technical means to counteract threats to the stability, security, and integrity of the functioning of the [...] internet."[36]

28 Maria Kolomychenko, "Roskomnadzor proposed testing Runet for 'sovereignty'" [in Russian], RBK, March 28, 2019, <https://www.rbc.ru/technology_and_media/28/03/2019/5c9cdfa09a79473d7d241980> (accessed January 6, 2020).

29 Thomas Lohninger, et al., "The Net Neutrality Situation in the EU," Epicenter Works, January 29, 2019, pp. 39–40, <https://epicenter.works/sites/default/files/2019_netneutrality_in_eu-epicenter.works-r1.pdf> (accessed January 6, 2020).

30 Philipp Winter, et al., "ScrambleSuit: A Polymorph Network Protocol to Circumvent Censorship," Arxiv Cornell University (New York), May 14, 2013, <https://arxiv.org/pdf/1305.3199.pdf> (accessed January 6, 2020).

31 See note 14: Article 65[1] of "Federal Law No. 90-FZ."

32 "On approval of the procedure for centralized management of the public communication network" [in Russian], Federal portal of draft regulatory legal acts, <https://regulation.gov.ru/projects#npa=91558> (accessed January 6, 2020).

33 Ibid., article 2.

34 Article 2, "Order of the Federal Service for Supervision of Communications, Information Technologies, and Mass Communications No. 224 dated July 31, 2019 'On the Approval of the Rules for Routing Telecommunication Messages in the Case of Centralized Management of a Public Communication Network'" [in Russian], Official internet portal for legal information, November 6, 2019, <http://publication.pravo.gov.ru/Document/View/0001201911060018?index=2&rangeSize=1> (accessed January 6, 2020).

35 Ibid., article 4.

36 Ibid., article 5.

Furthermore, this new amendment creates a control mechanism for connection lines crossing the border of the Russian Federation. All owners of such communication lines are obliged to report not only their purpose, but also which facilities exist on that line to Roskomnadzor.[37]

Russia has more than 40 providers on its borders, and – for now – no large choke points

The Danger of a Kill-Switch

The aforementioned stipulations give state authorities the potential to create a "kill-switch," a relatively easy to use mechanism that can be used to shut down most of the Russian internet. In the event of such a shutdown, even DPI bypass systems, VPNs, or other unidentified connections will not work – communication becomes physically impossible.

The global internet is strong and redundant because its traffic is handled by a web of computers and servers; data can therefore take many different paths in order to reach its destination. The amount of centralized traffic exchange and choke points strongly affects the power of a government to censor and repress data flows.[38] The lower the amount of choke points, the more easily they can be controlled.

With implementation of this new amendment, Russian authorities will weaken the robust structure of the Russian internet by guiding traffic through centralized, state-controlled connection points, which can be shut down in case of a "threat." Russian authorities might soon be able to cut off major parts of the network and thus prevent information that is critical of the government from entering or spreading within the country.

In the past, several deliberate internet shutdowns have occurred in different countries on different scales. An intentional local shutdown is theoretically possible in any country with a weak legal system – because it can be pushed through with little juridical resistance. For example, one such shutdown took place in August 2019 during rallies in the center of Moscow; the BBC claims it was requested by law enforcement agencies.[39] In November 2019, Iran cut off most of its internet for several days. However, this nationwide shutdown was only possible because the country relies on data connections through choke points[40] and has a very limited number of ISPs, which are all state-controlled. In contrast to Iran, Russia has more than 40 providers on its borders, many ISPs, and – for now – no large choke points. These parameters had made any major internet shutdown in Russia hard to execute.[41] The new amendments, however, create a new legal basis for just such a scenario, thus enhancing the probability of a shutdown.

3. The Implementation of a Russian National Domain Name System (DNS)

This key amendment concerns the creation of a Russian national Domain Name System (DNS), which is due to be implemented by January 2021.[42] It aims "to ensure a stable and safe use of domain names on the territory of the Russian Federation."[43] The Russian national domain zone will be composed of its own infrastructure, which means root servers and proprietary domain names. Roskomnadzor is again vested with enormous power: it will define regulations on the national DNS, requirements for it, and the procedure for its establishment, as well as the rules for its use. It will also determine the list of domain name groups constituting the Russian national domain system.[44]

37 See note 14: Article 56² of "Federal Law No. 90-FZ."

38 Monique Clement, "Choke points and censorship: Protecting free flow of information on internet," Arizona State University, September 10, 2018, <https://ui.asu.edu/content/choke-points-and-censorship-protecting-free-flow-information-internet> (accessed January 6, 2020).

