# Country Focus Report: Russian Federation Internet-Related Laws and United Nations Deliberations

**Developments in the Field of Information and Telecommunications in the Context of International Security (Cybersecurity)**

Veni Markovski
Alexey Trepykhalin
19 January 2021
GE-006

ICANN

## TABLE OF CONTENTS

# Introduction

This paper is the first in a periodic series of country-specific reports that will provide an overview of activity relevant to the Internet Ecosystem and ICANN's mission. The series begins with the Russian Federation because of the important role and level of activity it is currently displaying in the global cyber ecosystem as well as its record for involvement and activity in UN bodies.

The paper focuses on Russian Federation laws, international positions, and United Nations initiatives, as it has a long record of proposing United Nations General Assembly (UNGA) cyber-related resolutions[1].

This report provides analyses based on primary source texts drawn from some of the Russian Internet-related laws, which touch on the DNS, Internet Protocol (IP) addresses, protocol parameters, and so forth. Additionally, it provides information on relevant texts and statements about Russian positions on the same issues at the United Nations (UN); thus, providing the ICANN community with the necessary information and a better understanding of the deliberations taking place at the United Nations.

This is in line with the ICANN organization's strategic objective to "Address geopolitical issues impacting ICANN's mission to ensure a single, globally interoperable Internet," and strategic goal to "Identify and address global challenges and opportunities within its remit" found in ICANN's Strategic Plan for 2021-2025.

The ICANN org's Government Engagement team has already covered the status of the cybersecurity and cybercrime deliberations taking place at the United Nations in previous publications.[2]

# Background

The Russian Federation is a permanent member of the United Nations Security Council and is actively engaged in international cyber-related initiatives.[3] At the same time, it is also one of the countries that in recent years has drafted and passed a number of domestic laws, regulations, ordinances, and other acts, dealing with different aspects of the Internet. Given these cyber-related policy activities, it would be useful for the broader ICANN community to have a closer look at the national legislation of the Russian Federation and the extent to which it informs the understanding of the Russian position in international initiatives. For ICANN org, it is important to examine the current state of affairs in regard to the technical governance of the Internet.

[1] The Russian Federation doesn't use the term cybersecurity in official documents; instead it uses "information security"; the UN-resolutions use terms like "developments in the field of information and telecommunications in the context of international security". This document uses "cybersecurity" as a shorter term.
[2] Markovski, Veni, "Brief Overview of UN Deliberations on Cybersecurity and Cybercrime," Government and Intergovernmental Engagement Function, ICANN, 28 February 2020, https://www.icann.org/en/system/files/files/ge-001-28feb20-en.pdf; Markovski, Veni, "United Nations Update: Cyber-Related Discussions," Government and Intergovernmental Engagement Function, ICANN, 15 July 2020, https://www.icann.org/en/system/files/files/ge-005-15jul20-en.pdf
[3] At the UN, but also within other intergovernmental organizations it is a member of.

# Laws and Regulations

For the purposes of this report, the focus will be on the laws and regulations that went into effect from November 2019 until the end of October 2020.

On 1 November 2019, the Russian Federal Law N90-FZ, "On the Introduction of Changes to the Federal Law 'On Communications' and 'On Information, Information Technologies and Information Protection'" widely known as "the Sovereign Internet Law," went into effect.[4]

The explanatory memorandum to this law stated that it takes into account the "aggressive nature of the 2018 U.S. National Cyber Strategy," and that there is a need for "protective measures to secure the long-term and stable functioning of the Internet in Russia..."[5]

This law introduced new controls of the Internet within Russia by:

(1) Requiring the Internet Service Providers (ISPs) to ensure the installation of technical equipment on the networks in order to counter threats to the Internet's stability, security, and functioning.
(2) Designating the governmental body to coordinate the functions as per point (1).
(3) Granting to this body the authority to monitor "the Internet and public communications networks" in order to "identify threats" to these networks' "stability, security and [...] functioning";
(4) Ensuring that the body will serve as the centralized manager of "public communications networks" in case of a threat.
(5) Postulating the creation of a "national domain name system."[6]

See Appendix 1 for a list of the Russian Federation's provisions governing DNS as part of its Sovereign Internet Law.

The law[7] is scheduled to go fully into effect starting 1 January 2021. Major ISPs in the Russian Federation would then be required to use the national domain name system, and government authorities of all levels would have to provide the option for using Russian cryptography in their electronic communications.[8]

[4] Sovereign Internet Law Adopted, Russian State Duma News, 16 April 2019, http://duma.gov.ru/news/44551/.
[5] Russian State Duma, Legislation 608767-7, On Amendments to the Federal Law 'On Communications' and the Federal Law "On Information, Information Technologies and Information Protection', 1 May 2019, https://sozd.duma.gov.ru/bill/608767-7.
[6] See Articles 1 and 2 of the Law on Sovereign Internet, Russian Federal Law, "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'", 22 April 2019, http://publication.pravo.gov.ru/Document/Text/0001201905010025.
[7] The law did not create a separate legal act but amended two existing federal laws: "On Communications" and "On Information, Information Technologies and Information Protection".
[8] See Article 3 of the Law on Sovereign Internet, 22 April 2019, http://publication.pravo.gov.ru/Document/Text/0001201905010025.

