Vestnik RUDN. International Relations. ISSN 2313-0660 (print), ISSN 2313-0679 (online)
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2022 Vol. 22 No. 2 342—351
http://journals.rudn.ru/international-relations

SCIENTIFIC SCHOOLS

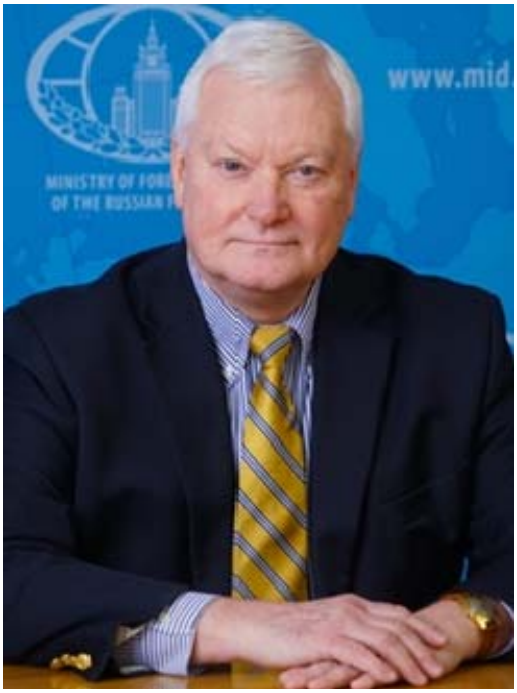
НАУЧНЫЕ ШКОЛЫ

DOI: 10.22363/2313-0660-2022-22-2-342-351

International Information Security: In Search of Consolidated Approaches

Interview with ANDREY V. KRUTSKIKH,
Special Representative of the President of the Russian Federation
for International Cooperation in the Field of Information Security,
Ambassador Extraordinary and Plenipotentiary,
Acting Director of the Department of International Information Security
of the Russian Ministry of Foreign Affairs

Abstract. Andrey Vladimirovich Krutskikh is the Special Representative of the President of the Russian Federation for International Cooperation in the field of Information Security since 2014, and a leading expert in this field in Russia and around the world. He served as Chairman of the UN Panel of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the SCO Member States Panel of Experts on International Information Security (IIS). Since 2020, A.V. Krutskikh holds the position of Director of the Department for International Information Security (DIIS) of the Ministry of Foreign Affairs of Russia, since 2017 he is Director of the Center for International Information Security, Science and Technology Policy of MGIMO University. Andrey Vladimirovich is the author of fundamental works devoted to IIS issues, the scientific editor of the three volume comprehensive textbook "International Information Security: Theory and Practice," prepared by the CIIS team of authors. During the interview A.V. Krutskikh spoke about Russia's approaches to international information security, the role of our country in developing the rules of the responsible State behavior in the global information space.



Key words: international information security, information and communications technologies, United Nations, Russia, United States, China

For citation: Krutskikh, A. V. (2022). International information security: In search of consolidated approaches : Interview with Andrey V. Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security. Interviewed by D. A. Piskunov. *Vestnik RUDN. International Relations*, 22(2), 342—351. https://doi.org/10.22363/2313-0660-2022-22-2-342-351

Международная информационная безопасность: в поисках консолидированных подходов

Интервью с АНДРЕЕМ ВЛАДИМИРОВИЧЕМ КРУТСКИХ, Специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Чрезвычайным и Полномочным Послом, директором Департамента международной информационной безопасности МИД России

Аннотация. Андрей Владимирович Крутских — Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности с 2014 г., ведущий эксперт в данной сфере в России и в мире. Он занимал должность председателя Группы правительственных экспертов ООН по достижениям в сфере информации и телекоммуникаций и Группы экспертов государств — членов ШОС по международной информационной безопасности (МИБ). С 2020 г. А.В. Крутских является директором Департамента международной информационной безопасности (ДМИБ) МИД России, с 2017 г. — директором Центра международной информационной безопасности и научно-технологической политики (ЦМИБ) МГИМО МИД России. Андрей Владимирович — автор фундаментальных работ, посвященных вопросам МИБ, научный редактор комплексного учебного пособия «Международная информационная безопасность: теория и практика» (в трех томах), подготовленного авторским коллективом ЦМИБ. В ходе интервью А.В. Крутских рассказал о подходах России в области МИБ, роли Российской Федерации в выработке правил ответственного поведения государств в глобальном информационном пространстве.