39 Elizaveta Foht, "The Internet could be jammed during rallies in Moscow at the request of security forces" [in Russian], BBC, August 6, 2019, <https://www.bbc.com/russian/features-49255791> (accessed January 6, 2020).

40 Ivana Kottasová, Sara Mazloumsaki, "The 'internet as we know it' is off in Iran. Here's why this shutdown is different," CNN, November 19, 2019, <https://edition.cnn.com/2019/11/19/middleeast/iran-internet-shutdown-intl/index.html> (accessed January 6, 2020).

41 David Belson, "The Migration of Political Internet Shutdowns," Oracle Dyn, November 28, 2019, <https://dyn.com/blog/the-migration-of-political-internet-shutdowns/> (accessed January 6, 2020).

42 See note 14: Article 14² of "Federal Law No. 90-FZ."

43 Ibid.

44 Ibid.

The creation of a proprietary national DNS has never been successfully achieved by any country. It is therefore very hard to predict if such a system could work in parallel to the worldwide DNS in current use, which is allocated and managed by the International Corporation for Assigned Names and Numbers (ICANN). A national DNS would only make sense if a country opts for a long-term and complete isolation of its internet. If Russia manages to implement the new amendments providing for the control of all networks and servers on its own territory and allowing for their disconnection from the global internet, it would then need its own domain name system. This would segregate Russian websites from the international DNS, making them unavailable in all other parts of the world. At the same time, Russia would likely become unable to use the global DNS.

Aspiring to Independence from ICANN

In an explanatory note about Russia's new law on the "sovereign internet," the Russian legislature claims that it was created in light of "the aggressive nature of the US National Cyber Security Strategy adopted in September 2018."[45] In it, the US accuses Russia – along with China, Iran, and North Korea – of using "cyber tools to undermine [its] economy and democracy, [and to] steal [its] intellectual property."[46] Furthermore, the document states that the United States will punish those who use cyberattacks against them.[47] According to the explanatory note, Russia needs to take "protective measures to ensure the long-term and stable operation of the internet in Russia, and to increase the reliability of Russian internet resources."[48]

But it would be misleading to consider Russia's new internet legislation as a mere reaction to the US National Cyber Security Strategy of 2018. Since 2012, Russia has been actively criticizing ICANN's dominant position in coordinating the global DNS, allocating IP addresses, and governing the internet.[49] In parallel, Russia is pushing for an alternative internet governance model with strong state sovereignty and within the framework of the International Telecommunication Union (ITU) of the United Nations.[50]

Russia is pushing for an alternative internet governance model with strong state sovereignty

Russian fears of getting cut off from the internet expressed in the explanatory note are not fully plausible. First and foremost, because ICANN is an independent organization,[51] interference from the US government is legally almost out of the question. Moreover, the US government is most likely not technically capable of shutting down domains related to Russian websites. The worldwide DNS is managed by IANA (the Internet Assigned Numbers Authority), a function of ICANN located in California. Top Level Domains (TLDs) like .ru or .de are stored on so-called root zone files. These files, which are managed by ICANN and can be considered the backbone of the internet, are primarily stored on 13 root zone servers worldwide – ten of which are located in the US, and one each in the Netherlands, Sweden, and Japan.[52] But TLD files are also stored on many other name servers.[53] If the 10 root servers on US soil are modified so that the domains of Russian websites are redirected, for example, there are still three other root servers and all the name servers left. As soon as manipulation of the root zone files is detected, DNS providers can stop the mirroring process from US root servers. Hence, all the remaining DNS servers would still have the files which grant access to the Russian domain names. Consequently, even if

45 "The Sovereign Internet law has been passed" [in Russian], State Duma, April 16, 2019, <http://duma.gov.ru/news/44551/> (accessed January 6, 2020).

46 "National Cyber Strategy of the United States of America," The White House, September 2018, p. 1, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (accessed January 6, 2020).

47 Ibid., p. 3.

48 See note 45: "The Sovereign Internet law has been passed."

49 "Russia backtracks on internet governance proposals," BBC, December 11, 2019, <https://www.bbc.com/news/20676293> (accessed January 6, 2020).

50 Adi Robertson, "New World Order: is the UN about to take control of the internet?", The Verge, November 29, 2012, <https://www.theverge.com/2012/11/29/3706352/un-itu-talks-dubai-guide> (accessed January 6, 2020).

51 "Why is America giving up control of ICANN?", The Economist, September 30, 2016, <https://www.economist.com/the-economist-explains/2016/09/29/why-is-america-giving-up-control-of-icann> (accessed January 6, 2020).

52 "List of Root Zone Servers," IANA, https://www.iana.org/domains/root/servers (accessed January 6, 2020).

