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

6 June 2022
GE-011

ICANN

TABLE OF CONTENTS

Introduction

This is part of the Internet Corporation for Assigned Names and Numbers (ICANN) organization's (ICANN org) periodic update on the Russia Country Focus Report, first published in January 2021, with an earlier update issued in April 2021.[1]

This update covers the period from 21 April 2021 to 6 April 2022 and is divided into two parts. The first looks at the Russian cyber- and Internet-related foreign policy statements and initiatives, and the second covers the Internet-related national policy statements and initiatives. As with previous similar documents, primarily only statements and quotes that touch on ICANN's mission are referenced. In this paper, ICANN org's Government and Intergovernmental Organization Engagement (GE) team also provides context on some of the foreign policy statements and initiatives that may require background information for better understanding by the broader ICANN community.

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

On 21 April 2021, in his annual address to the Russian Parliament, President Putin said:[2], "Clearly, there is a reason why our Western colleagues have been stubbornly rejecting Russia's numerous proposals to establish an international dialogue on information and cyber security. We have made these proposals many times. Everyone avoids even discussing this matter."[3]

Context: International dialogue on "information and cybersecurity" has been ongoing for years at the United Nations. The U.N. Open-Ended Working Group (OEWG), which was open to all Member States, was convened in 2019 "with a view to making the United Nations negotiations process on security in the use of information and communications technologies more democratic, inclusive, and transparent."4 All Member States participated in the OEWG cybersecurity negotiations. The OEWG also held intersessional consultative meetings that took place with industry, civil society, and academia. In its final session in March 2021, a month prior to President Putin's comments, the OEWG adopted a report by consensus.5 Parallel to the OEWG negotiations, Russia and "Western colleagues" (the term used by Mr. Putin) worked together in another U.N. process on cybersecurity negotiations within the Group of

[1] All publications by ICANN Government and Intergovernmental Organization Engagement: https://www.icann.org/en/government-engagement/publications

[2] Vladimir Putin, Presidential Address to the Federal Assembly, Moscow, Kremlin website, 21 April 2021, http://kremlin.ru/events/president/news/65418

[3] This quote and all other quotes in this document have been translated into several languages for information only. The original statements in Russian can be obtained at the appropriate web addresses provided in the footnotes. The web addresses were working as of the date referred to in the footnotes.

[4] U.N. General Assembly Resolution A/73/27 established an Open-Ended Working Group (OEWG) in December 2018 https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F27&Language=E&DeviceType=Desktop&LangRequested=False

[5] OEWG Final Substantive Report, 10 March 2021: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

> *Governmental Experts (2019-2021), which also finished with a consensus report.*[6] *Additionally, see below a statement by Russia Foreign Ministry diplomat Dmitry Bukin on 15 June 2021, which provides further context.*

On 28 April 2021, Valentin Makarov, who, in 2016 was appointed to the Expert Council at the Russian Ministry of Digital Development, Communications, and Mass Media (MoC),[7] in a discussion held at the Gorchakov Fund,[8] said: “There is also executive power. From this point of view the Internet that we use worldwide is solely American, right? There is ICANN, located in California, where it is registered. As far as I know, out of 21 Board members, 13 are Americans. It is all regulated by American law, legislation, and so executive power essentially belongs to just one country. Despite the fact that the Russian side has repeatedly proposed, and not just Russia, Brazil too, for example, making ICANN report to the international community, to the ITU, the International Telecommunication Union, for example, these proposals have not been accepted.”[9]

> *Context: The “Internet that we use worldwide” is not “solely American;” it does not belong to any one country. The ICANN Board has 20 members (16 voting directors and four liaisons). The ICANN Bylaws require geographic diversity among the Board and prohibit more than five directors from any single geographic region at any time. In April 2021, there were five directors on the Board from the North American region and one liaison, not 13, as Mr. Makarov claimed. It is not clear what “executive power” in “the hands of one country” Mr. Makarov had in mind, nor which country he had in mind. It is also unclear what “reporting to the international community” means, but ICANN already is accountable to the whole global ICANN community, to all of its constituencies, including the ICANN Governmental Advisory Committee (GAC), where Russia is a member, and the International Telecommunication Union (ITU) is an observer organization.*

Mr. Makarov further added: “...for example, out of 13 key root data centers 10 are located in the U.S. or in Japan, Holland or Sweden, this does not in any way guarantee for other countries without these root data centers against just getting shut off. Trust needs to be created through executive power and not solely through the legislative power.”

> *Context: It is not correct to say that there are "13 key root data centers." When talking about the root server system, there are 12 organizations that collectively operate more than 1,500 instances globally. Root servers are a network of hundreds of servers in many countries around the world, and not just in four, as stated by Mr. Makarov. The Root Server Operators will not “shut off” any country as per their commitment to RSSAC055 (with or “without these root data centers”); this is not how the root servers operate. There are more than a dozen instances from different Root Server Operators in the territory of the Russian Federation alone—without taking into account the large number (greater than 1,500) spread over the globe.*[10] *Shutting off a few root servers in*

[6] The 2019-2021 Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security (GGE) report, 14 July 2021: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[7] Registry of Russian Software Procurement According to Federal Law 188. Expert Council on Russian Software, 31 December 2015, https://reestr-minsvyaz.ru/sostav-ekspertnogo-soveta/

[8] The Gorchakov Fund is the public diplomacy arm of the Russian Ministry of Foreign Affairs (MFA). The Gorchakov Fund, Mission and Goals, https://gorchakovfund.ru/portal/page/4c40a0df-e8c8-48d3-983f-a979f42188d1

[9] Valentin Makarov’s remarks at the Alexander Gorchakov Public Diplomacy Fund discussion “Global Internet: Space of Threats or Space of Opportunities?”, 28 April 2021, https://youtu.be/Hmub5SY0E08?t=3026 (starts at 50:26)

[10] See full list of all root server instances; as of 5 April 2022, there are more than 1,500 instances all over the planet. https://root-servers.org/

> *a country does not affect that country's Internet connectivity nor the resolution of the DNS top-level domains; at most, it slows down a small percentage of queries. The loss of a root server might reduce the speed of a small fraction of the Domain Name System (DNS) resolution but would not stop devices on the Internet in that country, or globally, from resolving names in the DNS.*

In his remarks made at the same event at the Gorchakov Fund on 28 April 2021, in a discussion of the work of the new U.N. Open-ended Working Group (2021 - 2025), Ambassador Andrey Krutskikh said: "All the interested forces and people need to be brought into this process. This is (I do not like this word) — the multistakeholder approach. Now, the new Open-ended Group [OEWG] will be built on this very principle. And so all those who are interested in reaching consensus in order to build a safety net for humankind need to step up their efforts."[11]

> *Context: The OEWG indeed aims at including in its work other stakeholders; however, the U.N. General Assembly does not work in a multistakeholder manner. It's part of a multilateral organization, which does not treat all stakeholders equally. The first OEWG (2019–2021) did not allow participation of non-governmental stakeholders on equal footing with the member states. At the moment of conclusion of the second substantive session (1 April 2022) of the second OEWG (2021–2025), participation of non-governmental stakeholders on equal footing was still not allowed.*

On 31 May 2021, Nikolai Patrushev, Secretary of the Russian Security Council, in an interview with Russian daily Rossiyskaya Gazeta, enumerated the threats to Russian national security, and said that potential online threats against Russia are the reason for "...a need to define a new strategic national priority—that of information security. Its implementation will preserve the country's sovereignty in information space. Moreover, Russia supports the development of international cooperation in the interest of establishing a global international and legal framework, which would ensure safe and equitable use of information and communications technologies."[12]

On 7 June 2021, in an interview, Ambassador Krutskikh said: "Russia has been consistently in support of internationalizing Internet governance and of expanding the role of governments in this process."[13]

> *Context: Internet governance is internationalized; this has been established in the WSIS Tunis Agenda.[14] The U.N. WSIS+10 outcome document[15] reconfirmed the role of governments and all other stakeholders in Internet governance. Russia was an active participant in the WSIS+10 negotiations; however, the country's views as expressed by Mr. Krutskikh are not widely shared by other U.N. member states.*

[11] Andrey Krutskikh's remarks at the Alexander Gorchakov Public Diplomacy Fund discussion "Global Internet: Space of Threats or Space of Opportunities?", 28 April 2021, https://youtu.be/Hmub5SY0E08?t=2384 (starts at 39:45)

[12] Rossiyskaya Gazeta, "No Fear, No Reproach", 31 May 2021, https://rg.ru/2021/05/31/patrushev-raskryl-neizvestnye-podrobnosti-zhenevskoj-vstrechi-s-sallivanom.html

[13] Andrey Krutskikh, The International Affairs, Global Agenda: Diplomatic Victory, 7 June 2021. Interview with the Director of the Department of International Information Security of the Ministry of Foreign Affairs of Russia, https://interaffairs.ru/news/show/30374