According to some,[9] "technical equipment" relates to deep packet inspection (DPI). The provisions of this law also introduce centralized control over transborder connection lines, internet exchange points, and autonomous system (AS) numbers. It also establishes the requirement for ISPs and "other" AS number holders to participate in Internet drills,[10] as described in this law.

This law's provisions currently in effect and the numerous regulations and orders enacted to date, designate the Russian Ministry of Digital Development, Communications and Mass Media (MoC), its subordinate agency, the Federal Service for Communications, Information Technology and Mass Media Oversight (Roskomnadzor) as the main implementation authorities.[11]

This law specifies that the government is responsible for the Internet drills and for providing the ISPs with training in practical skills,[12] while Roskomnadzor oversees and coordinates "the Internet and public communications networks" and, in the case of a potential threat, should function as the "centralized authority" over public networks.[13]

In September 2020, the MoC issued new draft legislation for public discussion, which, among other things, intends to forbid the use of encryption protocols within the Russian Federation that allow masking of website names.[14] The explanatory memorandum says that the draft legislation will regulate the following protocols: *TLS 1.3, ESNI, DoH (DNS over HTTPS),* and *DoT (DNS over TLS).*[15] This draft legislation is currently being deliberated within the government.[16]

[9] Maria Kolomychenko, "Ex-head of Nokia in Russia to Spearhead the Deployment of "Sovereign Runet, Technologies to be Used to Block Telegram", RosBusinessConsulting (RBK), 26 September 2019, https://www.rbc.ru/technology_and_media/26/09/2019/5d8b4c1c9a7947d3c58f9a48; Ekaterina Kinyakina, "The Law of the Year. Why Internet Will Not Become Sovereign in Russia", Vedomosti, 26 December 2019, https://www.vedomosti.ru/technology/articles/2019/12/26/819870-zakon-goda;
"The Government Has Adopted Rules for Installing and Operating Equipment for the Sovereign Runet at Internet Provider Facilities", denis-19, Xabr, 17 February 2020, https://habr.com/ru/news/t/488718/; Ilya Sharapov, Yevgeny Medvedev, "Runet of the Foreseeable Future. Slow, Censured, a Third 'Chinese'", 29 March 2019, *Snob*, https://snob.ru/entry/174726/.

[10] Russian Federal Law, "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'".

[11] See Appendix 2 for a list of implementation regulations.

[12] See Article 1 of the Sovereign Internet Law: Russian federal law, "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'".

[13] The definition of the "public communications network" as "telecommunications network" can be found here: Article 13, Paragraph 2 Russian Federal Law No. 126-ФЗ (revised), "On Communications", July 7, 2003, http://www.consultant.ru/document/cons_doc_LAW_43224/9bfb991d2b91aa76860cfcc8b8f5870431f7113e/

[14] "On Amendments to Articles 2 and 10 of the Federal Law 'On Information, Information Technologies and Information Protection'", Federal Draft Regulatory Legal Act Portal, 21 September 2020, https://regulation.gov.ru/projects#npa=108513.

[15] "On Amendments to Articles 2 and 10 of the Federal Law 'On Information, Information Technologies and Information Protection'", Federal Draft Regulatory Legal Act Portal, 21 September 2020.

[16] Shadaev, Maksut Igorevich, Maksut Shadaev Comments on the Bill to Prohibit Some Encryption Methods, Official Announcement, Ministry for Digital Development, Communications and Mass Media, 22 September 2020, https://digital.gov.ru/ru/events/40090/.

The COVID-19 pandemic caused the rescheduling of two out of the four planned drills. The MoC, however, cancelled the third scheduled drill on different grounds related to changes in the legislation, resulting in only one drill taking place, in December 2019.[17]

## Russian Cyber-Related Foreign Policy Statements and Initiatives in 2020

The Russian Federation has been involved in a number of international cybersecurity-related[18] initiatives dating back to 1998 (UNGA resolution 53/70[19]). As noted above, ICANN org is only focusing on the relevant statements made by high-level government officials from November 2019 till the end of October 2020, which are reflective of the changes in the national legislation.

On 22 October 2020, President Vladimir Putin said in a virtual session of the Valdai Discussion Club: "I will remind you that Russia is actively promoting bilateral and multilateral agreements in the cybersphere. We have introduced two draft conventions at the UN on this issue, and started an Open-ended Working Group to that effect."[20]

On 2 October 2020, the Russian Security Council (RSC) published a read-out of the meeting in Geneva between the U.S. National Security Adviser Robert O'Brien and the Secretary of the RSC Nikolai Patrushev, stressing that "the dialogue on counterterrorism issues and questions of informational security is called for."[21]

On 28 September 2020, Foreign Minister Sergey Lavrov published an article in the journal International Economic Relations,[22] in which he mentions the ongoing cyber deliberations at the United Nations, and notes: "All states without exception must be involved in resolving and discussing this global problem. It is also important to consider the opinions of other stakeholders (businesses, civil society and the scientific community)."

