

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

Post-November 2020 Policy Initiatives

Veni Markovski
Alexey Trepukhalin
29 April 2021
Updated 7 May 2021
GE-007



TABLE OF CONTENTS

Introduction	3
Russian Cyber- and Internet-Related Foreign Policy Statements and Initiatives	3
Russian Internet-Related National Policy Statements and Initiatives	9
Conclusion	11

Introduction¹

A previous paper from ICANN organization's Government Engagement team focused on Internet-related policy statements by the Russian Federation through the end of October 2020.² Since then, a number of Russian officials have made statements and taken actions which touch on ICANN's mission. This paper is an update covering the period from 24 October 2020 to 21 April 2021. The first part looks at Russian Cyber- and Internet-related foreign policy statements and initiatives, and the second part looks at the Internet-related national policy statements and initiatives. As per usual, we are only mentioning those statements that touch on ICANN's mission, and not any other Internet-related issues announced over this period.

Russian Cyber- and Internet-Related Foreign Policy Statements and Initiatives

On 24 October 2020, the Deputy Chairman of the Russian Security Council Dmitry Medvedev said that the "U.N. structures could become a platform for the adoption of a universal international treaty based on generally recognized principles and norms of international law and meeting common interests in the information sphere."³

On 10 November 2020 at the Internet Governance Forum (IGF) Parliamentary Roundtable session, Alexander Khinsein, Chairman of the State Duma Committee on Information, Information Policy, Information Technologies, and Communication (Committee on Information) told the audience that the Russian Federation has put forward a "General Assembly resolution on the counteracting of information technologies to commit crime".⁴ He mentioned that the cybercrime convention draft text is widely distributed at the U.N.,⁵ and recommended the participants to "consider" this "draft document" which could become a catalyst "for the development of unified methods to fight against internet technologies, as well as cybercrime".⁶

On 17 November 2020, the Deputy Minister of Digital Development, Communications, and Mass Media (MoC) Maxim Parshin said during the closing session of the IGF: "There are new challenges. First of all [among them] are questions related to Internet security, personal data protection, fakes, and disinformation. It would be fair to ask in this connection: Can the existing Internet governance system cope with these threats, provide a proper answer to these global challenges? We are confident that it must be based on the principles of mutual trust, and guarantee security, while observing fundamental human freedoms, under equal

¹ This paper has been updated to correct errors and to reflect new information

² "Country Focus Report: Russian Federation Internet-Related Laws and United Nations Deliberations", *GE Publications*, ICANN, 19 January 2021, <https://www.icann.org/en/system/files/files/ge-006-19jan21-en.pdf>

³ Dmitry Medvedev "75 Years UN - old problem, new challenges and global solutions", *Russia Today*, 24 October 2020, <https://russian.rt.com/world/article/795600-dmitrii-medvedev-oon-75-let>

⁴ Alexander Khinsein, Chairman of the State Duma Committee on Information, *IGF 2020*, presentation at the Parliamentary Round Table (English), 10 November 2020, <https://www.youtube.com/watch?v=NuBY0hifiQs> (49:00)

⁵ V. Nebenzia, "Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General" *A/C.3/72/12*. 16 October 2017, <https://undocs.org/A/C.3/72/12>

⁶ Alexander Khinsein, Chairman of the State Duma Committee on Information, *IGF 2020*, presentation at the Parliamentary Round Table (English), 10 November 2020, <https://www.youtube.com/watch?v=NuBY0hifiQs> (50:00)

rights of states to manage the critical Internet resources. In connection with this, we think it is important to develop a global pact, a global document, that would, among others: clearly distribute roles and responsibility of states, society, and technology companies, define a unified approach to security, rights and freedoms, and personal data protection, as well as measures for fighting disinformation that is coming primarily through social media and messengers. We suggest defining a body within the U.N. framework that would be responsible for developing and implementing legal norms and standards in the area of Internet governance. The International Telecommunication Union (ITU) could become such a body. It is important to note that since its founding, the role of the IGF has been limited to that of a discussion venue; it does not adopt decisions. That is why we suggest that we need to focus on developing mechanisms that would make it possible to change the results of its work in such a way as to make its decisions not purely declarative. We think that this would make the IGF more effective. In conclusion I want to say that Russia has received official U.N. confirmation that it will host the anniversary edition of IGF 2025. This is a great honor for us, and we aim to ensure all stakeholders participate in this Forum.”⁷