[14] World Summit on the Information Society, Geneva 2003–Tunis 2005, WSIS-05/TUNIS/DOC/6 (Rev. 1)-E, 18 November 2005, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[15] Resolution A/RES/70/125, Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, 16 December 2015, https://unctad.org/system/files/official-document/ares70d125_en.pdf

Mr. Krutskikh said: “The situation where the Internet is regulated solely by the private sector and where the role of governments has been made equal to that of others […] has proved to be ineffective a long time ago.”[16] And: “Within the U.N. system framework, Russia insists on adopting an entire range of coordinated measures, such as expanding the role of governments in Internet governance, developing, on inter-governmental level, global policies related to Internet governance, using international law to ensure its stability and security, preserving the sovereign right of governments to regulate their national segments of the Internet.”[17]

> *Context: The private sector does not regulate the Internet; as mentioned above, both the WSIS Tunis Agenda and the WSIS+10 Outcome Document have defined the roles and responsibilities of all stakeholders in the development of the Internet and its governance, including the roles of the private sector and of governments.[18] Different countries have different legal regimes vis-a-vis the Internet; some have some form of regulation, licensing, or registration, while others have none.*

Further, Mr. Krutskikh noted: “It is becoming important to grant the proper authority to the International Telecommunication Union (ITU), which is the body that has the necessary remit and is currently actively involved in developing various standards and protocols for the Internet.”[19]

> *Context: The ITU is actually involved in developing a small number of the standards and protocols for the Internet. Standardization for the Internet is primarily done at the Internet Engineering Task Force (IETF), in which the ITU participates. The Internet protocols are developed by the IETF, and the ITU has its own set of competing protocols (X.25, X.400, and others). The IETF actively cooperates with the ITU when IETF protocols overlap with ITU areas (MPLS-TE and others).*

On 15 June 2021, at the XII International IT Forum attended by BRICS[20] and SCO[21] countries, Dmitry Bukin, Deputy Head of the Russian Ministry of Foreign Affairs Department on International Information Security, said: “...it is fundamentally important that constructive atmosphere at the U.N. negotiations on IIS[22] is currently being restored. This gives cautious optimism that [...] a global discussion of IIS [...] within the framework of the new OEWG [on cybersecurity] will continue. [...] We can expect that this will satisfy the desire of the larger international community to revert the U.N. discussions on IIS back to a single track framework and that the new OEWG will be set in the U.N. system as a sort of golden

[16] Andrey Krutskikh, The International Affairs, Global Agenda: Diplomatic Victory, 7 June 2021. Interview with the Director of the Department of International Information Security of the Ministry of Foreign Affairs of Russia, https://interaffairs.ru/news/show/30374

[17] Andrey Krutskikh, The International Affairs, Global Agenda: Diplomatic Victory, 7 June 2021. Interview with the Director of the Department of International Information Security of the Ministry of Foreign Affairs of Russia, https://interaffairs.ru/news/show/30374

[18] World Summit on the Information Society, Geneva 2003 – Tunis 2005, WSIS-05/TUNIS/DOC/6 (Rev. 1)-E, 18 November 2005, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html, A/RES/70/125, Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, 16 December 2015, https://unctad.org/system/files/official-document/ares70d125_en.pdf

[19] Andrey Krutskikh, The International Affairs, Global Agenda: Diplomatic Victory, 7 June 2021. Interview with the Director of the Department of International Information Security of the Ministry of Foreign Affairs of Russia, https://interaffairs.ru/news/show/30374

[20] BRICS refers to Brazil, Russia, India, China and South Africa

[21] Shanghai Cooperation Organization

[22] International Information Security

standard venue for discussing this issue on an inclusive and open, transparent and truly democratic foundation."[23]

> *Context: As explained in the context of the 21 April 2021 statement by President Putin, this is one more observation of a Ministry of Foreign Affairs official that there was a constructive atmosphere at the U.N. cybersecurity-related negotiations, while President Putin claimed the opposite.*

On 15 June 2021, at the same forum, Grigory Logvinov, Deputy Secretary General of the SCO said: "...there is a fairly widespread worldwide understanding that uncontrollable development of the Internet is unacceptable. It would seem that this understanding should prompt the international community to develop universally acceptable norms of behavior in the information space. Unfortunately, this objective necessity comes up against powerful opposition of forces trying to establish monopoly control over the global network by Internet companies from just one country and closely tied to its government structures. To call things by their proper names — to establish dominance of one country over a major part of the world network exchanges."[24]

> *Context: There is no "control over the global network" by "Internet companies from just one country." The Internet is a network of networks—some 70,000 of them.[25] Nobody controls the Internet, because nobody controls all of these networks.*

On 15 June 2021, Ilya Kostunov, advisor to the leader of the United Russia All-Russian Political Party fraction in the State Duma of the Russian Federation, said: "In the meantime, for the owners of the Internet system, for those that develop the router system, this anonymity is becoming nothing but a word. Things become not about anonymity anymore but rather about physical access. [...] This imbalance needs to be remedied too in the process of establishing sovereignty of the different segments of the Internet."[26]

On 23 June 2021, Ambassador Vasily Nebenzya, the Permanent Representative of Russia to the U.N., said in reference to the U.S.-Russia summit meeting in Geneva in the context of a wider cyber dialogue: "I hope that if the bilateral track develops positive momentum, it will provide new impetus to multilateral negotiations on IIS here at the United Nations."[27]

On 23 June 2021, Alexander Bortnikov, the Director of the Federal Security Service (FSB), said: "We believe the negotiations process should be expanded with the goal to harmonize international legal rules in the area of information security under the aegis of the U.N. We are ready for a dialogue with any partner wishing to create safe cyberspace."[28]

[23] IT Forum Ugra, Infoforum. Plenary, "Russia and the World. Urgent Issues of International Information Security Within the Framework of BRICS, Shanghai Cooperation Organization, Collective Security Treaty Organization," 15 June 2021, https://youtu.be/hWdZbzrexIU?t=4466 (starts at 1:14:26)

[24] IT Forum Ugra, Infoforum. Plenary, "Russia and the World. Urgent Issues of International Information Security Within the Framework of BRICS, Shanghai Cooperation Organization, Collective Security Treaty Organization," 15 June 2021, https://youtu.be/hWdZbzrexIU?t=1571 (starts at 26:11)

[25] Internet Society, Internet Way of Networking Use Case: Data Localization How mandatory data localization impacts the Internet Way of Networking, 30 September 2020, https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/

[26] IT Forum Ugra, Infoforum. New Digital Technologies and Information Security — Development of Trust and Cooperation, https://youtu.be/bc-BNilRIxg?t=5857 (starts at 1:37:37).

[27] IX Moscow Conference on International Security, Plenary Session "Information Security: Problems and Solutions", 23 June 2021, https://youtu.be/MMG0kuXDqRw?t=990 (starts at 16:31)

[28] TASS, FSB Will be Working with the United States on Identifying Hackers, Pursuant to an Agreement, 23 June 2021, https://tass.ru/obschestvo/11723445

On 24 June 2021, Sergei Lavrov, Minister of Foreign Affairs, said that Russia is: "...actively working on adopting a code of responsible conduct of states in the global information space from the point of view of each country's interests in the area of military and political security. We are also concurrently promoting the draft universal convention on fighting cybercrime."[29]

On 28 June 2021, Oleg Khramov, Deputy Secretary of the Security Council, said in an interview: "Another strategic area is to create a mechanism for ensuring security, stability and development of the Internet on the basis of equitable participation of all the members of the world community. We presume that the key role in managing the Internet should be played by the International Telecommunication Union as well as appropriate institutions of sovereign countries. The Russian draft of the framework for the convention which would regulate this subject matter, was presented back in 2017 and will be updated in the near future to reflect the current circumstances."[30]

> *Context: Mr. Khramov is talking about a "concept for the convention" but it is not clear if he has in mind the Russian draft for a U.N. Cybercrime Convention[31] from 2021, or the concept published by the Russian Ministry of Communications in 2017,[32] or another concept altogether. As of 1 April 2022, no previously published draft text has garnered support at the U.N.*

On 28 June 2021, Russia and China issued a joint statement, in which they noted "...their unity on issues related to Internet governance, which include ensuring that all States have equal rights to participate in global-network governance, increasing their role in this process and preserving the sovereign right of States to regulate the national segment of the Internet. Russia and China emphasize the need to enhance the role of the International Telecommunication Union and strengthen the representation of the two countries in its governing bodies."[33]

> *Context: Russia and China state that there is a "need to enhance the role of the ITU"; however, if this enhancement is related to expanding the role of the ITU in Internet governance, no such need has been formally proposed in the appropriate format, or brought to the attention of the ITU member states. The joint statement properly indicates that the states have a sovereign right to regulate the national segment of the Internet; if they didn't have this sovereign right, they wouldn't be able to preserve it.*