[17] Ministry of Digital Development, Communications and Mass Media Did Not Hold Runet Resilience Drill on September 20, *TASS*, 21 September 2020, https://tass.ru/ekonomika/9507051, see Appendix 3 for full schedule of the 2019/2020 Internet drills.
[18] As mentioned earlier, they are called "Developments in the field of information and telecommunications in the context of international security", see Footnote 1.
[19] "Developments in the field of information and telecommunications in the context of international security," Committee Report A/53/5764, UN General Assembly, January 1999, https://digitallibrary.un.org/record/265311?ln=en.
[20] Valdai Discussion Club Meeting Transcript, Kremlin News, 22 October 2020, http://kremlin.ru/events/president/news/64261.
[21] Report on the working meeting between the Secretary of the Security Council of the Russian Federation Nikolai Patrushev with Assistant to the President for National Security Affairs Patrick O'Brien, News and Information, Russian Federation Security Council, 2 October 2020, http://www.scrf.gov.ru/news/allnews/2848/.
[22] Lavrov, S.V., "Global Cybersecurity Issues and Russia's International Initiatives for Fighting Cybercrime", *Vneshneekonomicheskie svyazi [International Economic Relations]*, 28 September 2020, https://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4350978

On 25 September 2020, President Putin issued a statement[23] "on a comprehensive program of measures for restoring Russia-US cooperation in the field of international information security," which states, among other things that "One of today's major strategic challenges is the risk of a large-scale confrontation in the digital field. A special responsibility for its prevention lies with the key players in the field of ensuring international information security."

On 22 September 2020, President Putin addressed the United Nations 75th General Assembly, and said[24] the following on the subject of cybersecurity: "However, just like any other innovation, digital technologies tend to spread uncontrollably and, just like conventional weapons, can fall into the hands of various radicals and extremists not only in the regional conflict zones, but also in quite prosperous countries, thus engendering enormous risks. In this regard, matters related to cybersecurity and the use of advanced digital technology also deserve a most serious deliberation within the United Nations. It is important to hear and appreciate the concerns of people over the protection of their rights, such as the right to privacy, property and security, in the new era."

On 18 September 2020 Vladimir Shin[25] said in an interview aired on CCTV (China Central Television), "Crucially, our joint efforts led to the creation of the first universal negotiation mechanism – the Open-ended Working Group on international information security at the UN. We expect the international community to be able to develop concrete solutions to establish 'rules of the road' in the information space in the coming years."[26]

On 17 September 2020, during the 10th High-Level Brazil, Russia, India, China, and South Africa (BRICS) Meeting of Security Representatives, special attention was paid to the issue of providing security in the area of Information and Communications Technologies (ICT). The importance of developing unified approaches to these problems was raised during the discussion.[27]

In the 16 September 2020 video address[28] at the meeting of the Security Council Secretaries of the member states of the Shanghai Cooperation Organization (SCO), Mr. Vladimir Norov (Secretary-General of the SCO) said that to ensure cybersecurity "…more attention is required to enhance the coordination of the relevant positions of the SCO member states on a common multilateral platform."

---

[23] "Statement by President of Russia Vladimir Putin on a comprehensive program of measures for restoring the Russia – US cooperation in the field of international information security," Kremlin News, 25 September 2020, http://en.kremlin.ru/events/president/news/64086

[24] "Vladimir Putin delivered a pre-recorded video address to the 75th anniversary session of the United Nations General Assembly," Statement, Kremlin News, 22 September 2020, http://en.kremlin.ru/events/president/news/64074

[25] Vladimir Shin is Deputy Director of the Department of International Information Security of the Russian Ministry of Foreign Affairs

[26] V.A.Shin, Deputy Head of the Department of International Information Security of the Ministry of Foreign Affairs of Russia, responding to the China Central Television (CCTV) correspondent, (Moscow, 18 September 2020), Russian Ministry of Foreign Affairs, 21 September 2020, https://www.mid.ru/web/guest/publikacii/-/asset_publisher/nTzOQTrrCFd0/content/id/4342420.

[27] "10th Meeting of BRICS National Security Advisors", Russian Federation Security Council, 17 September 2020, http://www.scrf.gov.ru/news/allnews/2842/

[28] "Review of SCO Secretary-General's speech at the 15th meeting of Security Council Secretaries of SCO Member States," Shanghai Cooperation Organization, 16 September 2020, http://eng.sectsco.org/news/20200916/677622.html.

On 15 September 2020 during the SCO Security Council Secretaries' meeting "the importance of developing, under the UN auspices, of universal rules, norms and principles of states' responsible behaviour in the information space as well as a legally-binding counter-cybercrime instrument was reaffirmed."[29]

On 11 September 2020 the joint statement of foreign ministers of Russia and China mentioned that both sides "also underscore common positions on internet governance, including the importance of ensuring the equal rights of states to govern the global network, and emphasise the need to enhance the role of the International Telecommunication Union (ITU) in this context."[30]

On 7 September 2020, Andrey Krutskikh,[31] addressing an OSCE conference on cybersecurity, noted,[32] "...countries need to secure their digital sovereignty, ensure safe operation of an integrated telecommunications network, and protect their critical infrastructure…" And also, "In the international arena, Russia consistently advocates for the establishment of professional and constructive cooperation in the field of international information security and the soonest possible development of rules, norms and principles of responsible behavior of states in cyberspace. That can only be achieved through the unique universal platform – the United Nations."