53 "List of Root Servers", Root Servers, <https://root-servers.org/> (accessed January 6, 2020).

almost all the root servers are located in the USA, a shutdown of TLDs related to Russian websites by the US government is not a realistic scenario.[54]

Against this background, it seems as though the aim of this new amendment is not to defend the internet in Russia from outside attacks, but rather a proactive step toward splitting its own national segment off from the infrastructure of the global internet in order to gain state sovereignty over it. First of all, a proprietary DNS would make Russia independent from ICANN,[55] which the Kremlin sees as being dominated by the USA. And – although technical implementation seems far from easy – a national DNS is the key part which would allow the state to cut off the domestic internet for the long term. Russia would then not have to cope with international traffic and, thus, undesired information leaving or entering the country.

RUSSIA WILL LIKELY BUILD UP ITS PARTNERSHIP WITH CHINA

Russia's ambitions to build a model of state-backed internet control, create its own national DNS, and set new rules in cyberspace only make sense if it teams up with other countries. It remains to be seen how many countries would want to join its experiment. However, Russia already has a longstanding relationship with China when it comes to the internet. Both countries have had several high-level meetings on cybersecurity and internet control.

In May 2015, Russia and China signed a bilateral agreement on cooperation in the field of international information security[56] and defined a broad range of forms in which such cooperation could take place. The agreement includes the "creation of communication channels and contacts to jointly respond to threats," "exchange of information on the legislation of the states on ensuring information security," and "interaction in the development and promotion of international law standards to ensure national and international information security."[57]

Additionally, in June 2016, Vladimir Putin and Xi Jinping signed the joint statement on cooperation in information space development. Both leaders stress they "uphold as always the principle of respecting national sovereignty in information space," and "explore the possibilities of developing universal rules of responsible behavior in the information space within the UN framework."[58] Indeed, China has often supported Russia's initiatives in setting rules in cyberspace within the UN framework.[59]

A Sino-Russian cooperation could lead to the fracturing of the global internet

Such cooperation with China can be beneficial for Russia's ambitions in the internet in both domestic and international politics in a number of ways. First of all, Russia's divergence from the West means it might need technology from China; in fact, it is already striking deals with Chinese companies. In June 2019, for example, Huawei signed – in the presence of President Vladimir Putin and President Xi Jinping – a contract with MTS, one of the biggest Russian telecom companies, to develop Russia's 5G network.[60] Just a couple of months later, they jointly launched the first 5G test zone in Moscow.[61]

54 Roman Goncharenko, "Russia moves toward creation of an independent internet," Deutsche Welle, January 17, 2018, <https://www.dw.com/en/russia-moves-toward-creation-of-an-independent-internet/a-42172902> (accessed January 6, 2020).

55 Ibid.

56 "Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security" [in Russian], Ministry of Foreign Affairs of the Russian Federation, May 8, 2015, <https://www.mid.ru/foreign_policy/international_contracts/2_contract/-/storage-viewer/bilateral/page-42/43921> (accessed January 6, 2020).

57 Ibid.

58 "Joint statement between the presidents of China and Russia," China Daily, June 26, 2016, <https://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm> (accessed January 6, 2020).

59 See "Sixty-sixth session, Item 93 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security, A/66/359," United Nations General Assembly, September 14, 2011, <https://undocs.org/A/66/359> (accessed January 6, 2020); and "Sixty-ninth session, Agenda item 91, Developments in the field of information and telecommunications in the context of international security, A/69/723," United Nations General Assembly, January 13, 2015, <https://undocs.org/A/69/723> (accessed January 6, 2020).

60 "MTS and Huawei to Develop 5G in Russia" [in Russian], RBK, June 5, 2019, <https://www.rbc.ru/technology_and_media/05/06/2019/5cf7d7ab9a79475b30e51df3> (accessed January 6, 2020).

61 Dimitri Simes, "Russia and Huawei team up as tech cold war deepens," Nikkei Asian Review, October 28, 2019, <https://asia.nikkei.com/Politics/

Secondly, Russian authorities can benefit from China's experience in internet regulation and surveillance when it comes to implementing its new legislation on internet control. According to press reports, Roskomnadzor and its Chinese counterpart – the Cyberspace Administration of China – are going to cooperate in countering the spread of prohibited information.[62]

Cooperation between Moscow and Beijing does not, however, automatically mean that the Russian authorities can simply imitate China's procedures in blocking undesired traffic. As already mentioned, given the fact that China began its isolation process and the implementation of its so called "Great Firewall" in the early days of its participation in the internet, the structure of China's network is, for now, very different from Russia's, which has been fully integrated into the global, decentralized internet from the outset. While the Chinese internet has only very few cross-border traffic exchange hubs, Russia's has many – some of which are not even on the radar of its state authorities.[63]