[29] Ministry of Foreign Affairs of the Russian Federation, Foreign Minister Sergey Lavrov's remarks at the 9th Moscow Conference on International Security, Moscow, 24 June 2021, https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4798212?p_p_id=101_INSTANCE_cKNonkJE02Bw&_101_INSTANCE_cKNonkJE02Bw_languageId=en_GB

[30] Security Council of the Russian Federation, Interview given by Deputy Secretary of the Security Council of the Russian Federation Oleg Khramov to RIA-NOVOSTI Information Agency, 28 June 2021, http://www.scrf.gov.ru/nehttp://www.scrf.gov.ru/news/allnews/3017/ws/allnews/3017/

[31] United Nations, Office on Drugs and Crime, First session of the Ad Hoc Committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html

[32] Ministry of Digital Development, Communications and Mass Media of the Russian Federation, Ministry of Communication Presents a New Draft Concept of the U.N. Convention, 14 April 2017, https://digital.gov.ru/ru/events/36739/

[33] Embassy of the Russian Federation to the United Kingdom of Great Britain and North Ireland, Joint Statement of the Russian Federation and the People's Republic of China on the Twentieth Anniversary of the Treaty of Good Neighborliness and Friendly Cooperation Between the Russian Federation and the People's Republic of China, 28 June 2021, 29 June 2021, https://www.rusemb.org.uk/fnapr/7007 On 29 June 2021, the Chinese Embassy in Moscow announced that the Treaty of Good Neighborliness and Friendly Cooperation between the Russian Federation and the People's Republic of China, signed on 16 July 2001, had been extended. Embassy of the People's Republic of China in the Russian Federation, Extension of the Treaty of Good Neighborliness and Friendly Cooperation Between the Russian Federation and the People's Republic of China, 29 June 2021, http://ru.china-embassy.org/rus/zgxw/t1887982.htm

The sovereignty of states upon certain elements of the Internet is noted in the 2005 WSIS Tunis Agenda.

In the July 2021 edition of The International Life Magazine, Ernst Chernukhin, Section Head at the MFA's Department of International Information Security, wrote: "The Russian Federation has been consistently calling for the internationalization of Internet governance, as well as for expanding the role of governments in this process. The one-sided Internet governance model where the role of governments has been made equal to that of others, while governments are the guarantors of the rights and freedoms of their citizens and play a major role in issues of the economy, security and stability of the Internet's critical information infrastructure, has demonstrated its ineffectiveness a long time ago. For the purposes of carrying out these objectives, the Russian Federation, within the United Nations framework, insists on adopting a set of coordinated measures, which include: ensuring stability and security of the Internet on the basis of international laws; preserving the sovereign right of governments to regulate [their] national segment of the Internet; increasing the level of coordination of international, regional and national efforts in the area of Internet governance; developing, at intergovernmental level, a global Internet governance policy. Nominating and electing the Russian candidate to the position of the Secretary-General of the International Telecommunication Union at the 2022 elections and holding the anniversary U.N. Internet Governance Forum in Russia in 2025 may help achieve these strategic objectives. From this point of view, the international expert community views the ITU as one of the only guarantors of a fair and equitable world order in the digital sphere."[34]

Context: The role of governments within the model of Internet governance is well defined by the WSIS Tunis Agenda. This model is not "one-sided" but quite the opposite—it includes all stakeholders, each of them with well-defined roles.[35] Russia has participated in the discussions about this model at the WSIS in Tunis, as well as in the negotiations of the U.N. WSIS+10 Outcome Document. The "coordinated measures" described by Mr. Chernukhin, are also defined in the WSIS Tunis Agenda. There is no evidence supporting the view that there is some unspecified "international expert community" that views the ITU as a "guarantor" of a "fair and equitable world order in the digital space."

On 12 July 2021, Olga Melnikova, Section Head at the Department of International Information Security at the Ministry of Foreign Affairs of Russia wrote: "Internet Corporation for Assigned Names and Numbers (ICANN) plays a key role in managing the Net. The Administration of the United States has a virtual monopoly over the Internet despite the fact that ICANN, which has been tasked with managing the Net, has officially been a non-profit organization since 2009. ICANN is accountable to the global multistakeholder community, in other words—to no one, and, for all intents and purposes, it is still controlled by the Administration of the United States."[36] (Please see Appendix 1 for the unofficial translation of the excerpts from the article from Russian).

Context: ICANN was established in 1998, not 2009. ICANN does not "manage the Net." No single governmental administration has any kind of monopoly (virtual or not) "over the Internet." ICANN's Bylaws detail the ways in which the organization is held

[34] Ernst Chernukhin, (Ministry of Foreign Affairs Special Coordinator on Issues of and Communication Technologies for Political Use), The International Life, On Russia's Approach to Ensuring Digital Sovereignty Based on the Example of International Organizations, Issue 7, 2021, https://interaffairs.ru/jauthor/material/2531

[35] World Summit on the Information Society, Geneva 2003 – Tunis 2005, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[36] Olga Melnikova, International Telecommunication Union - Technical Regulator or the New Confrontation Arena, International Affairs Magazine, 12 July 2021, https://interaffairs.ru/news/show/30759

> *accountable to the ICANN community. ICANN is designed to operate with a high degree of transparency and seeks public input, specifically governmental input, as part of its policy development activities. The constituent parts of ICANN (including the Governmental Advisory Committee or GAC) have the ability to come together jointly through a group called the Empowered Community to approve key governance changes, reject Board approval of budgets and plans, and even to remove and then re-seat the entire Board of Directors. Individuals and entities also have multiple ways to challenge ICANN decision making. The GAC also has a unique position in that if it provides consensus public policy advice to ICANN, the ICANN Board has to follow that advice unless it goes through an intensive dialogue process with the GAC and achieves a high voting threshold. Also, aside from the authority a government might hold over any entity subject to its jurisdiction, ICANN has not had any form of contract with the U.S. Government since 2016 that would give the United States any heightened level of authority over ICANN or its activities.*

On 31 August 2021, Alexander Fyodorov, professor at MGIMO[37] (Moscow State Institute of International Relations), SVR (External Intelligence Service) expert,[38] and a cyber negotiator said: “Americans understand the word ‘cybersecurity’, as affirmed by Trump at government level, to mean security of networks and systems defined by these networks, which operate on the basis of, let’s say, the Internet Protocol. That is, they are operating under the management of an assembly of American legal entities that have both rights and obligations in relation to these networks and their systems of operation. This is also why the issue of internationalizing Internet governance has come to a full stop. You understand that these conditions make Internet governance rather complicated, and this manifested itself very clearly, so to speak, at the World Summit on the Information Society meetings, even though there were mechanisms that were created there, and so on, so on, so on, and there were giant plans, which actually still exist and are being implemented. And the Chinese, by accepting the post of ITU Secretary-General for their representative, put the creation of a department at the forefront, or rather, he, naturally, in his electoral program, put at the forefront the creation of a department within the ITU for international regulation of the Internet. Well, that was in 2014, I think, seven years ago, and things haven’t budged an inch since.”[39]

> *Context: This is difficult to understand. Mr. Fyodorov is talking about American legal entities, which “have rights and obligations” toward networks that are in the United States. Similarly, there are Russian legal entities, which “have rights and obligations” towards networks on their territory, as is the case in other countries, including the U.S.A. These networks are subject to the laws and regulations of each country wherein they are situated. The “commitments” of Mr. Zhao for the position of the Secretary General are reflected in two ITU documents from 2014 and 2018 with the same title, “Candidacy for the post of Secretary-General: Mr Houlin ZHAO (People's Republic of China).”[40] The two official interviews of Mr. Zhao in 2014 and 2018, in*

[37] MGIMO University, Fyodorov Alexander Valentinovich, https://mgimo.ru/people/2436/

[38] Biography reference for Mr. Fyodorov at the Scientific Notes of the PIR Center under general editorship of A.V. Fyodorov, Superterrorism: the New Challenge of the New Century, 2002, p. 389, http://www.pircenter.org/media/content/files/9/13464203190.pdf

[39] Alexander Fyodorov, PIR-center, recording of the webinar “Patch for Diplomatic Relations: Prospects for Russian – American Consultations on Information Security,” 31 August 2021, published 5 September 2021, (1:12:57) https://youtu.be/qoKIuudRqaE?t=4377

[40] Plenipotentiary Conference (PP-14), Busan, 20 October–7 November 2014, Document 10-E, 4 November 2013, Candidacy for the post of Secretary-General: Mr Houlin ZHAO (People's Republic of China), https://www.itu.int/md/S14-PP-C-0010/en and Plenipotentiary Conference (PP-18), Dubai, 29 October – 16 November 2018, Document 7-E, 15 November 2017, Candidacy for the post of Secretary-General: Mr Houlin ZHAO (People's Republic of China), https://www.itu.int/md/S18-PP-C-0007/en

> *which he talks about his plans in the capacity of the ITU Secretary General, do not contain any references to "international regulation of the Internet."*[41]