On 22 November 2020 in Minsk, during a joint meeting of the leadership teams of the foreign ministries of the Russian Federation and Belarus, the Russian Minister of Foreign Affairs, Sergey Lavrov said in his speech, “Traditionally, international information security is on the agenda.⁸ Recent international developments have clearly shown the importance of cooperation on this matter of all countries without exception, rather than a select few. Clearly, without universal agreements, the world risks plunging into cyber chaos fraught with catastrophic consequences. It is amid a cyberwar supported from outside that illegal subversive activities start to flourish, and information and communication technology is used for criminal purposes. It is important to continue to jointly uphold our approaches in this sphere at multilateral platforms, in regional mechanisms and bilateral formats. We note the well-coordinated interaction of the delegations of Russia and the Republic of Belarus during the start of the U.N. Open-Ended Working Group on International Cybersecurity and an ad hoc U.N. committee of experts to draft a convention on combating cybercrime. We are also working on the text of a Joint Statement of the CIS Heads of State on this subject.”⁹

On 18 December 2020, the Commonwealth of Independent States (CIS) countries signed a statement on cooperation around international information security. In it, they stressed the need to adopt a U.N. cybercrime convention and acknowledged the importance of “developing cooperation on issues related to the use and management of national segments of the Internet” and singled out “the need to expand the role of the ITU in this context.”¹⁰

On 12 January 2021, the ITU published a contribution from the Russian Federation to the ITU Council Working Group on Child Online Protection (CWG-COP). The proposal suggested that the CWG-COP arrange discussion of issues related to implementation of

⁷ Maxim Parshin, Deputy Minister of the Ministry of Digital Development, Communications and Mass Media (MoC). IGF 2020 High-Level Leaders Track: UN Wrap-up, 17 November 2020, <https://youtu.be/3GxCREczsko?t=1292> (21:32 in Russian).

⁸ The Russian Federation usually uses the term “information security” in their documents; others use “cybersecurity”.

⁹ Foreign Minister Sergey Lavrov’s opening remarks at a joint meeting of the leadership teams of the foreign ministries of the Russian Federation and the Republic of Belarus, Minsk, November 26, 2020. Ministry of Foreign Affairs (MFA website), 26 November 2020, https://www.mid.ru/ru/integracionnye-struktury-prostranstva-sng/-/asset_publisher/r17Fzr0mbE6x/content/id/4460580?p_p_id=101_INSTANCE_r17Fzr0mbE6x&_101_INSTANCE_r17Fzr0mbE6x_languageId=en_GB

¹⁰ “CIS Heads Adopt a Joint Statement on Cooperation in the Area of International Information Security”. CIS Internet Portal, CIS News, 18 December 2020, <https://e-cis.info/news/564/89858/>

Encrypted Server Name Indication (ESNI), DNS over HTTPS (DoH), and DNS over TLS (DoT) Internet encryption protocols enabling the concealment of name (identifier) of an Internet resource in CWG-COP.¹¹

On 14 January 2021, the ITU published two contributions from the Russian Federation for the upcoming meeting of the ITU Council Working Group on international Internet-related policy issues (CWG-Internet).¹² The proposals were similar and introduced the Russian Federation's suggestion that the ITU CWG-Internet should hold open consultations with all stakeholders, as suggested: "The current status of the global governance system for management and development Internet resource, including Internet domain names and addresses and critical Internet infrastructure and possible ways to overcome the challenges associated with dependence on the decisions of one national administration for further building an independent, democratic and equidistant from all states Internet governance system." In response to requests from the ICANN community, ICANN organization's Government Engagement (GE) team emailed comments on these three proposals to the ICANN Engagement Group on Internet Governance (EGIG) mailing list.¹³