Germany should add coordinating support for the existing multi-stakeholder model of internet governance

Furthermore, as China has its own global internet services, it does not rely on YouTube, WhatsApp, Google, or Facebook. In Russia, the US companies Google and Facebook currently provide some of the most widely used internet platforms.[64] Many of these companies operate on an international level. Google, for instance, stores user data on many different servers worldwide,[65] making them hard to regulate. Because Russia's society and economy rely so heavily on services such as social networks, search engines, financial services, and Software as a Service (SaaS), replacing foreign ones with domestic versions seems to be a nearly insurmountable task. Simply shutting down foreign platforms would also have tremendous negative consequences for the economy and likely generate social outrage.

In addition, Russia needs to partner with China at the international level to promote the idea of state sovereignty in cyberspace. As previously suggested, Russian fragmentation from the global internet would only make sense if the country had allies with whom it could establish a parallel network. In November 2017, it became known that Russia's Security Council instructed the Ministry of Communications and the Ministry of Foreign Affairs to develop ideas for a separate internet infrastructure and its own DNS root server system for the BRICS countries – Brazil, Russia, India, China, and South Africa – independent from ICANN.[66] Successfully establishing a regional segment of the internet will depend on Russia and China developing a network infrastructure which can be sustained without the architecture of the global internet. As yet, it is difficult to predict if they will succeed. It is also still unclear to what extent it will be attractive for other countries to shut themselves off from the global internet. However, with the new legislation, Russia has created a legal framework whose implementation must be taken seriously.

RECOMMENDATIONS

First, Germany and the EU should begin assessing the risks and long-term implications of Russia's new internet legislation for European companies and civil society actors in a timely manner. The EU needs a clear understanding of Russia's dependence on the internet ecosystem, its technical capability, and its political goals in order to differentiate between the officially proclaimed goals of the Russian state and

International-relations/Russia-and-Huawei-team-up-as-tech-cold-war-deepens> (accessed January 6, 2020).

62 "Roskomnadzor will sign an agreement with China's Internet regulator" [in Russian], RBK, October 8, 2019, <https://www.rbc.ru/rbcfreenews/5d9cad499a7947c9c1a6d665> (accessed January 6, 2020).

63 Alexandra Prokopenko, "Russia's Sovereign Internet Law will kill innovation," Carnegie Moscow Center, April 19, 2019, <https://carnegie.ru/commentary/78946> (accessed January 6, 2020).

64 "Top Websites ranking in the Russian Federation," SimilarWeb, November 1, 2019, <https://www.similarweb.com/top-websites/russian-federation> (accessed January 6, 2020).

65 "Discover our data center locations," Google Data Centers, <https://www.google.com/about/datacenters/locations/> (accessed January 6, 2020).

66 Maria Kolomychenko, "Russian Security Council instructed to create an 'independent internet' for the BRICS countries" [in Russian], RBK, November 28, 2017, <https://www.rbc.ru/technology_and_media/28/11/2017/5a1c1db99a794783ba546aca?from=main> (accessed January 6, 2020).

its real intentions – which is, in turn, a prerequisite for taking appropriate action.

Second, EU institutions need to consider taking active steps to protect the companies and civil society actors of EU member states operating in Russia from disadvantages created by the Putin regime's new regulations. The European Commission with its geopolitical focus and ambitions could play a particularly key role in creating and implementing such measures.

Third, the German government could play an important role in advocating for an open and free internet. Concretely, Germany should add coordinating support for the existing multi-stakeholder model of internet governance to the tasks of its upcoming EU presidency, which begins in the second half of 2020. Standards for transnational legal regulations, for example, need to be developed as soon as possible – particularly because the ongoing cooperation between China and Russia in filtering, controlling, and regulating the internet poses a real danger of segmenting the existing internet and shifting global power.

Finally, Germany and the EU should actively promote the advantages of the global internet and involve major stakeholders, civil society actors, and business entities in a broad discussion on how to sustain and enhance its future. Ideally, they should develop a common long-term strategy for preserving the internet in its current, non-segmented, truly global form, which would involve widening the scope of existing platforms such as the United Nations' Internet Governance Forum.

Acknowledgment: The author wishes to thank Philipp Dietrich for his excellent support in the research, writing, and discussion of this DGAP Analysis.

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin

Tel. +49 (0)30 25 42 31 -10

info@dgap.org
www.dgap.org
@dgapev

Publisher
Deutsche Gesellschaft für Auswärtige Politik e.V.

ISSN 1611-7034

Editing Helga Beck

Layout Charlotte Merkl
Design Concept: WeDo

Author picture(s) © DGAP