On 9 September 2021, the Russian Federation submitted two contributions to the ITU's Council Working Group on International Internet-related Public Policy Issues (CWG-Internet). The first contribution under the title "Proposals on the Topic for the Next Open Consultations" featured a proposal from Russia to hold consultations on the following topic: "The role of states in ensuring the integrity, resilience and stability of the public core of the Internet and the need for international acts to guarantee the integrity, resilience and stability of the public core of the Internet."[42] The second contribution proposed to "organize work on the analysis of risks of the existing governance and operational model [of the Internet], preparation of recommendations and further draft international legal acts in line with ITU responsibilities."[43] In order to achieve this, the Russian Federation suggested member states submit to the 17th CWG-Internet meeting their "vision of the risks of the current Internet governance and operation model," their views on how to "overcome existing challenges and mitigate risks," and invited member states to present their views on "the preparation of international legislation to overcome existing challenges and risks associated with the management system of Internet's critical infrastructure in order to guarantee the integrity, stability and security of the Internet's public core."[44] On 23 September 2021, these contributions were reviewed by the CWG-Internet, but due to lack of consensus, they were noted in the chair's report, but were not taken into consideration.[45]

> *Context: There is no agreed-upon definition at the U.N. or at the ITU regarding the term "public core of the Internet," as explained in GE paper 008.*[46] *The first OEWG (2019–2021) and the GGE (2019–2021) did not reach an agreement to use this term. Furthermore, in none of the discussions of the ITU has there been a consensus on the need for the preparation of international legislation to "overcome" the alleged "challenges and risks".*

On 23 September 2021, the Ministry of Foreign Affairs of the Russian Federation reported that Russia and ASEAN[47] had a meeting where "experts held a comprehensive exchange of views on cooperation in the field of ICT security, including cooperation within the framework of global initiatives proposed by Russia – the Open-ended Working Group on Security of and Use of Information and Communications Technologies 2021–2025 and Ad-hoc Intergovernmental Committee to Elaborate a Comprehensive International Convention on

[41] Interview with Houlin Zhao, ITU Secretary-General Elect, 2014, ITU, https://www.itu.int/en/plenipotentiary/2014/Pages/zhao-interview.aspx and ITU News Magazine 04/18, Q&A Interview with Houlin Zhao Candidate for the Post of the ITU Secretary General, 24 October 2018, https://www.itu.int/web/pp-18/uploads/2018-itunews04-hzhao.pdf

[42] Contribution by the Russian Federation, Proposals on the Topic for Next Open Consultations, Council Working Group on International Internet-related Public Policy Issues, Document CWG-Internet-16/3-E, 9 September 2021, https://www.itu.int/md/S21-RCLINTPOL16-C-0003/en

[43] Contribution by the Russian Federation, Risk Analysis of the Existing Internet Governance and Operational Model, Council Working Group on International Internet-related Public Policy Issues, Document CWG-Internet-16/4-E, 9 September 2021, https://www.itu.int/md/S21-RCLINTPOL16-C-0004/en

[44] Contribution by the Russian Federation, Risk Analysis of the Existing Internet Governance and Operational Model, Council Working Group on International Internet-related Public Policy Issues, https://www.itu.int/md/S21-RCLINTPOL16-C-0004/en

[45] Report by the Chairman, Report of the Sixteenth meeting of the Council Working Group on International Internet-related Public Policy Issues (CWG-Internet), 23 September 2021, https://www.itu.int/md/S21-RCLINTPOL16-C-0008/en

[46] ICANN, Country Focus Report: The Netherlands and the "Public Core of the Internet," 28 May 2021, page 8, https://www.icann.org/en/system/files/files/ge-008-28may21-en.pdf

[47] ASEAN – Association of the Southeast Asian Nations

Countering the Use of Information and Communications Technologies for Criminal Purposes, as well as in the International Telecommunication Union."[48]

On 25 September 2021, Foreign Minister Lavrov said: "Russia advocates for the use of the U.N. as a platform for reaching agreements on ways to ensure international information security. Here, too, the criteria should not be someone's special rules but universal agreements enabling transparency in addressing all concerns in a transparent manner on the basis of facts."[49]

On 17 October 2021, Kommersant Daily published information on the joint U.S.-Russian Draft Resolution at UNGA First Committee: "Russia and U.S. presented a draft resolution[50] during informal consultations at the UN. Speaking at the event, the special representative of the President of Russia for International Cooperation on International Security, [and] Director of the Department of International Information Security at the Ministry of Foreign Affairs Andrey Krutskih noted that this was a 'historic moment'. It followed from his statement that the resolution is significant not just in terms of its content but also as a strategy because its adoption will make it possible to bring an end to the era of two cybersecurity platforms operating at the U.N. in parallel, which the world community has long been calling for. His American counterpart, Deputy Coordinator for Cyber Issues in the Office of the Coordinator for Cyber Affairs of the Department of State Michelle Markoff, thanked the Russian delegation for the cooperation. In her statement she recalled that the existence of two negotiation mechanisms in the area of cybersecurity, the OEWG and the GGE, was a subject of contention. However, over the course of recent months, these two groups have managed to adopt two significant reports, which, taken together, constitute a framework for a code of responsible state behavior in cyberspace. According to her, the intent of the new Russian-American resolution is to call on states to abide by these norms and to create conditions for future work at the U.N. on this topic."[51] The draft resolution, co-sponsored by the U.S. and Russia and supported by a number of member states, was distributed on 8 October 2021 and adopted without a vote 3 November 2021.[52]

On 7 December 2021, Deputy Prime Minister Dmitry Chernyshenko said: "I would also like to stress the importance of harmonizing international regulations in the area of global Internet network regulation and technology companies. It is important to develop uniform approaches to issues concerning data protection on the global level in order to balance out rights and responsibilities of all the parties operating within the digital space. In this regard we welcome the U.N. Secretary-General's recent initiative to develop a Digital Global Compact. Russia is open to dialogue with all interested countries, companies and expert communities."[53]

[48] Ministry of Foreign Affairs of the Russian Federation, Press Release, "On the Outcome of the First Meeting of the Russia-ASEAN Dialogue on ICT Security-related Issues," 24 September 2021, https://www.mid.ru/ru/foreign_policy/international_safety/1778293/?lang=ru

[49] YouTube, United Nations, Sergey Lavrov, Minister of Foreign Affairs of the Russian Federation Minister Addresses the United Nations General Debate at the 76th Session of the General Assembly of the United Nations, New York, 25 September 2021, (starts at 10:04), https://youtu.be/CGckUwpyR3w?t=605

[50] United Nations Document System, Seventy-sixth session, First Committee Agenda item 95, Developments in the field of information and telecommunications in the context of international security, 8 October 2021, A/C.1/76/L.13, https://undocs.org/A/C.1/76/L.13

[51] Elena Chernenko, Kommersant Daily, Binary Code, 17 October 2021, https://www.kommersant.ru/doc/5038983

[52] United Nations Document System, Seventy-sixth session, First Committee Agenda item 95, Developments in the field of information and telecommunications in the context of international security, 8 October 2021, A/C.1/76/L.13, https://undocs.org/A/C.1/76/L.13 adopted on 3 November 2021 without a vote: https://www.un.org/en/ga/first/76/pdf/FC_List_draft_proposals_76_Voting_Results.pdf

[53] Government of Russia, Dmitry Chernyshenko on the Harmonization of International Legislation and Cooperation in the IT Field at the 16th U.N. Internet Governance Forum, 7 December 2021, http://government.ru/news/44028/

> *Context: It is not clear what “international regulations” Mr. Chernyshenko had in mind. There are no international regulations that could be harmonized, nor are there international regulations “in the area of global Internet network regulation and technology companies.”*

On 14 December 2021, Russia and Indonesia concluded an international cooperative agreement on international information security. “The Agreement stresses the need for cooperation between countries aimed at improving the existing Internet governance model, including the need to ensure that governments have equal rights when it comes to Internet governance and to expand the role of the International Telecommunication Union.”[54]

> *Context: All governments participate in the Internet governance processes on equal footing, as explained in the WSIS Tunis Agenda and the WSIS+10 Outcome Document.*

On 29 December 2021, Deputy Minister of Foreign Affairs Oleg Syromolotov said: “As for issues of Internet regulation, Russia calls for internationalizing Internet governance, making sure governments are able to participate in this process on equal footing, preserving the sovereign right of governments to regulate their national segment of the Internet and concluding an agreement on intergovernmental regulation of the Internet which will be effective only if is adopted by all the states.” He added: “These issues are being discussed at the International Telecommunication Union (ITU), and we are actively participating in its work, including the work of absolutely all of ITU's study and working groups.” Mr. Syromolotov continued: “The Russian Federation has put forward its candidates in order to strengthen the leading role of this specialized U.N. agency for telecommunications and information and communications technologies: Rashid Ismailov as ITU General Secretary and Nikolai Varlamov to the new Radio Regulations Board. We are also running for re-election to the ITU Council.”[55]