On 12 August 2020 Deputy Chair of the Russian Security Council, D.A. Medvedev,[33] said[34] on his official Facebook page,[35] during a virtual call[36], and as quoted in the accompanying note on Facebook: "At this time the U.S. fully controls the Domain Name System used to resolve IP-addresses. That's how it happened historically, but simply and bluntly put, it shouldn't be this way." He also added, "Taking into consideration the urgency of the problem, it is necessary to speed up the discussion of common approaches to the Internet governance system at the international level, including at the UN."

[29] Russia Chaired the Remote Fifteenth Meeting of the Secretaries of Security Councils of the Members of Shanghai Cooperation Organization, Russian Federation Security Council, 15 September 2020, http://www.scrf.gov.ru/news/allnews/2838/.

[30] "Joint Statement by the Foreign Ministers of the Russian Federation and the People's Republic of China, Moscow," Russian Federation Ministry of Foreign Affairs, 11 September 2020, https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4335948?p_p_id=101_INSTANCE_cKNonkJE02Bw&_101_INSTANCE_cKNonkJE02Bw_languageId=en_GB.

[31] Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security.

[32] "Statement by Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security Andrey Krutskikh at the International OSCE Conference on Cybersecurity," Russian Federation Security Council, 15 September 2020, https://osce.mid.ru/web/osce-en/-/statement-by-special-representative-of-the-president-of-the-russian-federation-for-international-cooperation-in-the-field-of-information-security-andr.

[33] Dmitry Medvedev is former Prime Minister and former President of the Russian Federation.

[34] Meeting on Establishing Equality for Parties Involved in Internet Governance, video recording of Dmitry Medvedev's statement, 12 August 2020, https://www.facebook.com/watch/?v=617263725858982.

[35] See Appendix 4 for full transcript

[36] Titled "Meeting on Establishing Equality for Parties Involved in Internet Governance".

Also worth mentioning is the press release[37] issued at the end of the bilateral interagency consultations on cyber between Russia and France[38] on 18 November 2019, which says that the Russian and French ambassadors "stressed the need to develop international cooperation in this domain, first of all within the framework of the United Nations (UN). The sides noted the importance of ensuring the uninterruptedness and continuity of the negotiation process on international security in the field of [information and communications technologies] ICT under the auspices of the UN, both within the Open-ended Working Group and the Group of Governmental Experts…"

# Conclusion

The Russian Federation has had a tradition of proposing cyber-related resolutions at the United Nations, dating back to 1998. The above quoted statements demonstrate Russia's increasing frequency, over the years, of raising cyber-related issues internationally, at the United Nations and other intergovernmental organizations (IGOs) where cyber-related discussions are taking place.

ICANN org, through its Government Engagement team, will continue to provide information to the ICANN community when such statements or proposals touch on the technical governance of the Internet or ICANN's mission.

[37] "Press Release on the Outcome of the Russian-French Interagency Consultations on International Security in the Field of Information and Communication Technologies (ICT) (Moscow, November 15, 2019)," Russian Federation Ministry of Foreign Affairs, 18 November 2019, https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3904684.

[38] Report on the Russian-French Interagency Consultations on International Security of Information and Communication Technologies, 26 August 2020, French Embassy in Moscow, https://ru.ambafrance.org/Ob-itogah-rossijsko-francuzskih-mezhvedomstvennyh-konsul-tacij-po.

# Appendix 1
## DNS-related Provisions of the Sovereign Internet Law

"Article 14.2. Ensuring Sustainable and Safe Use of Domain Names within the Russian Federation"[39] (excerpts).

"1. In order to ensure sustainable and safe use of domain names in the Russian Federation, a national domain name system is being created, which is a combination of interconnected software and hardware designed for storing and retrieving information about network addresses and domain names."

"2. The regulation defining the national domain name system, the requirements, the procedure for creating it, for generating the information contained in it, as well as the rules for its use, including the conditions and procedures for providing access to information, are determined by the federal executive government body responsible for mass media, mass communications, information technologies and communications oversight and control."

"3. The federal executive government body responsible for mass media, mass communications, information technologies and communications oversight and control [40], determines the list of groups of domain names that constitute the Russian national top-level domain."

"4. Coordination of the creation of domain names that are part of the groups of domain names that constitute the Russian national top-level domain is carried out by a non-profit organization, of which the Russian Federation is one of the founders, and which is the registered with international organizations for the distribution of network addresses and domain names as the owner of the databases holding information about this top-level domain. On behalf of the Russian Federation, the functions and powers of the founder are carried out by the federal executive government body responsible for mass media, mass communications, information technologies and communications oversight and control."