On 15 January 2021, Maria Zabolotskaya mentioned the work of the OECE¹⁴ in her official address to the U.N. General Assembly (UNGA): "The level of threat posed by cybercriminals increased manifold during the pandemic, which proves global relevance of this task. Proceeding from this, Russia attaches special importance to the soonest launch of full-fledged activity of the ad hoc committee on elaboration of the convention as envisaged by UNGA resolution 74/247."¹⁵

During a press conference on 18 January 2021, Minister Lavrov mentioned the importance of "multilateral decisions" and expressed "hope that those who have tried for years and even decades to hinder discussions on making Internet governance more democratic, and those who have been putting spokes in the wheels of the Russian initiative set out in the U.N. General Assembly resolution on advancing responsible state behavior in cyberspace and in the draft Convention on Cooperation in Combating Cybercrime will see the problem in a different light, especially when it comes to more democratic internet governance". This "subject", he said, "has been under discussion for years at a specialized U.N. body, the International Telecommunication Union. Nearly all countries are willing to coordinate universally acceptable forms, but the Americans are categorically against this".¹⁶

¹¹ Contribution by the Russian Federation - Challenges generated by using encryption protocols on the Internet enabling concealment of name (identifier) of an Internet resource, CWG-COP, ITU website, 12 January 2021, <https://www.itu.int/md/S21-CLCWGCOP17-C-0004/en>

¹² Contribution by the Russian Federation - Proposal to CWG-Internet Open Consultations <https://www.itu.int/md/S21-RCLINTPOL15-C-0005/en>, Contribution by the Russian Federation - Role of ITU and ITU Member States in ensuring trust and security in the Internet at the international level, ITU website, 14 January 2021, <https://www.itu.int/md/S21-RCLINTPOL15-C-0006/en>

¹³ ICANN CCWG-IG mailing list, archives from January 2021: <https://mm.icann.org/pipermail/ccwg-internet-governance/2021-January/003899.html>

¹⁴ The full name is "Open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" as per UNGA resolution A/res/74/247. <https://undocs.org/en/A/RES/74/247>

¹⁵ Statement by representative of the Russian Federation Maria Zabolotskaya at the plenary meeting of the General Assembly under agenda item "Countering the use of information and communications technologies for criminal purposes". Permanent Mission of the Russian Federation to the UN, Permanent Mission website, 15 January 2021, <https://russiaun.ru/en/news/icts15012021>

¹⁶ Foreign Minister Sergey Lavrov's remarks and answers to media questions at a news conference on the results of Russian diplomacy in 2020, Ministry of Foreign Affairs (MFA) website, 18 January 2021.

On 26 January 2021, the Russian Federation and the Islamic Republic of Iran signed an intergovernmental agreement on cooperation in the cyber sphere.¹⁷ Ambassador Andrey Krutskikh¹⁸ commented on this document: “The agreement between Russia and Iran on information security envisions coordination of activities, exchange of technologies and training of specialists.”¹⁹ The document contains new and expanded definitions of the terms, “information infrastructure,” and “critical information infrastructure.”^{20 21}

On 26 January 2021, Ambassador Krutskikh told the press that “cooperation in the cyber sphere [...] is one of the priorities not only for us, but if you put away all the American ideology, for Washington as well. There are some signs that the USA will be interested in engaging in a dialogue with us soon.”²²

On 1 February 2021, Deputy Secretary of the Security Council Dmitry Medvedev said in an interview, “The Internet appeared at a certain time and without a doubt the key rights to manage [it] are with the United States of America.”²³