> *Context: Deputy Minister Syromolotov’s words are misleading; the ITU has not discussed the “internationalization of Internet governance,” as this issue has already been discussed and agreed upon in the WSIS Tunis Agenda and the U.N. WSIS+10 Outcome Document. It is important to point out that there is no consensus at the ITU for “intergovernmental regulation of the Internet.” The discussion at the ITU to which he refers has only taken place in the ITU CWG-Internet and was initiated only through contributions by the Russian Federation itself and has never been accepted on a consensus basis.*

On 7 January 2022, Russia made two contributions to the ITU CWG-Internet. [56,57]. Both suggest that the CWG-Internet should discuss issues of ICANN’s and RIRs’ missions. In these contributions, Russia made several statements that need context:

[54] Security Council of the Russian Federation, News and Information, Russia and Indonesia concluded an intergovernmental cooperative agreement on international information security, 14 December 2021, http://www.scrf.gov.ru/news/allnews/3151/

[55] RIA NEWS, Oleg Syromolotov: Russia calls for equal participation of governments in internet governance, 29 December 2021, https://ria.ru/20211229/syromolotov-1765883993.html

[56] Contribution by the Russian Federation - Proposals to discuss the challenges and lack of operational activity organizations/operators of critical Internet infrastructure (first phase), Council Working Group on International Internet-related Public Policy Issues Seventeenth meeting – 19-20 January 2022, 7 January 2022, https://www.itu.int/md/S22-RCLINTPOL17-C-0003/en

[57] Contribution by the Russian Federation - Proposals on the topic for next open consultations, Council Working Group on International Internet-related Public Policy Issues Seventeenth meeting – 19-20 January 2022, 7 January 2022, https://www.itu.int/md/S22-RCLINTPOL17-C-0004/en

"...legal relations on the Internet are not sufficiently regulated at the international level. To date, there are no universal international legal agreements in international law that could regulate Internet governance issues. The problem lies not only in the lack of consensus at the international level, but also in the global nature, multilevel and multilateral participation in the formation of legal regulation related to the Internet."

> *Context: There is no consensus that there is any need for "sufficient regulation at the international level" of any "legal relations." There is no consensus on the need for "universal international legal agreements" to "regulate Internet governance issues." Internet governance has been discussed at two major U.N. meetings: WSIS 2003 in Geneva and WSIS 2005 in Tunisia. The roles of each stakeholder in the current model of Internet governance are defined in the WSIS Tunis Agenda and the WSIS+10 Outcome Document. Further, Russia alleges that there is a problem that consists of "lack of consensus at the international level," but the WSIS and WSIS+10 outcome documents are examples that there is consensus, and that consensus is in fact at the international level. The global nature of the Internet was not an impediment to reaching this consensus.*

The Russian contribution continued: "The lack of coordination of national Internet regulation is the most serious challenge and the reason for the fragmentation of the global network that has already begun."

There was no consensus on the Russian proposals and Russia issued a statement, in which it alleged that there is an "ongoing process of fragmentation of the Internet and degradation of the common digital space" and called for "transformation of the existing Internet governance system" and encouraged member states to engage in "a dialogue within the ITU."[58]

> *Context: In this statement, as in previous contributions, Russia alleges there is "fragmentation of the Internet," and adds that there is "degradation of the common digital space," but there is no evidence for either and no explanation of what these terms actually mean. Furthermore, the existing Internet governance system is constantly being discussed at appropriate venues, such as the Internet Governance Forum. Ideas for improvements of the multistakeholder Internet governance model are being shared and discussed among all participants. In contrast, the ITU CWG-Internet does not allow participation of any stakeholders except member states.*

On 3 February 2022, Ernst Chernukhin, Section Head at the MFA's Department of International Information Security, said: "Many experts have noted the new round of technological competition on the global market that will soon unfold in a struggle for, first and foremost, global telecommunication networks that are the basis for the spread of digital technologies primarily in the developing countries."[59]

On 3 February 2022, Olga Melnikova, Section Head at the MFA's Department of International Information Security, said: "Against the backdrop of these geopolitical risks and global cyber threats, the issue of the new geopolitical standoff escapes attention. I mean the

[58] Report of the seventeenth meeting of the Council working group on international Internet-related public policy issues (CWG-Internet), 24 January 2022, https://www.itu.int/md/S22-RCLINTPOL17-C-0006/en
[59] Ernst Chernukhin, Infoforum, Information Sovereignty and International Information Security, 3 February 2022, (10:15) https://youtu.be/bmXZzRWvIEo?t=615

desire of the West to preserve the possibility of technical dominance and attempts to take the International Telecommunication Union under single-handed control."[60]

> *Context: There is no evidence for any "desire of "the West"" (Ms. Melnikova's words) to take any functions of the ITU under "single-handed control." In fact, the only country that has talked about changing the functions of the ITU is the Russian Federation. As stated by a number of officials quoted in the Russia Country Focus Papers available at the GE publication page, Russia plans to attempt a change in the mandate of the ITU if its candidate for Secretary-General is elected.*

On 4 February 2022, Russia and China signed a joint statement in which they expressed "their readiness to deepen cooperation in the field of international information security and to contribute to building an open, secure, sustainable and accessible ICT environment." China and Russia confirmed the "willingness to speak with one voice" at the OEWG and confirmed that they "presented a joint draft convention as a basis for negotiations" at the AHC. Furthermore, both countries said that they "support the internationalization of Internet governance, advocate equal rights to its governance, believe that any attempts to limit their sovereign right to regulate national segments of the Internet and ensure their security are unacceptable, [and] are interested in greater participation of the International Telecommunication Union in addressing these issues."[61]

On 15 February 2022, International Affairs magazine published an article co-authored by three staffers of the Ministry of Foreign Affairs Department of International Information Security. They wrote: "Apparently, reforming the forum in this way may ramp up the discussion of internationalizing the governance of the Internet and facilitate the transfer of this urgent matter to the U.N. agencies. First and foremost — to the International Telecommunication Union, which is specialized in issues of stable and sustainable operation of the Net. Holding IGF25 in Russia immediately before the 20th anniversary review of decisions made at WSIS will help create a conducive environment for implementing the proposals made by the U.N. Secretary-General."[62]

On 18 February 2022, Dmitry Medvedev, Deputy Chairman of the Russian Security Council, emphasized the importance of multilateral processes at the U.N. with regards to the discussions on the U.N. Cybercrime convention: "We understand that there are different poles, there are countries that do not want our approaches to advance. It is important to work on universal rules, to try to lend them a legally binding character. At the same time, we must understand that on top of that there is digital sovereignty of states and the regime of equal rights in Internet governance."[63]

[60] Olga Melnikova, Infoforum, Information Sovereignty and International Information Security, 3 February 2022, (1:16:22), https://youtu.be/bmXZzRWvIEo?t=4582

[61] Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development, 4 February 2022, http://en.kremlin.ru/supplement/5770

[62] Vladimir Malinkin, Chief Advisor, Department of International Information Security at the Ministry of Foreign Affairs of Russia, Alexander Koshkin, First Secretary, Department of International Information Security of the Ministry of Foreign Affairs of Russia, Alexander Fedorenko, Third Secretary, Department of International Information Security at the Ministry of Foreign Affairs of Russia, U.N. Internet Governance Forum. Does It Have a Future? The International Life Magazine, 15 February 2022, p.61, https://interaffairs.ru/virtualread/ia_rus/22022/files/assets/downloads/publication.pdf

[63] Security Council of the Russian Federation, Deputy Chairman of the Security Council of the Russian Federation Dmitry Medvedev held a meeting themed "Forming International Mechanisms for Fighting Cybercrime and Ensuring Stability in the Information Space", 18 February 2022, http://www.scrf.gov.ru/news/allnews/3191/

> *Context: Mr. Medvedev states a fact: the Internet governance model is based on the equal rights of all participants. His statement seems more accurate than some of the statements of other Russian officials on the same topic.*

On 29 March 2022, during the second substantive session of the OEWG the Russian Federation representative said: "For example, there is an absolutely real possibility of an entire country being cut off from the international communications systems, in particular from the Internet, or the interbank system for carrying information and making payments, SWIFT. It is not a theoretical threat; it is what is happening to my country. Experience shows that technology makes it possible to carry out this threat, as these systems are managed by one country or a very small group of countries. And so, taking the Internet as an example, this would be the corporation for managing domain names and IP addresses, ICANN. It is an international non-profit organization, which de facto is fully controlled by the United States of America. These conditions make any country - any! - vulnerable to the political decisions of such a country."[64]