Ключевые слова: международная информационная безопасность, информационно-коммуникационные технологии, ООН, РФ, США, КНР

Для цитирования: *Крутских А. В.* Международная информационная безопасность: в поисках консолидированных подходов : интервью с Андреем Владимировичем Крутских, Специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности / интервью провел Д. А. Пискунов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 342—351. https://doi.org/10.22363/2313-0660-2022-22-2-342-351

— Russia initiated of the process of developing norms, rules and principles of responsible State behavior in the field of ICTs at the UN in 1998. Significant progress in this area was achieved through cooperation with regional associations — the Commonwealth of Independent States (CIS), the Collective Security Treaty Organization (CSTO), the Shanghai Cooperation Organization (SCO), BRICS, the Association of Southeast Asian Nations (ASEAN), the Arab League, and the African Union. Does this mean that Russia is one of the leaders in ICTs norm setting?

— Russia stood at the origins of the discussion of the problems of ensuring international information security (IIS). In 1998 our country submitted a draft resolution "Developments in the field of informatization and telecommunications in the context of international security"[1] to the First Committee of

[1] Resolution A/RES/53/70 adopted by the General Assembly "Developments in the field of information and

the UN General Assembly. The document proposed by the Russian Federation was supported by the vast majority of the UN Member States.

Negotiation process evolved gradually. In 2001, Russia initiated the creation of the UN Group of Governmental Experts (GGE), a forum where the representatives of 15—25 States took part in their personal capacity (Biryukov & Alborova, 2019). The goals of this mechanism evolved from studying threats in the ICTs sphere to developing norms, rules and principles of responsible State behavior in the information space. The work of the GGE proved its efficiency, thus basic principles of cooperation in the field of IIS were enshrined in the final reports of 2010, 2013 and 2015,[2] adopted by consensus. In particular, 11 voluntary norms recommended by the GGE 2015 were included in the initial set of international rules, norms and principles of responsible behavior of States, enshrined in the resolution of the UN General Assembly No. 73/27 proposed by Russia.[3]

Over time, the circle of States that wished to participate and had the right to vote in the UN discussion on IIS has expanded. In response to the request from the international community, in 2018 Russia proposed the creation of the new negotiating mechanism — the UN Open-ended Working Group (OEWG). Its fundamental difference from the GGE was the ability of all UN Member States without exception to participate "on an equal footing" in the specific decisions in the field of IIS and to defend the interests of national security. The OEWG, known as the "Cyber General Assembly," is the first universal, inclusive, transparent and truly democratic negotiating mechanism on IIS issues in the UN system (Zinovieva, 2020). Despite the difficulties caused by the pandemic, the OEWG successfully completed its activities in March 2021 and adopted final report by consensus of all 193 UN Member States.[4]

On December 31, 2020, with the support of an impressive majority of States, the UN General Assembly during its 75th session approved the Russian draft resolution deciding to convene a new OEWG on security of and in the use of information and communications technologies in 2021—2025 starting from 2021.[5] This decision confirms the relevance and necessity of ensuring the global negotiation process on IIS issues.

It is worth noting that the new OEWG is authorized to discuss profile proposals put forward by States, issues of capacity building, as well as establishing a dialogue between States (with the leading role of Governmental representatives), business, non-governmental

telecommunications in the context of international security" // The United Nations. January 4, 1999. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&Lang=E (accessed: 01.04.2022).

[2] See: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201) // The United Nations. July 30, 2010. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&Lang=E (accessed: 01.04.2022); Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98) // The United Nations. June 24, 2013. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&Lang=E (accessed: 01.04.2022); Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174) // The United Nations. July 22, 2015. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement (accessed: 01.04.2022).