On 5 February 2021, Deputy Minister of Foreign Affairs Oleg Syromolotov stated in an interview that Moscow adheres to the “internationalization” of Internet governance and that “the existing Internet governance model, which has equalized the role of states that are the guarantors of rights and freedoms of their citizens and that play a major role in issues related to the economy, security and stability of the Internet’s critical information infrastructure, has shown its ineffectiveness a long time ago and does not guarantee the safety of Internet users, which is why it requires fundamental reform.”²⁴

At the Infoforum conference on 12 February 2021, Ernst Chernukhin, special coordinator at the Russian Ministry of Foreign Affairs on issues of political use of Information and Communication Technologies (ICT) and Head of Division, Department of International Information Security at the MFA, said, “the Russian Federation consistently speaks in favor

¹⁷ On Negotiations of the Minister of Foreign Affairs of the Russian Federation S.V. Lavrov with the Minister of the Foreign Affairs of Islamic Republic of Iran M.D. Zarif. Ministry of Foreign Affairs of the Russian Federation (MFA) website, 26 January 2021, https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4544717

¹⁸ Andrey Krutskikh is an ambassador and director of the Department of International Information Security at the Russian Ministry of Foreign Affairs, https://www.mid.ru/activity/shots/new_appointments/-/asset_publisher/2TDCzbl45VHK/content/id/4012794?p_p_id=101_INSTANCE_2TDCzbl45VHK&_101_INSTANCE_2TDCzbl45VHK_languageId=en_GB

¹⁹ MFA Discloses Details of Agreement between Russia and Iran on Information Security. *Izvestia*, 26 January 2021, <https://iz.ru/1116475/2021-01-26/mid-raskryl-detali-soglasheniia-irana-i-rossii-ob-informatcionnoi-bezopasnosti>

²⁰ “Agreement between the Government of the Russian Federation and the Government of the Islamic Republic of Iran on Cooperation in the Field of Information Security”. Ministry of Foreign Affairs, January 2021, <https://mddoc.mid.ru/api/ia/download/?uuiid=a514b469-da93-4f0c-8c2c-b6ad8a05ced3>

²¹ This sentence was updated to correct the previous version: “The document contains new and expanded definitions of the terms “critical infrastructure” and “critical information infrastructure.”

²² “MFA Describes the U.S. Interest in Cyber Cooperation”. *RIA Novosti*, 26 January 2021, <https://ria.ru/20210126/kibersfera-1594646999.html>

²³ Medvedev Called on the Users and Administrators of Social Media to be Polite with Each Other. *TASS Interview*, 31 January 2021 <https://www.youtube.com/watch?v=SPFf4d2FN4U> (starts at 7:15)

²⁴ “Deputy Minister of Foreign Affairs O.V. Syromolotov: Internet Has Become a Platform for Political Manipulations”. *TASS*, 5 February 2021, <https://tass.ru/interviews/10631379>

of internationalizing Internet governance and expanding the role of states in this process.”²⁵ He underlined that, within the U.N., Russia insists on “preserving the sovereign right of the states to regulate the national Internet segment, which is very important” and on developing “global governance policy at the intergovernmental level.”²⁶

On 24 February 2021, President Vladimir Putin stated, “A system for ensuring international information security needs to be developed jointly with our partners from other countries.”²⁷

On 8 March 2021, Minister of Internal Affairs Vladimir Kolokoltsev said in a speech that Russia supports “the central coordinating role of the U.N.” in fighting “global criminal challenges”. He also added that “Russia, as do many other countries, sees the development under the U.N. auspices of a universal convention to counter informational crime, as a solution. The document should include principles of sovereign equality and non-interference in the internal affairs of states.”²⁸

On 12 March 2021, Ambassador Krutskikh stated that the report of the [U.N.] Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG), created in 2018 [by the UNGA] upon Russia’s initiative, “represents a triumph of Russian diplomacy against the backdrop of escalation of the international situation by some countries.”^{29 30}