> *Context: ICANN is not in the position to "cut off" (stop, shut down, etc.) any country from the Internet. This is stated quite clearly in a letter dated 2 March 2022, from ICANN's President and CEO to a Ukrainian Deputy Prime Minister.[65] This was also noted on 5 April 2022, when former US government official Fiona Alexander[66] said: "The Russian Federation was better protected in the multistakeholder model than it has been in the U.N. system. So while the Ukrainian minister asked both RIPE and ICANN to take away their Internet resources, both said "no."[67] But in the ITU World Telecom Standardization Assembly, which happened in March 2022, the Russian government was stripped of leadership positions in the study groups at the request of Ukraine.[68] So, even though the Russian Federation participates in ICANN, at every turn [it] always wants to have it taken over by the ITU or replaced. It was ironic to me that the multistakeholder model actually better protected the people of Russia and the Internet than the U.N. system where the Russian government was actually stripped of its role."[69] On 6 April 2022 the White House issued a fact sheet on U.S., G7, and EU sanctions on Russia, in which it says that access to the Internet is not a target of the sanctions.[70]*

[64] Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 3rd meeting, statement by Vladimir Shin speaking as the representative of the Russian Federation within the framework of the informal session https://media.un.org/en/asset/k1l/k1l7rcax4f (51:05)

[65] Letter from Göran Marby, President and CEO, Internet Corporation for Assigned Names and Numbers (ICANN) to Mykhailo Fedorov, Deputy Prime Minister, Minister of Digital Transformation Ukraine, 2 March 2022, https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[66] Fiona Alexander is currently a Distinguished Policy Strategist in Residence in the School of International Service and Distinguished Fellow at the Internet Governance Lab at American University. For close to 20 years, Fiona served at the National Telecommunications and Information Administration (NTIA) in the U.S. Department of Commerce where she was Associate Administrator for International Affairs, Fiona Alexander - Biography, https://community.icann.org/display/EURALO/Fiona+Alexander+-+Biography

[67] RIPE NCC Response to Request from Ukrainian Government Letter from the Vice Prime Minister of Ukraine to RIPE NCC (PDF), Response from Managing Director of the RIPE NCC (PDF), Amsterdam, 10 March 2022, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[68] Official Twitter account of the Permanent Mission of Ukraine to the U.N. Office in Geneva, 9 March 2022, https://twitter.com/UKRinUNOG/status/1501658319932600326, Website of the Permanent Mission of the Czech Republic to the U.N. Office in Geneva, 9 March 2022, https://www.mzv.cz/mission.geneva/en/specialized_agencies/international_telecommunication_union/russia_s_military_aggression_against.html

[69] Fiona Alexander, ITIF webinar, Internet Governance During Times of War and Conflict, 5 April 2022, (58:57), https://itif.org/events/2022/04/05/internet-governance-during-times-war-and-conflict

[70] The White House, Briefing Room, FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia, 6 April 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/

On 30 March 2022, the Netherlands, during the second substantive session of the OEWG said: “For the Netherlands, safeguarding the public core includes respecting its multistakeholder governance model, and preventing the introduction of standards and protocols that would undermine the open and interoperable nature of the Internet. In this context, and in reaction to what was suggested yesterday, I’d like to highlight that the role of the multistakeholder organizations like ICANN and Regional Internet Registries (RIRs) is to ensure the technical coordination of the Internet and work to uphold a single, global and interoperable Internet, that continues to operate at all times, and is accessible to all…”[71]

Russian Internet-Related National Policy Statements and Initiatives

On 20 April 2021, the MoC reported the creation of “[...] a subsystem for monitoring and managing the national domain name system of the information system for monitoring and managing the public communications network (hereinafter – NDNS MAS). [This subsystem] is designed to provide the technical capacity to monitor performance and service quality of the service ensuring NDNS operations, to manage NDNS parameters, and to provide the technical capacity to send reports to the information system at the Center for Monitoring and Administering Public Communications Network about threats to stability, security and integrity of the national domain name system, as part of the agreement dated 1 September 2020 No. NSDI-2020.”[72]

On 20 April 2021, the MOC also mentioned that the second stage of the information system at the Center for Monitoring and Administering Public Communications Network was brought online in testing mode on 15 December 2020. The following subsystems have been created and brought online: “[...] Internet Address and Number Resource Register subsystem (ANRR) that enables ISPs, owners or other proprietors of technical communications networks, entities that organize the dissemination of information on the Internet, as well as other Autonomous System Number holders to provide and receive information in a timely fashion; - subsystem for monitoring and managing the national domain name system of the information system for monitoring and managing the public communications network (hereinafter – NDNS MAS); - a subsystem for communicating with external systems (ESCS) designed for communicating with ANRR, NDNS MAS, other PCN MAS, Roskomnadzor's Single Information System (SIS); - Visualisation Support Subsystem (VSS).”[73]

On 26 May 2021, President Putin signed into law provisions on administrative liability for violating critical information infrastructure security requirements and violating the procedure of the information exchange on computer incidents between subjects of critical information

[71] (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, statement by Ambassador at-Large for Security Policy and Cyber H.E. Nathalie Jaarsma of the Netherlands within the framework of the informal session, https://media.un.org/en/asset/k1g/k1gu15nuh2 (1:00:05)

[72] Revised Annual Report on the Implementation and Assessment of the Information Society Program Run by the Russian Federation Government, 20 April 2021, p. 61, https://digital.gov.ru/uploaded/files/utochnennyj-godovoj-otchet-2020.pdf

[73] Revised Annual Report on the Implementation and Assessment of the Information Society Program Run by the Russian Federation Government, 20 April 2021, Table 17 p. 27, https://digital.gov.ru/uploaded/files/utochnennyj-godovoj-otchet-2020.pdf

infrastructure within Russia and between subjects of critical information infrastructure in Russia and officially designated foreign authorities.[74]

On 19 June 2021, a new government decree expanded the scope of the MOC's mission related to "use of number resources in communications networks."[75] (Please see Appendix 2 for relevant provisions of the new regulations.)

In June 2021, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) published a report on its activities over the previous year. The report mentions that "the first version of the automated system for ensuring the security of the Russian segment of the Internet (ASSI) has been created as part of the effort to implement Federal Law dated 7 July 2003 No. 126-FZ 'On Communications.' ASSI is designed to mitigate threats to stability, security, and integrity of the Internet and the public communications network within the Russian Federation. The system consists of a centralized system for managing equipment for countering threats (TCE), installed directly within the ISPs' communication equipment."[76]

On 30 June 2021, the Russian government adopted regulations on federal government enforcement (oversight) of compliance with requirements related to the dissemination of information over information and telecommunications networks, including the Internet. Oversight is to be carried out by Roskomnadzor.[77]

On 1 July 2021, President Putin signed a law regarding the presence of foreign Internet platforms within the Russian Internet. The law stipulates that various foreign entities which "perform activities" on the Internet within the Russian territory and have over 0.5 million visits per day "will have to register with the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) and establish an office in Russia."[78] The law went into effect on 1 January 2022.

On 2 July 2021, President Putin approved the new National Security Strategy for Russia. The Strategy has for the first time included a new chapter on "Information Security." This chapter states: "The goal of information security is to strengthen the sovereignty of the Russian Federation within the information space." And: "information security is achieved by implementing government policy aimed at addressing the following objectives: [...] increasing the safety and stability of the single telecommunications network in the Russian Federation, the Russian segment of the Internet, and other significant information and communication infrastructure units, as well as prevention of foreign control over operation." The document also mentions the importance of "minimizing the number of instances of restricted access information leaks and of personal data and decreasing the number of violations

[74] President of Russia, Documents, Administrative Liability Established for Violating Critical Information Infrastructure Security Requirements, 26 May 2021, http://kremlin.ru/acts/news/65660

[75] Government of the Russian Federation, Decree No. 943 Dated 19 June 2021, "On Introducing Changes to the Decree On the Ministry of Digital Development, Communications, and Mass Media and on Repealing Some Laws of the Government of the Russian Federation", Official Legal Information Internet Portal, 24 June 2021, http://publication.pravo.gov.ru/Document/View/0001202106240011

[76] Ministry of Digital Development, Communications, and Mass Media of the Russian Federation, Federal Service for Supervision of Communications, Information Technology and Mass Media, Report on Government Enforcement (Oversight) and of the Effectiveness of this Enforcement (Oversight in 2020), p.114, https://rkn.gov.ru/plan-and-reports/reports/

[77] Gosuslugi, https://regulation.gov.ru/projects#npa=116422

[78] Kremlin.ru, Law Regulating the Activity of Foreign Entities On the Internet Within Russia Has Been Signed, 1 July 2021, http://kremlin.ru/acts/news/65985; Sistema Obespechenia Zakonodatelnoy Deyatelnosti, Activity of Foreign Entities on the Internet Within the Russian Federation, https://sozd.duma.gov.ru/bill/1176731-7

of requirements related to the protection of this type of information and personal data, as established by the Russian laws."[79]