[39] Russian Federal Law, "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'".
[40] For a description of Roskomnadzor's remit, see: "On The Federal Service for Communications, Information Technologies and Mass Communications Oversight", Decree No. 228, 16 March 2020, http://rkn.gov.ru/about/.

# Appendix 2
## Regulations Governing Implementation

The decrees of the Russian Government provide details on the Sovereign Internet Law amendments by -

1. Tasking the MoC to develop procedures to implement regulations on:
   a) Internet resilience to threats to its stability, security and functioning within Russia.
   b) Ensuring the functioning of Internet exchange points [subject to coordination with the Federal Security Service (FSB)].
   c) Requirements for the ISPs that have a unique identifier for the aggregate means of communication and other technical equipment connected to the Internet (hereinafter – AS number holders) covering the reliable functioning of the means of communication used to connect to other ISPs and proprietors or other owners of communication networks, including those abroad.
   d) Rules for the ISPs holding an AS number covering the functioning of hardware and software (including means of communication) used to identify internet network addresses corresponding to domain names.
   e) Rules covering support by networks and owners of the means of communication or other owners of public communications networks that have autonomous system numbers, of law enforcement intelligence or national security operations (subject to coordination with law enforcement intelligence or national security authorities);[41]

2. Authorizing Roskomnadzor
   - ***To oversee and control:***
   f) The centralized administration of public communications networks and the Internet by passing down orders to be executed by: ISPs, proprietors or other owners of public communications networks, internet exchange points, connection lines crossing the Russian Federation border (hereinafter – transborder connection lines), parties that disseminate of information on the Internet that are AS number holders or other parties with this number.
   g) The coordination of a stability, security, and integrity of the functioning of the Internet within Russia.
   h) Granting to the ISPs a free-of-charge technical equipment for countering threats to the stability, security, and functioning of the Internet and public communications networks within Russia.
   i) Informing ISPs (proprietors or other owners of public communications networks, internet exchange points, transborder connection lines, parties that disseminate information on the Internet that are AS number holders or other parties with this

[41] See points 5.2.25(24) – 5.2.25(28) here: Russian Federation, "Decree On the Ministry of Digital Development, Communications, and Mass Media", Decree No. 418, http://www.consultant.ru/cons/cgi/online.cgi?from=344975-28&rnd=635D454F0459377425C6760CF334CA25&req=doc&base=LAW&n=362130&REFDOC=344975&REFBASE=LAW#55adl94r1cc.

number) in case the stability, security and functioning of the Internet or public communication networks are under threat.

j) Monitoring the functioning of the Internet and public communications networks to identify threats to the stability, security, and functioning of these networks within the Russian Federation.

- ***as well as to establish:***

**k)** the accountability procedures for the ISPs (or other owners of public communications networks, proprietors or other owners of internet exchange points, proprietors or other owners of transborder connections lines or other AS number holders) that are responsible for providing information to Roskomnadzor about transborder connection lines and their communication with other connection lines, the purposes for using these connection lines, the means of communication installed on these connection lines, and the cooperation procedures of the owners of these communication lines that are AS number holders, with law enforcement intelligence authorities.

l) routing rules for electronic communication transmissions in case centralized management of public communication networks is introduced.

m) the procedure for verifying the accuracy and entirety of information provided by ISPs, proprietors and other owners of transborder connection lines, about the purposes for using these connection lines and the means of communication installed on these connection lines.

n) the procedure for verifying compliance by the ISPs (proprietors and other owners of public communication networks, parties that disseminate information on the Internet and that are AS number holders**)** with the requirement to use internet exchange points listed in the registry of internet exchange points for the purposes of communicating with ISPs (proprietors and other owners of public communication networks or other parties) for electronic transmissions.

o) the procedure for verifying compliance by owners or other title holders of internet exchange points with the ban on connecting to internet exchange points on the communication networks, whose their owners do not comply with the Federal Law “On Communication”; a requirement to assist law enforcement with access to the networks and the means of communication, including autonomous systems, if the system has a number, a ban on disclosing undercover and investigative activity carried out by law enforcement agencies.

p) the list of groups of domain names constituting the Russian national top-level domain.

q) the national domain name system, requirements for it, the procedure for creating it, including the procedure for organizing information contained wherein, as well as rules governing its use, including the conditions and process for granting access to the information.

r) the regulation governing the verification by the Center for Monitoring and Administering Public Communication Network within the Radio Frequency Service of ISP compliance with the requirement to install technical equipment for

countering threats to the stability, security and functioning of Internet within Russia and to public communication networks, to disclose, within 3 days, information about the exact installation location of this equipment, and to satisfy the technical parameters of such equipment and communication networks. The Center may also act as centralized administrator of public communication networks if there are threats to the stability, security and functioning of the Internet and public communication networks in Russia;

s) technical specifications for installing technical equipment for countering threats to the stability, security, and functioning of the Internet and public communications networks within the Russian Federation, as well as requirements for the communication networks when they use this technical equipment.

t) Requirements for the technical equipment used to verify the compliance of ISPs, proprietors and other owners of public communications networks with the federal laws "On Communications" and "On Information, Information Technologies and Information Protection."[42]