On 15 March 2021, the Russian MFA issued a statement on the OEWG’s final substantive report. It says that the report “enshrines basic approaches advanced by Russia and its partners in the area of international information security.”³¹

At a meeting of the Russian Security Council on 26 March 2021, President Putin said, “We believe it is necessary to conclude universal international legal agreements designed to prevent conflicts and build a mutually beneficial partnership in the global cyberspace.”³² He also added that “it is important to jointly develop and agree on universal and fair-for-all rules on the responsible behavior of states in the cyberspace with clear and easy-to-follow criteria for acceptable and unacceptable actions and to make them legally binding” and talked about Russia’s efforts within the U.N. on this issue.³³ Security Council Secretary Nikolai Patrushev

²⁵ Ernst Chernukhin, presentation at the 23rd Infoforum, Big National Forum for Information Security, Session Topic 1. Digital Security: New Challenges. Infoforum YouTube channel, streamed 12 February 2021, https://youtu.be/naN4_OglSFs?t=5015 (starts at 1:23:35)

²⁶ Ernst Chernukhin, presentation at Infoforum (1:24:18)

²⁷ Session of the FSB Collegium [*leadership of the Russian Federal security service*], Moscow. Kremlin website, 24 February 2021, <http://kremlin.ru/events/president/news/65068>

²⁸ “Vladimir Kolokoltsev, presentation at the XIV UN Congress on Crime Prevention and Criminal Justice, Ministry of Interior website, 8 March 2021: <https://mvd.rf/news/item/23344408>

²⁹ “Russia Says the UN OEWG Will Start its Work in June”. TASS, 13 March 2021, <https://tass.ru/politika/10895625>

³⁰ This sentence was updated to accurately reflect the original statement.

³¹ Press release, Update on the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, Ministry of Foreign Affairs (MFA) website, 15 March 2021, https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4632970

³² Security Council meeting, Novo-Ogaryovo, Moscow Region, Kremlin website, 26 March 2021, <http://en.kremlin.ru/events/president/news/65231>

³³ Security Council meeting, Novo-Ogaryovo, Moscow Region, Kremlin website, 26 March 2021, <http://en.kremlin.ru/events/president/news/65231>

announced that a new version of the Basic Principles of State Policy in International Information Security will be published later in 2021.^{34 35}

On 1 April 2021, Minister Lavrov said in an interview, “The United States categorically refuses to discuss the democratization of Internet governance and some kind of general rules that would regulate social media.”³⁶

On 6 April 2021, the Deputy Head of the Presidential Administration Sergey Kiriyenko said at the Youth Russian Internet Governance Forum, “We are moving to a stage, where norms and rules for global companies, users, and states involved in the development of Internet space are becoming more international. The international community will inevitably need to convene and agree on what these new rules should be.”³⁷

On 7 April 2021, the MoC announced that the Russian Federation's candidate for the Secretary-General³⁸ of the ITU is Rashid Ismailov.³⁹ This news was also announced by the Minister of Digital Development, Communications and Mass Media, Maxut Shadayev, at the opening ceremony of the Russian Internet Governance Forum (RIGF).⁴⁰ During the first session of RIGF, Deputy Minister Maxim Parshin reiterated what he said at the global IGF, stating, “We believe it is important to define an entity, within the U.N. framework, that would develop and implement legal norms and standards in the field of Internet governance. We think that the ITU could become such an entity.”⁴¹

On 12 April 2021, President Putin put into effect the new Basic Principles of State Policy in International Information Security.⁴² Item 11a in the document states that the Russian Federation should work “to create conditions enabling the U.N. member states to pass a Convention for providing international information security.” Item 11i, calls for work “to advance the national standards of the Russian Federation related to information security, in international and regional cooperation in the area of standardization, and work to facilitate their adoption as international, regional and interstate standards.”⁴³ Item 15a expresses the Russian Federation’s support for the work of the UNGA Open-Ended Committee of Experts (covered in the GE paper with updates from the UNGA working groups meetings⁴⁴). Item

³⁴ Russia, “Basic Principles of State Policy in International Information Security for the period till 2020”, Website of the Security Council of the Russian Federation, 24 July 2013, <http://www.scrf.gov.ru/security/information/document114/> and “Security Council Secretary Nikolai Patrushev’s statement for the media following Security Council meeting”, 26 March 2021, <http://en.kremlin.ru/supplement/5628>

³⁵ This sentence was updated to correct the previous version, which attributed the statement to President Putin.