On 21 July 2021, the RBC media outlet announced that "The documents of the Information Security Working Group at the Digital Economics ANO[80] (responsible for the national program by the same name) show that drills in support of stability, security and integrity of the Internet were held between 15 June and 15 July." One RBC source reported: "The objective of the drill is to establish that RUNET will be operational in case there are external distortions, blocking or other threats. The official conclusions have not been drawn up yet, preliminary reports indicate the drill was completed successfully." According to another RBC source, "the drill was designed to test the ability to physically disconnect the Russian segment of the Internet."[81]

On 17 August 2021, the United Russia Party[82] presented their Digital Manifest, listing in it the priorities in the area of the Internet. The main ideas of the document were described by the Deputy Secretary of the General Council of the United Russia, the Head of the State Duma Committee on Information Alexander Khinshtein during the party's strategy session "Russia's Digital Future." According to Section 3, Khinshtein conveyed that, "the Russian segment of the Internet has to be secure and stable 'under any sanctions and external disconnections,' though that does not mean a 'digital iron curtain' will be introduced."[83] The Russian media reported that "Deputy Minister of Digital Development, Communications, and Mass Media of the Russian Federation Oleg Kachanov expressed support for key provisions of the Digital Manifest at a United Russia party session." Mr. Kachanov said: "The key provisions that we would like to support and that we definitely support, are those provisions of the manifesto that deal with security, freedom and development. As it relates to our remit, first and foremost this means the development of digital technologies which also brings with it the development of the country and society overall. As for security, one of the most important areas for us is personal data protection, privacy protection and protection against abuse. Freedom means ensuring not just equal Internet access, it also means free, equal, fee-free access to services and socio-economically significant resources."[84]

In August of 2021, MoC posted for public comment new draft requirements governing traffic transmission across data transmission networks with the use of deep packet inspection (DPI) equipment.[85] On 21 August 2021 Roskomnazdor announced that the new draft decree is "designed to ensure effective protection of Russian citizens from the restricted content." "According to the draft decree, the equipment will be installed primarily on the networks of large and medium-size ISPs, and small ISPs will also be given the option to connect to these types of aggregation nodes. This will make the current setup more effective, lower the number of pieces of equipment as well as associated operating costs. To date, equipment has been installed on ISP networks in all of Russia's federal districts and covers 100% of mobile traffic and 60% of fixed-line traffic," reported Roskomnadzor's press

[79] Official Legal Information Internet Portal, National Security Strategy of the Russian Federation, 3 July 2021, http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1
[80] ANO - Autonomous Noncommercial Organization
[81] RBC, Russia Tests RUNET Operation in Case of Its Disconnection from the Global Network, 21 July 2021, https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739
[82] United Russia is the ruling party holding 325 seats out of 450 in the State Duma (national parliament), https://ru.wikipedia.org/wiki/Государственная_дума
[83] TASS, United Russia Presents the Party's Digital Manifest, 17 August 2021, https://tass.ru/ekonomika/12149831
[84] TASS, United Russia Presents the Party's Digital Manifest, 17 August 2021
[85] Gosuslugi, MoC's Draft Decree on Enacting Traffic Transmission Requirements in Data Networks, August 2021, https://regulation.gov.ru/projects#npa=119334

service.[86] The decree was scheduled to start operating on 1 December 2021; however, experts were doubtful that the Ministry of Justice would let it pass because the MoC did not have the right to establish requirements governing traffic transmission across data transmission networks by the date of its proposed enactment.[87] The decree is signed by the prime minister and scheduled to go into effect at a later date on 1 January 2023.[88]

On 9 September 2021, a number of Russian IT experts said that the public DNS service was temporarily blocked by authorities with methods that use DPI filtering. Some experts indicated that the blocked DNS services were provided by Google and Cloudflare.[89,90].

On 10 September 2021 Habr.com published the following information: "In September Roskomnadzor will test the ability to block a number of foreign internet protocols technologies, which mask site names, including Mozilla's and Google's DoH[91]. According to officials these technologies make it harder to block access to banned resources. They advise state companies to move to the National Domain Name System (NDNS)."[92]

On 19 October 2021, the head of Roskomnadzor, Mr. Lipov, talked about the drills that tested the Russian segment of the Internet: "According to Roskomnadzor all the drills carried out to date have been carried out successfully." And: "The drills are aimed at making sure these types of disruptions do not happen, and they have shown that we are ready for all of this to work in a stable and secure manner under any type of external influence."[93]

On 3 November 2021 Chairman of the State Duma Committee on the Information Policy, Technologies and Communications Alexander Khinshtein made the following comments on the Sovereign Internet Law: "The law stipulates a move to a more technologically advanced level, which will satisfy the requirements of the legislation on information thanks to the use of more precise tools for working with internet traffic that shall not affect the quality and the speed of access to internet services for people and companies."[94]

On 22 November 2021, Mr. Khinshtein also said: "Events in the online space are becoming as real as those in traditional life these days. The issue of preserving digital sovereignty is becoming the issue of national security. In light of the importance of the internet in the modern world our country has to ensure stable operation and reliable protection of the Russian segment of the worldwide Net against all threats, including external ones. The Law on Stable RuNET launched this process."[95]

[86] TASS, MoC: The Use of Threat Countering Equipment to Transmit Traffic Will Create Conditions for Strengthening Russia's Security, 17 August 2021, https://tass.ru/ekonomika/12151637

[87] Yulia Melnikova, The DPI is Getting Closer, COMNEWS, 19 August 2021, https://www.comnews.ru/content/216028/2021-08-19/2021-w33/tspu-vse-blizhe

[88] Ministry of Digital Development, Communications and Mass Media of the Russian Federation, Decree on Enacting Traffic Transmission Requirements in Data Networks, (no date is given in the document) https://regulation.gov.ru/projects#npa=119334

[89] Fontanka, Russia Blocked Google Services in a Mass Test Run, 9 September 2021, https://www.fontanka.ru/2021/09/09/70126808/

[90] New York Times, Russia Is Censoring the Internet, With Coercion and Black Boxes, 22 October 2021, https://www.nytimes.com/2021/10/22/technology/russia-internet-censorship-putin.html

[91] DoH – DNS over HTTPS

[92] Habr.com, In September Roskomnadzor Will Cut Off the Ability to Use Foreign [I]nternet Technologies to Circumvent Access Blocks, 10 September 2021, https://habr.com/ru/news/t/577234/

[93] TASS, Roskomnadzor Says Drills Performed Under the Provisions of the Sovereign Internet Law Were Successful, 19 October 2021, https://tass.ru/ekonomika/12701201

[94] State Duma of the Federal Assembly of the Russian Federation, News, Update on the Sovereign RuNET Law, 3 November 2021, http://duma.gov.ru/news/52623/

[95] Gazeta.ru, Khinshtein Talks About Key Elements of Digital Sovereignty, 22 November 2021, https://www.gazeta.ru/social/news/2021/11/22/n_16897759.shtml?updated

On 3 February 2022, Mr. Khinstein said: “[The Net] will continue working on the territory of our country even when switched off from the external source. And in addition, we now have a wonderful instrument for dialogue with our foreign partners.”[96]

On 6 March 2022, Kommersant Daily newspaper reported: “Vice Premier Dmitry Chernyshenko has tasked the MoC with preparing priority measures aimed at defending the country's information infrastructure.” The newspaper cited a governmental cable addressed to the executive branch of the constituent federal and regional entities of the Russian Federation and signed by the Deputy Minister of Communication Andrey Chernenko where he ordered all “government websites and portals by March 11 to switch to DNS servers (domain name system is a system that matches the website address with its IP-address), located in Russia, to remove all javascript code that is downloaded from foreign resources (banners, counters, etc.) from all html page templates, move resources on foreign hosting services to Russian hosting services, move resources to .RU and implement a stricter password policy.”[97]

Conclusion

To some readers, the statements quoted above might make it appear as though Russia is increasing the frequency of proposing new resolutions at the ITU, touching on or aimed at ICANN’s mission, and that this focus is new. In fact, this is not the whole case. The Russian Federation has been proposing cybersecurity-related resolutions at the U.N. since 1998. Through previous papers[98] published by ICANN org’s Government Engagement team, the ICANN community has become familiar with the Russian Federation’s recent history of proposing cybersecurity-related resolutions at the U.N. and at the ITU. There is in fact a long history of this type of initiative. To put it in perspective, in 2011, during a meeting between then Russian Prime Minister Putin and ITU Secretary-General Hamadoun Touré, Mr. Putin told Mr. Touré: “We are thankful to you for the ideas that you have proposed for discussion. One of them is establishing international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union.”[99]

For the purpose of clarity and to support better understanding by readers, ICANN org wanted to provide additional facts about and context for some of the statements from the Russian Federation. ICANN org, through its GE team, will continue to provide information to the ICANN community when such statements or proposals touch on technical Internet governance or have the potential to impact ICANN’s mission.