3. The following government and Roskomnadzor decrees were issued in support of legislation mentioned above:
   u) The accountability procedure for owners of transborder connection lines, ISPs, automatic system numbers, and other "subjects."[43]
   v) Russian national top-level domains .RU; .РФ; .SU, as well as other TLDs managed by legal entities registered in Russia that are registered with international organizations for the distribution of network addresses and domain names as owners of the databases holding information about these top-level domains).[44]
   w) Procedures for Internet drills.[45]
   x) Rules and procedures for an internet exchange points registry.[46]
   y) Changes to the regulations governing the Radio Frequency Service.[47]

[42] Russian Federation, "On Amendments to the Regulation Governing the Federal Service for Communications, Information Technologies and Mass Communications Oversight", Decree No. 1234, 21 September 2019, http://publication.pravo.gov.ru/Document/View/0001201909250005?index=0&rangeSize=1.
[43] Roskomnadzor, "On Communications", Order 217, 29 July 2019 (Published 1 November 2019), http://publication.pravo.gov.ru/Document/View/0001201911010028?index=0&rangeSize=1.
[44] Roskomnadzor, "List of Groups of Domain Names Constituting Russia's National Top-Level Domain", Order No. 216, 29 July 2019, http://publication.pravo.gov.ru/Document/View/0001201908210010?index=2&rangeSize=1.
[45] Russian Federation, "Decree to Adopt the Regulations Covering Exercises in Support of Stability, Security and Integrity of the Functioning of the Internet and Public Communications Network within the Russian Federation", Decree No. 1316, 12 October 2019, http://publication.pravo.gov.ru/Document/View/0001201910210025?index=0.
[46] Russian Federation, "Decree to Adopt the Rules Governing the Maintenance of the Registry of Internet Exchange Points", Decree No. 1311, 12 October 2019, http://publication.pravo.gov.ru/Document/View/0001201910210026?index=0.
[47] Russian Federation, "On Amendments to Item 5 of the Regulations Governing the Radiofrequency Service", Decree No. 1148, 3 September 2019, http://publication.pravo.gov.ru/Document/View/0001201909050018?index=0.

z) Procedures governing the interaction between ISPs, proprietors and other owners of public communications networks that hold AS numbers, and law enforcement intelligence gathering and national security authorities.[48]

aa) Procedures for monitoring the deployment of the means of communication within Russia by persons involved in centralized management of public communications networks.[49]

bb) Draft procedure for centralized management of public communications networks; includes definitions of threats.[50]

cc) Draft procedure for installing on communication networks the technical equipment designed for countering threats; the text of the decree is being sent for final approval to the government.[51]

MoC and Roskomnadzor regulations provide further details regarding the sovereign internet –

dd) MoC – development of requirements for DNS software and hardware.[52]

ee) MoC – development of draft requirements for internet exchange points.[53]

ff) Roskomnadzor – procedure for verifying compliance with the requirement to use internet exchange points listed in the registry.[54]

---

[48] Russian Federation, "Decree to Adopt the Rules Governing Communication Between Proprietors or Other Owners of Communication Networks and Holding AS Numbers, and Authorized Government Law Enforcement Intelligence and National Security Operations", Decree No. 1385, 29, September 2020, http://publication.pravo.gov.ru/Document/View/0001201911010006?index=0.

[49] Russian Federation, "Decree on Enforcement of the Obligations Assigned to Parties Involved in Centralized Management of Public Communications Network Relating to Installing within the Russian Federation the Means of Communication Used to Carry Out Instructions for Centralized Management of the Public Communications Network", Decree No. 1375, 26 October 2019, http://publication.pravo.gov.ru/Document/View/0001201911010011?index=0.

[50] Russian Federation, "Decree to Adopt Procedures of Centralized Management of Public Communications Network", Draft Decree, Federal Legal Information Portal: https://regulation.gov.ru/projects#npa=91558

[51] Russian Federation, "Decree to Adopt Procedures Governing the Installation, Operation and Upgrades On an ISP's Communications Network of Technical Equipment for Countering Threats to Stability, Security and Integrity of Operation of the Internet and of the Public Communications Network within the Russian Federation", Draft Decree, Federal Legal Information Portal: https://regulation.gov.ru/projects#npa=91945

[52] Ministry of Digital Development, Communications and Mass Media, "Order to Adopt Requirements Governing the Functioning of Hardware and Software (including means of communication), Used to Match Network Addresses with Domain Names on the Internet", Order No. 510, 16 September 2019, http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=342312&fld=134&dst=100001,0&rnd=0.746375104687729#07031038076827105.