³⁶ Sergey Lavrov, Interview to “Bolshaya Igra” TV Show. *The International Affairs Magazine (Mezhdunarodnaya Zhizn)*, 1 April 2021, <https://interaffairs.ru/news/show/29610>

³⁷ “Kiriyenko said there’s a need for international rules for Internet companies”. TASS, 6 April 2021, <https://tass.ru/ekonomika/11081727>

³⁸ Elections are going to take place at the ITU Plenipotentiary Conference in October-November 2022.

³⁹ Russia Nominates Its Candidate for the Position of the ITU Secretary General, MoC website, 7 April 2021, <https://digital.gov.ru/ru/events/40758/>

⁴⁰ 11th Russian Internet Governance Forum (RIGF), YouTube channel of the Russian ccTLD manager, 7 April 2021, <https://www.youtube.com/watch?v=ZnUv-8baBZk> (at 39:00, in Russian)

⁴¹ 11th RIGF, YouTube channel of the Russian ccTLD manager, 7 April 2021, <https://www.youtube.com/watch?v=ZnUv-8baBZk> (at 2:55:53, in Russian)

⁴² Presidential Decree “Basic Principles of State Policy in International Information Security”, Kremlin website, 12 April 2021, <http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZPTuc5TrdHURpA4vpN5UTwM.pdf>

⁴³ Presidential Decree “Basic Principles of State Policy in International Information Security”

⁴⁴ See <https://www.icann.org/en/system/files/files/ge-005-15jul20-en.pdf>

17b, addresses the State Policy aim to provide “assistance in ensuring the secure and stable functioning and development of the Internet, based on equal participation of the member states in the management of the Internet and enhancing the role of the ITU in this management.”⁴⁵

On 21 April 2021, Ernst Chernukhin, while speaking at a livestreamed conference, said: “About the ITU: the Russian Federation has been consistently calling for the internationalization of the management of the Internet, as well as for increasing the role of governments in this process.” He also said, “The multistakeholder model of Internet governance [...] has demonstrated its ineffectiveness a long time ago,” and added: “The Russian Federation, within the U.N. system, insists on adopting a number of coordinated measures, including ... development at the intergovernmental level of global policies in the area of Internet management, among others within the framework of achieving agreement on new international telecommunication regulations (ITRs). As we see it, the optimal option for this would be transferring Internet management prerogatives specifically to the ITU, as it is a specialized U.N. body, which has the needed expertise on these issues ... This strategic objective may be achieved by electing or promoting the Russian candidate to the position of the ITU Secretary-General in the 2022 elections ... and by holding the 2025 anniversary U.N. Internet Governance Forum in Russia.”⁴⁶

Russian Internet-Related National Policy Statements and Initiatives

On 29 October 2020, during an investment forum question and answer session President Putin said: “You are asking if we want a Chinese or a European data protection mechanism? We will have a Russian one.”⁴⁷

On 16 December 2020, the Russian Federation became a member of the Bureau of the Consultative Committee of Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data.⁴⁸

On 23 December 2020, President Putin spoke about national projects in Russia and stressed that informational security is an “element of digital maturity” and that the state must protect its citizens in this new digital environment and protect Russian “information systems and state systems.”⁴⁹

⁴⁵ Presidential Decree “Basic Principles of State Policy in International Information Security”, Kremlin website, 12 April 2021, <http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZPTuc5TrdHURpA4vpN5UTwM.pdf>

⁴⁶ Ernst Chernukhin, special coordinator of MFA on the Issues of Political Use of Information and Communication Technologies. 2nd Inter-regional Conference on Information Security and Informational Interaction in the Central Federal District “Infoforum”, Yaroslavl, 20-23 April 2021, Infoforum YouTube channel, streamed 21 April 2021, <https://youtu.be/5qzrrKBv3M?t=7163> (from 01:59:23 hrs.)