[96] Alexander Khishtein, Infoforum, Plenary session, 3 February 2022, (52:14) https://youtu.be/xUJzUIPOduQ?t=3134
[97] Kommersant Daily, Authorities Isolate Networks, 6 March 2022, https://www.kommersant.ru/doc/5249500
[98] ICANN, Government Engagement Publications, https://www.icann.org/en/government-engagement/publications
[99] New York Times, Regulating the Internet in a Multifaceted World, 26 July 2015 https://www.nytimes.com/2011/06/27/technology/internet/27iht-internet27.html ; Archive of the Russian Government, V.V.Putin meets ITU Secretary-General Hamadoun Toure, 15 June 2011, http://archive.premier.gov.ru/events/news/15601/

Appendix 1

Olga Melnikova, Section Head at the Department of International Information Security at the Ministry of Foreign Affairs of Russia, “International Telecommunication Union - Technical Regulator or the New Confrontation Arena,” International Affairs Magazine, 12 July 2021,[100] excerpts.

“Political and technological competition between the US and PRC is heating up, which results in the emergence of new standards and solutions that have been developed by the Celestial Empire [China], which are rarely accepted by the West. This situation undoubtedly affects the leadership of the United States as it deprives it of its role as the technology unifier of the entire world and weakens the leading positions of its high-tech industries. At the same time, the emergence of China's own ICT solutions will strengthen China's positions.

“It is a technological competition that is pitting the United States and China against each other at the International Telecommunication Union (ITU) — one of the oldest international organizations in existence and a United Nations agency specialized in ICT.

“The ITU manages the use of the radiofrequency spectrum and satellite orbits, approves technical standards that ensure smooth communication between networks and technologies, and aims to expand access to ICT across the world, strengthens international cooperation for the benefit of developing countries, including the development of telecommunications networks.

“Against the background of a steady growth of demand for the limited natural resource that is “spectrum/orbit” that is used for ground-based and space systems, ITU's priority is the development of the methods for effectively distributing radiofrequency spectrum and of rules governing its use, as well as technical underpinnings that support the operation of the radio systems.

“In other words, the development of all generations of mobile communications, the use of algorithms for compressing audio and video and the use of internet protocols would be impossible without the ITU.

“To paraphrase the famous European magnate Nathan Rothschild: “He who controls ITC, controls the world.”

“The ITU is not directly involved in internet governance. It plays an important role strictly limited to supporting technical operations of communications networks.

“Under the conditions of constantly intensifying rivalry in the digital space, the United States is trying to preserve its technological dominance and virtual monopoly in matters of internet governance.

“The World Summit on the Information Society's Tunis Program (2005) set the mission to ensure equal participation of governments in internet governance. A Working Group (CWG-Internet) was created within the ITU Council to this end. This means that internet governance is being officially discussed at the ITU. However, the Group has not produced any tangible results because it is being blocked by the United States and its partners in every way.

[100] Olga Melnikova, International Telecommunication Union - Technical Regulator or the New Confrontation Arena, International Affairs Magazine, 12 July 2021, https://interaffairs.ru/news/show/30759

“The Internet Corporation for Assigned Names and Numbers (ICANN) plays a key role in managing the Net. The Administration of the United States has a virtual monopoly over the Internet despite the fact that ICANN, which has been tasked with managing the Net, has officially been a non-profit organization since 2009. ICANN is accountable to the global multistakeholder community, in other words — to no one, and, for all intents and purposes, it is still controlled by the Administration of the United States.

“As part of their strategic partnership, Russia and China have been consistently speaking in support of internationalizing the governance of the global internet, expanding the role of governments in this process, and preserving their sovereign right to regulate the national internet segment.

“Making the ITU responsible for internet governance would be the optimal solution as it has the necessary expertise in this area. This modality runs counter to the fundamental approach of the United States as far as maintaining control over the internet is concerned, and, therefore, has every chance of being blocked by the United States.

“Americans are aiming to take sole control over the ITU to further their interests. Their compatriot, the Director of the ITU's Telecommunication Development Bureau (BDT) Doreen Bogdan-Martin, has been nominated to the position of the ITU Secretary-General (elections are to be held at the ITU's regular Plenipotentiary Conference in the fall of 2022). If she wins it will mean that all the real levers of power related to ICT will be concentrated in the hands of the United States. This may become yet another threat to international information security (IIS) and destroy the already delicate balance in this area.

“Even in her very politically delicate post of the director of BDT, the American woman still holds the levers she can use to influence governments by interacting with them via the ITU's regional offices and by handing out generous promises to developing countries which remain on paper, as was the case, for example, at the World Telecommunication Development Conference in 2017 in Buenos Aires.

“R. Ismailov, Russia's candidate, has a radically different approach to managing the ITU. He is a professional, with extensive experience in managing the most technologically advanced companies — Ericsson, Nokia, Huawei. The former Deputy Minister of Communications of Russia (2014-2018) and current president of VimpelCom (Beeline brand) believes that the most important element of the technology sector is people.

“R. Ismailov's election campaign is built on the premise that the digital revolution, which has enabled mass adoption of technologies that used to be expensive and complex, has also created an enormous potential for conflict. Today's biggest challenge is adapting and humanizing modern technologies and reconciling people with the new digital world.

“ITU is meant to restore trust in ICT by minimizing crisis processes related to its use. It is important to acknowledge that technological advances are not done for their own sake but to improve the lives and security of people. According to Russia's candidate, the ITU should create equal opportunities in the area of telecommunications and ICT, thus preventing the growth of economic inequality between countries. The efforts of the world community, including the ITU, should be aimed at overcoming the digital divide.

“To ensure a stable, sustainable, and safe digital space, making the ITU more actively involved in multilateral efforts to ensure international information security should be a priority. Everyone on the planet should have access to ICT and the Internet by 2030. The ITU's potential should be used in areas such as information security, healthcare, and development of uniform artificial intelligence standards. R. Ismailov believes that strengthening cooperation between ITU member states and expanding engagement with the private sector and academia are fundamental for ITU's work. The Russian candidate's election campaign for the high-level position of ITU Secretary-General as well as Russia's approach to the work of this respected international agency are aimed at developing a depoliticized dialogue and expanding constructive cooperation between all stakeholders.”

Appendix 2

Decree No. 943 Dated 19 June 2021, “On Introducing Changes to the Decree On the Ministry of Digital Development, Communications, and Mass Media and on Repealing Some Laws of the Government of the Russian Federation”[101]

Under the new decree the MoC is solely responsible for regulating:

“Requirements for communications networks and relevant use of number resources; requirements for building communications networks, for relevant communication equipment and for managing communications networks; requirements for assigning numbers, for protecting communications networks from unauthorized access and for protecting information transmitted across them; requirements covering the use of the radiofrequency spectrum; requirements covering the procedure to be followed by ISPs for providing internal telecommunications services; requirements for maintaining separate records of income and expenses related to the different lines of business, communications services provided and parts of telecommunications network that are used to provide these services by ISPs that play a significant role within the public communications network; requirements for information system security, including information systems for personal data (excluding information systems for critical infrastructure), information and telecommunications networks and other communications networks; requirements for the data format used in government information systems; requirements covering the functioning of communications network management systems when threats to the stability, security and integrity of the internet within the Russian Federation and to the public communications network arise; by agreement with the Federal Security Service of the Russian Federation, requirements for the functioning of Internet exchange points, which include requirements for ensuring the stability of communications hardware and software and structures; requirements to be satisfied by the operators, owners and other proprietors of communications networks that have a unique identifier for the aggregate means of communication and other technical equipment connected to the Internet [hereinafter – AS number holders], for ensuring the stability of communications equipment used for communicating with communications equipment of AS number holders, including those located outside the borders of the Russian Federation; requirements for AS number holders, covering the functioning of communications hardware and software (including communications equipment) used for identifying network addresses on the Internet that match domain names; by agreement with authorized government agencies involved in domestic intelligence activities or in ensuring the security of the Russian Federation, requirements to be satisfied by communications networks and equipment of AS number holders for the purposes of enabling authorized government agencies involved in domestic intelligence activities or in ensuring the security of the Russian Federation in cases defined by federal laws, to perform tasks assigned to them; requirements that cover traffic transmission and routing procedures; requirements that cover communication between communications networks that comprise the single unified telecommunications network of the Russian Federation; requirements that cover descriptions of communications networks and equipment that comprise the single unified telecommunications network of the Russian Federation; requirements for designing, building, rebuilding and operating communications networks and structures; requirements for providing communications services, including universal ones; regulation governing Russia's numbering system and plan; procedure for

[101] Government of the Russian Federation, Decree No. 943 Dated 19 June 2021, “On Introducing Changes to the Decree On the Ministry of Digital Development, Communications, and Mass Media and on Repealing Some Laws of the Government of the Russian Federation”, Official Legal Information Internet Portal, 24 June 2021, http://publication.pravo.gov.ru/Document/View/0001202106240011

assigning numbers to dedicated communications networks; procedure for assigning numbers to the part of the communications network that connects to the public communications network."