[3] Resolution adopted by the General Assembly on 5 December 2018 "Developments in the Field of Information and Telecommunications in the Context of International Security" (A/RES/73/27) // The United Nations. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement (accessed: 01.04.2022).

[4] Developments in the Field of Information and Telecommunications in the Context of International Security // The United Nations. March 18, 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/72/PDF/N2106872.pdf?OpenElement (accessed: 01.04.2022).

[5] Resolution adopted by the General Assembly on 31 December 2020 "Developments in the field of information and telecommunications in the context of international security" A/RES/75/240 // The United Nations. January 4, 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement (accessed: 01.04.2022).

organizations and the scientific and academic community.

The success of the Group depends on a number of factors, among which substantive discussion is the key one. It is fundamentally important to give to the activities of OEWG the most pragmatic character, so that the result of its work would be practice-oriented norms, recommendations and assistance programs.

Undoubtedly, significant progress in this direction has been achieved in cooperation with regional IGOs. Russia is actively cooperating with the Member States of CIS, CSTO, SCO, BRICS, ASEAN, the Arab League, and the African Union. The work is aimed at agreeing on specific solutions to ensure IIS. The development of norms, rules and principles of responsible States behavior is being actively discussed in BRICS and SCO. Counteracting ICTs crime is one of the key aspects of the discussion between CSTO, CIS, ASEAN Regional Forum (ARF), and ASEAN. A conceptual apparatus in the field of the safe use of ICTs is being developed within the framework of ASEAN. Russia has also concluded a number of bilateral intergovernmental agreements that allow deepening the dialogue with like-minded States in the field of IIS (Krutskikh & Biryukov, 2017).

We can say that Russia continues to set the tone for international cooperation in this area, seeking to develop rules for responsible States behavior under the auspices of the UN, which should be based on such principles as sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.[6]

— **What scientific schools in the field of IIS, in your opinion, have developed in the world today? What research initiatives, which of authoritative experts can you mention in this regard? Could they be divided into several groups depending on the approaches?**

— Currently, public diplomacy plays an important role in international cooperation. Representatives of the scientific and academic community are actively involved in the discussion of various aspects of the IIS. On the basis of MGIMO University, the Center for International Information Security and Science and Technology Policy (CIIS) was founded, which is actively involved in the discussion of the use of ICTs within the OEWG framework, as well as regional and bilateral platforms.[7] In March 2022, the CIIS staff took part in an informal online meeting held by the OEWG Chairman B. Gafur with representatives of interested non-state parties, and later the CIIS analytical report on Russia's main approaches to IIS was published on OEWG's official site (Krutskikh & Zinovieva, 2021). In addition, the staff of the Center regularly delivers presentations at events organized by the CIS, CSTO, SCO, BRICS, ARF and ASEAN.

CIIS makes an important contribution to the professional personnel training. In 2019, a three-volume textbook "International Information Security: Theory and Practice" (Krutskikh, 2019) was published, which was republished and supplemented in 2021 (Krutskikh, 2021). This is the world's first comprehensive publication on this topic, which is actually a scientific ontology on IIS. On the basis of the textbook, innovative digital educational complex "International Information Security: Theory and Practice" was prepared, which after was nominated for the Russian Government Prize in the field of education for 2021 and included in the "short list" of nominees.

[6] Resolution adopted by the General Assembly on 31 December 2020 "Developments in the field of information and telecommunications in the context of international security" A/RES/75/240 // The United Nations. January 4, 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement (accessed: 01.04.2022).

[7] Center for International Information Security and Science and Technology Policy // MGIMO University. URL: https://mgimo.ru/about/structure/ucheb-nauch/ciis/ (accessed: 01.04.2022). (In Russian).

As part of the "Priority 2030" program, CIIS prepared the report "International Information Security: Russia's Approaches," which presents the most pressing problems of IIS in an accessible format for a wide audience, as well as comprehensively characterizes Russia's approaches to the formation of an international regime in the field of ICTs security on global, regional and bilateral levels (Krutskikh & Zinovieva, 2021). The report was presented at the UN platform and received wide recognition in the academic and diplomatic community.