⁴⁷ Vladimir Putin in a Q&A session during “Russia Calling! Investment Forum”, Moscow oblast Novo-Ogaryovo, Kremlin website, 29 October 2020, <http://kremlin.ru/events/president/news/64296>

⁴⁸ Ministry of Communications of Russia. “Russia Became a Member of the Council of Europe Bureau on Personal Data”, MoC website, 16 December 2020, <https://digital.gov.ru/ru/events/40246/> and <https://www.coe.int/en/web/data-protection/consultative-committee-tpd>

⁴⁹ Vladimir Putin. “Joint meeting of the State Council and the Council for Strategic Development and National Projects”, Novo-Ogaryovo, Moscow Region, Kremlin website, 23 December 2021, <http://kremlin.ru/events/president/news/64736>

On 28 December 2020, MoC issued ordinance No. 780, “On Defining Threats to the Stability, Security and Operational Integrity of the Internet and Public Communications Networks within the Russian Federation.”⁵⁰

In January 2021, Roskomnadzor (RKN)⁵¹ published an instruction for telecom operators and Autonomous System Number holders explaining what RKN considers to be “national domain name system” (NDNS). The instruction requires autonomous system number holders to change or add addresses of NDNS resolvers to the list of end user DNS servers and to add these addresses to the Dynamic Host Configuration Protocol (DHCP).⁵²

On 26 January 2021, Deputy Minister of Communications of the Russian Federation⁵³ Oleg Ivanov said that the plans to conduct Internet drills in Russia have been “postponed until after the pandemic”.⁵⁴

On 27 January 2021, the Federation Council, the upper chamber of the Russian Parliament, issued a statement where it stressed that “Internet companies, representing one country – USA – closely tied with its government entities, have a monopoly over the global network, and this situation is fraught with the potential establishment of supremacy of one state over most global network exchanges.”⁵⁵

On 2 February 2021, RKN published a public procurement contract for Internet service provider (ISP) data analysis,⁵⁶ and another one for the establishment of a register of Internet addresses and numbering resources for the information system at the Center for Monitoring and Administering Public Information Network.⁵⁷

On 16 February 2021, four deputies of the State Duma of the Russian Federal Assembly introduced a bill that would allow blocking of websites without a court order.^{58 59}

⁵⁰ Ministry of Digital Development, Communications and Mass Media (MoC). Order # 780 “On Defining Threats to the Stability, Security and Operational Integrity of the Internet and Public Communications Networks within the Russian Federation”, MoC website, 28 December 2020, <https://digital.gov.ru/ru/documents/7450/>

⁵¹ Roskomnadzor is the Federal Service for Supervision of Communications, Information Technology and Mass Media [Authors’ remark].

⁵² The link pointing to the instructions is no longer working (https://77.rkn.gov.ru/docs/77/Prezentacija_Internet.pdf)

⁵³ “Internet Resilience Drills Delayed Until After the Pandemic”. *Interfax*, 26 January 2021, <https://www.interfax.ru/russia/746893>

⁵⁴ See more on the drills in the GE publication “Russia: Country Focus Report: Russian Federation Internet-Related Laws and United Nations Deliberations” p. 17 <https://www.icann.org/en/system/files/files/ge-006-19jan21-en.pdf>

⁵⁵ “Federation Council Asserts that US Government Entities Have Usurped Control over the Internet”. *RIA Novosti*, 27 January 2021, <https://ria.ru/20210127/sovfed-1594743673.html>