[53] Ministry of Digital Development, Communications and Mass Media, "Decree to Adopt Requirements Governing the Functioning of Internet Exchange Points, Including Requirements for Ensuring Stable Functioning of Hardware and Software Means of Communication and Communication Facilities", https://regulation.gov.ru/projects#npa=91675

[54] Roskomnadzor, "Order to Adopt the Procedure for Verifying Compliance by ISPs, Proprietors and other Owners of Communication Networks, Parties that Disseminate Information on the Internet that Hold an AS number, with the Requirement to Use Internet Exchange Points Registered with Internet Exchange Point Registry, for Communicating with ISPs, Proprietors or Other Owners of Communication Networks and other Parties, Holding an AS number, for

gg) Roskomnadzor – Procedure for verifying accuracy and entirety of information about the purpose of using transborder connection lines.[55]

hh) Roskomnadzor – Procedure for verifying compliance with the ban on connecting to internet exchange points, whose owners fail to satisfy requirements defined by the laws of the Russian Federation.[56]

ii) Roskomnadzor – Order to report information by ISPs and other owners of automated system numbers about the technical equipment used to connect to transborder connection lines, including connections across other connection lines.[57]

jj) Roskomnadzor – Order to report information about the purpose for using transborder communication lines by the ISPs and other owners of the means of communication.[58]

kk) Roskomnadzor – Order to report information about the purpose of using transborder connection lines by the proprietors or other owners of the transborder connection lines.[59]

ll) Roskomnadzor – Regulations governing the routing of electronic transmissions in the event of centralized management of public communication network.[60]

---

the Purposes of Sending Electronic Transmissions", Order No. 226, 31 July 2019, http://publication.pravo.gov.ru/Document/View/0001201911080016?index=0

[55]Roskomnadzor, "Order to Adopt the Procedures for Verifying Accuracy and Entirety of Information Provided by Proprietors or Owners of Connection Lines the Purposes of Using Transborder Connection Lines, As Well As About the Means of Communication Installed on These Lines, Order No. 227, 11 July 2019, http://publication.pravo.gov.ru/Document/View/0001201911080047?index=0.

[56]Roskomnadzor, "Order to Adopt the Procedure for Verifying Compliance by Proprietors or Other Owners of Internet Exchange Points of the Ban on Connecting to Internet Exchange Points of Communications Networks Whose Owners Do Not Comply with the Requirements Defined by the Laws of the Russian Federation", Order No. 219, 31 July 2019, http://publication.pravo.gov.ru/Document/View/0001201911080006.

[57]Roskomnadzor, "Order to Adopt Deadlines, Procedures, Elements and Format of Information Provided Digitally by ISPs, Proprietors and Other Owners of Communication Networks, Parties that Disseminate Information on the Internet, as well as by Other Parties that Hold AS Numbers, as Required by Subitem 4 of Item 8 of Article 56.2 of the Federal Law "On Communications" No. 126-ФЗ, 7 July 2003,", Order No. 221, 31 July 2019, publication.pravo.gov.ru/Document/View/0001201911110028?index=0.

[58]Roskomnadzor, "Order to Adopt Dates, Procedures, Elements and Format of Information Provided Digitally by ISPs, Proprietors and Other Owners of Communication Networks and Other Parties, When Using Transborder Connection Lines, about the Means of Communication Used to Connect with These Connection Lines, Including Cases of Connections Across Other Connection Lines", Order No. 222, 31 July 2019, http://publication.pravo.gov.ru/Document/View/0001201911110024.

[59]Roskomnadzor, "Order to Adopt Dates, Procedures, Elements and Format of Information Provided Digitally by Proprietors or Other Owners of Transborder Connection Lines About the Purposes of Using the Connection Lines as well as about the Means of Communication Installed on That Connection Line", Order No. 223, July 31 2019, http://publication.pravo.gov.ru/Document/View/0001201911110033?index=0.

[60] Roskomnadzor, "Order to Adopt Rules Governing the Routing of Electronic Transmissions in Case Centralized Management of Public Communications Network is Deployed", 31 July 2019, Order No. 224, http://publication.pravo.gov.ru/Document/View/0001201911060018.

mm) Roskomnadzor – Decree to approve the establishment of a Center for Monitor and Administer a Public Communication Network.[61]

nn) Roskomnadzor – Order to develop procedures for providing equipment capable of limiting access to information and for defining technical specifications for this equipment, its installation and operation.[62]

oo) Roskomnadzor – Regulations regarding the National Domain Name System.[63]

pp) Roskomnadzor – Order to adopt technical requirements for installing technical equipment for countering threats, as well as requirements for communications networks using technical equipment for countering threats.[64]

[61] Roskomnadzor, "Order to Adopt the Regulation Governing the Center for Monitoring and Administering Public Communications Network", Order No. 225, 31 July 2019, http://publication.pravo.gov.ru/Document/View/0001201911250011.

[62] Roskomnadzor, "Order to Adopt the Procedure for Providing to ISPs, Proprietors or Other Owners of Communications Networks that are AS Number Holders, Technical Equipment for Verifying Compliance by Said Parties with the Requirements of the Federal Law "On Information, Information Technologies and Information Protection" and "On Communications", Limiting Access to Information, Including Requirements Covering These Types of Technical Equipment, Their Installation and Operation", Order No. 220, 31 July 2019, http://publication.pravo.gov.ru/Document/View/0001201911120025?index=0.

[63] Roskomnadzor, "Order to Adopt the Regulation Governing a National Domain Name System, Requirements For It, As Well As Rules for Using It, Including Terms and Procedures for Providing Access to Information", Order No. 229, 31 July 2019, http://publication.pravo.gov.ru/Document/View/0001201911080052?index=0.