In addition, on the basis of MGIMO University conferences, forums, seminars and round tables are held, where topical aspects of the digital agenda, that take into account promising areas of technological development and modern transformations of the international system, are discussed. Such an exchange of views contributes to the formation of a comprehensive understanding of the promising areas of domestic policy and interaction at the international level in this area.

We can say that a unique scientific school of MGIMO University in the field of international information security and science and technology policy has been formed around CIIS. The Center defends the national interests of the Russian Federation and provides expert support to the country's foreign policy in this field. Scientific works of CIIS are widely cited by Russian and foreign scientists and set the direction for further study of these issues and training new generation of researchers. The staff of the Center actively publishes articles in scientific journals, monographs, educational and methodical literature behind their authorship.

The practice-oriented direction of scientific research in the field of IIS is being formed on the basis of the National Association for International Information Security (NAIIS)[8] established in 2018. The President of the Association is the Advisor to the Secretary of the Security Council of the Russian Federation V.P. Sherstyuk, the members of the Association are the country's leading experts in the field of IIS. The Supervisory Board of NAIIS is headed by Oleg Khramov, Deputy Secretary of the Security Council of the Russian Federation. According to the Charter of the Association, one of its main goals is to promote the Russian initiatives in the field of providing IIS with the proactive study of problematic issues in the interests of forming the negotiating positions of State bodies. While the discussion of the draft "Fundamentals of the State Policy of the Russian Federation in the field of international information security" on March 26, 2021, President of Russia Vladimir Putin emphasized the role of NAIIS in the implementation of Russia's State policy in this area.[9]

Indeed, at a time when the collective West has unleashed an aggressive cyber war against Russia, interaction between the scientific and academic community is of particular importance since many contacts with Russia at the State level to ensure IIS have been interrupted. An in-depth expert conversation and a half-track diplomacy is a unique source of ideological "feeding" for Russia's efforts in the international arena and, at the same time, an objective and non-trivial look at the prospects for a multilateral discussion.

NAIIS, in turn, has great experience in holding international forums and conferences, for example, in Guatemala, Germany, China, Cuba, etc. In the context of the pandemic, the Association organized the forum "Partnership between the State, business and civil society in providing IIS," published collections of reports, as well as analytical, scientific and methodological works.[10]

[8] National Association for International Information Security (NAIIS). URL: https://namib.online/en/ (accessed: 01.04.2022).

[9] The President Held a Meeting of the Security Council via Videoconference, during Which the Draft "Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security" Was Considered [Президент провел в режиме видеоконференции заседание Совета Безопасности, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности»] // Security Council of the Russian Federation. March 26, 2021. (In Russian). URL: http://www.scrf.gov.ru/news/speeches/2952/ (accessed: 01.04.2022).

[10] Program XV International Forum "Partnership for State, Business and Civil Society in Ensuring International Information Security // NAIIS. September 24, 2021. URL:

Young researchers are also involved in the scientific research of the IIS and negotiation activities in this area. The driving force for promoting youth initiatives is the School of International Information Security of the Diplomatic Academy of the Ministry of Foreign Affairs of Russia, which regularly holds open lectures on its site on topical aspects of the IIS, participates in scientific conferences, seminars and round tables on specialized topics.[11]

Foreign researchers are also interested in the problem of providing IIS. It is impossible not to note the leading scientific centers of the People's Republic of China (PRC), which are engaged in the study of this area and applied work. First of all, we are talking about the China Internet Association,[12] the China Cyberspace Security Association,[13] the Committee Federation of Industry and Trade on the Operation and Maintenance of Big Data,[14] the "360" Security Center.[15] Considerable attention Chinese scientific and academic community gives to the study of global Internet governance. Yan Xuetong, Dean of the Institute of Contemporary International Relations, Tsinghua University, Editor-in-Chief of "China Journal on international politics", considers cyberspace as a key driver of the development of world politics and international relations. He highlights the global governance of cyberspace as a strategic area of confrontation between the US and China (Yan Xuetong, 2020). In addition, a special place in the literature of the PRC is occupied by the problem of technological competition between the United States and China and its consequences for the global governance of the Internet (Li Zhi & Tang Runhua, 2020). A number of authors consider the Chinese approach to global Internet governance in the context of national security and digital sovereignty (Xu Peixi, 2021; Wang Zheng, 2020).