⁵⁶ Unified Procurement Information System. Information on Contract # 57706228218210001340000. *Edinaya informatsionnaya sistema v sfere zakupok*, 2 February 2021, <https://zakupki.gov.ru/223/contract/public/contract/view/general-information.html?id=10895252&viewMode=FULL>

⁵⁷ Unified Procurement Information System. Information on Contract # 57706228218210001310000. *Edinaya informatsionnaya sistema v sfere zakupok*, 2 February 2021 <https://zakupki.gov.ru/223/contract/public/contract/view/general-information.html?id=10891921&viewMode=FULL>

⁵⁸ On Introducing Changes into the Federal Law ‘On Information, Information Technologies and Information Protection’. *Sistema Obespechenia Zakonodatelnoy Deyatelnosti*, <https://sozd.duma.gov.ru/bill/1113081-7>

⁵⁹ This sentence was updated to correct the quote, and to add additional source: “At workers’ request”, *Kommersant daily*, 17 February 2021, <https://www.kommersant.ru/doc/4693508>

On 24 February 2021, President Putin signed the law “On Changes in the Administrative Code of the Russian Federation.”⁶⁰ The law provides for a procedure to block (without a court order) Internet resources that do not comply with the Sovereign Internet Law and would impose fines on ISPs for noncompliance with it. The law also includes articles 13.44 and 13.45 establishing liability for noncompliance with the national DNS and centralized management of the “public service networks.”⁶¹

On 3 March 2021, RKN announced a public procurement contract for access to the DNS root servers’ backup and to cache DNS resolver service.⁶²

In an interview to the TASS news agency on 31 March 2021, the chairman of the Parliamentary State Duma Committee on Information, Alexander Khinshtein, said that the Law on Sovereign Internet “is being implemented” and that “there is still work to do toward ensuring its implementation.”⁶³ He also drew a comparison between an autonomous “generator downstairs” that alleviates your concern about continuous operation of “your refrigerator, heater, and light” if electricity to your dacha goes off, and with Russia’s Internet sector that “can be autonomous in case of external threats.”⁶⁴ He claimed that Russia “has such a generator.”⁶⁵ He also said that “colleagues from Roskomnadzor and MoC assure us that [Russia] has full [technical] capacity [to slow down and block any Internet resource within its borders].”⁶⁶ However, he stressed that he “does not want” to have the opportunity to see proof of their statements and “hopes that such mechanisms will not be called for.”⁶⁷ Mr. Khinshtein confirmed that the DPI equipment is being installed by the ISPs and that “major market players, such as Rostelecom, MTS, MegaFon, Vimpelcom, and Transtelecom have already installed it.”⁶⁸

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 in the last six months of raising cyber-related issues, both nationally as well as internationally, at the United Nations and other intergovernmental organizations (IGOs) where cyber-related and Internet-related discussions are taking place.

ICANN organization, 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.

⁶⁰ “Changes Introduced to the Administrative Code to Establish Liability for Non-compliance with the Requirements to Ensure, Stability, Security and Operational Integrity of the Internet Within Russia”. Kremlin website, 24 February 2021, <http://kremlin.ru/acts/news/65062>

⁶¹ Russia, Federal Law dated February 24, 2021 No. 19 FZ “On Introducing Changes into the Russian Federation Administrative Code”. Kremlin website, 24 February 2021, <http://kremlin.ru/acts/bank/46445>

⁶² Unified Procurement Information. Information on Contract # 57706228218210001330000 *Edinaya informatsionnaya sistema v sfere zakupok*, 3 March 2021, <https://zakupki.gov.ru/223/contract/public/contract/view/general-information.html?id=10901529&viewMode=FULL>

⁶³⁻⁶⁸ Interview with Alexander Khinshtein “Identity Verification of Internet Users Online Is a Question of Time”. TASS, 11 March 2021, <https://tass.ru/interviews/11032409>