[64] Roskomnadzor, "Order to Adopt Technical Requirements for Installing Technical Equipment for Countering Threats, as well as Requirements for Communications Networks Using the Technical Equipment for Countering Threats", Order No. 228, 31 July 2019, http://publication.pravo.gov.ru/Document/View/0001201909120028.

# Appendix 3
# List of Internet Drills 2019/2020

| Threat | Date of the drill | Status |
|---|---|---|
| Communication sustainability and security of cellphone communications, Internet of Things (IoT) security | 23 December 2019 | Completed |
| Development of capabilities for blocking Internet traffic encrypted with DoH and DoT | 20 March 2020 | Rescheduled (due to COVID-19)[65] |
| Mitigating threats to stable operation of the network due to interruptions of service in parts of the network and due to external destabilizing natural or manmade events | 20 June 2020 | Rescheduled (due to COVID-19)[66] |
| Development of instruments for countering threats that exploit the vulnerabilities of the Narrowband Internet of Things (NB-IoT) networks | 20 September 2020 | Not carried out (legislation not finalized)[67] |
| Development of tools for countering attacks that exploit BGP protocol vulnerabilities | 20 December 2020 | Pending |

[65] "Runet Resilience Drills Postponed Due to Coronavirus", *Interfaks*, 20 March 2020, https://www.interfax.ru/russia/700060.
[66] "MoC Has Again Postponed the RUNET Resilience Drill", *TASS*, 19 June 2020, https://tass.ru/ekonomika/8774051.
[67] "Ministry of Digital Development, Communications and Mass Media Did Not Hold Runet Resilience Drill on September 20", *TASS*, 21 September 2020, https://tass.ru/ekonomika/9507051.

# Appendix 4
# Unofficial transcript of Dmitry Medvedev's statement during his virtual meeting with FSB, GRU and MoC.[68]

Today we are going to address an issue which is not new and definitely not easy. The worldwide web today is what it is – it is the foundation that has shaped development across the globe, further demonstrated during the time when we all started dealing with the crisis caused by the coronavirus infection. Information technology has always played and will continue to play an enormous role in ensuring our country's national security. It is quite understandable that a host of countries, and above all the United States, are seeking to use the Internet as their fiefdom – in other words, as a tool for attaining solely their goals. Let me remind you that the U.S. fully controls the Domain Name System used to resolve IP-addresses. That's how it has happened historically, but simply and bluntly put, it shouldn't be like that. Suffice it to recall the latest decisions by the current U.S. administration, the Trump administration, concerning owners of social networks – it all shows that the United States intends to continue to pursue its own policy online and as they do so – to interpret companies' and countries' decisions solely from the standpoint of the United States' national interests, while disregarding international competition and any international regulations currently in effect. Naturally, they seek to ensure the competitiveness of American businesses, to address the country's internal issues like the upcoming elections. They also pursue their geopolitical challenges. Therefore, this kind of behavior, demonstrated by the United States and some of their partners, proves that against this background, neither Internet users nor businesses nor governments can be sure that their interests will be duly protected – which is why equal rights should be ensured. Let me remind you that a few years ago (in an incident unrelated to the Internet), the United States, in an effort to exert pressure on our country, was discussing how to cut Russia off from the payment verification system or SWIFT; it is currently the People's Republic of China that is subjected to the same rather significant amount of pressure. Some of these sanctions, some of these tools for exerting pressure are related to the Internet. And that is why we should be very well prepared for these types of decisions moving forward, where they may obviously involve the World Wide Web. Let me remind you that Russia has adopted a special piece of legislation aimed at creating a national system for routing network traffic, which should protect the Russian Internet resources in case they are attacked. We believe that nations should have the right to govern their information space independently because it is one of the characteristics of sovereignty. We should work towards that, and not within the country – we should work on the international level, which raises a range of issues that I suggest we discuss. Russia has been consistently advocating for many years for equal participation of all nations in Internet governance; the appropriate approaches were incorporated in the Safe Internet Framework Paper developed by the Ministry of Communications. The document includes breakthrough approaches to ensuring security and stability of the World Wide Web; and yet, all our numerous appeals and proposals have not met with the requisite response on the international arena. Some time ago our partners at BRICS and at the Shanghai Cooperation Organization cautiously mentioned the idea of establishing a special UN convention, which might be the first yet necessary step. Obviously all parties agree that equal participation of governments in Internet governance is necessary because the Internet is a tool for ensuring national security – it is no longer just a network created for scientific, military purposes or for fun. This view has been

[68] "Meeting on Establishing Equality for Parties Involved in Internet Governance", Transcript, Video recording of Dmitry Medvedev's statement, 12 August 2020, https://www.facebook.com/watch/?v=617263725858982

reflected in a number of decisions made at Summits of Heads of BRICS and SCO member states. Still, taking into consideration the urgency of the issue and the recent developments, some of which I have already mentioned, there is a need to update the draft framework paper developed by our country and arrange to discuss it in various formats at international fora. We need new momentum to ensure the governments' sovereign right to engage in internet governance in the domestic information space