The Leiden University Laboratory headed by R. Creemers is studying the problems of cybersecurity and the role of the PRC in its provision within the framework of the "China's Role in Cyber Security" project.[16] R. Creemers, professor at Leiden University and co-founder of the DigiChina project, explores China's regulation in the field of digital technologies as well as China's policy in global Internet governance (Creemers, 2022).

Bilateral relations between Russia and China are a comprehensive strategic partnership. Our countries adhere to similar views in the field of IIS — namely, support of the development of rules for the responsible States behavior in the information space under the auspices of the UN.

Western approaches differ from those promoted by Russia and China. The main achievement of the scientific school of the collective West in the field of IIS (it should be noted that the term "cybersecurity" is more often used in Western scientific discourse) is considered to be the publication of the Tallinn Manual and the Tallinn Manual 2.0 on the applicability of international humanitarian law to conflicts in cyberspace and cyber operations prepared by the staff of the NATO Cyber Defense Center in Tallinn under

https://namib.online/en/2021/09/program-xv-international-forum-partnership-of-state-business-and-civil-society-in-ensuring-international-information-security/ (accessed: 01.04.2022).

[11] IIS School // Diplomatic Academy of the Ministry of Foreign Affairs of Russia [Школа МИБ // Дипломатическая академия МИД России]. URL: https://www.dipacademy.ru/special-projects/mib-school/ (accessed: 01.04.2022). (In Russian).

[12] Zhongguo hulianwang xiehui [Internet Society of China]. URL: https://www.isc.org.cn (accessed: 01.04.2022). (In Chinese).

[13] Zhongguo wangluo kongjian anquan xiehui [Cyber Security Association of China]. URL: https://www.cybersac.cn (accessed: 01.04.2022). (In Chinese).

[14] Zhonghua quanguo gongshangye lianhehui [All-China Federation of Industry and Commerce]. URL: https://www.acfic.org.cn/zzjg_327/zmwyh/2021_wlaqwyh/2021_wlaqwyh_md (accessed: 01.04.2022). (In Chinese).

[15] 360 qiye anquan hui [Association of corporate security 360]. URL: https://www.360.cn (accessed: 01.04.2022). (In Chinese).

[16] China's Role in Cyber Security // Leiden Asia Centre. URL: https://leidenasiacentre.nl/chinas-role-in-cyber-security/ (accessed: 01.04.2022).

the guidance of professor of law M. Schmidt.[17] This publication is an academic work and is not legally binding, but it is aimed to promote the Western negotiating position on IIS, essentially legitimizing the use of ICTs for military purposes. It should also be noted that within the Western scientific school there are significant substantive and ideological divides.

In this context, I would like to note that Russia is in favor of more active involvement of business, NGOs and the scientific and academic community in the global discussion on IIS. In our opinion, the specificity of ICTs is such that representatives of non-state actors can make a significant meaningful contribution to solving the problems that international community faces in this area.

— **In 2020, the Chinese companies "China mobile" and "Huawei", with the support of interested ministries, put forward a proposal in the ITU working group on the development of new IP-address protocols that contribute to the further development of advanced technologies, including 5G. In your opinion, can the proposed standards become an alternative to the existing Internet protocols created at the request of the West?**

— The Corporation for the Management of Domain Names and IP Numbers (ICANN)[18] and its subsidiary, the Organization for Public Technical Identifiers (PTI),[19] play a key role in the Internet governance. Although ICANN is formally an independent non-profit organization, the US government actually controls the allocation of Internet names and numbers. The non-state status of ICANN acts as a "screen" designed to cover up the hegemony of the United States.

As for the International Telecommunication Union (ITU),[20] this specialized UN body is neither legally nor politically involved in Internet governance since its participation in this process is openly sabotaged by the United States and its partners. Russia has advocated the transfer of Internet governance prerogatives to the ITU, which has the necessary expertise and legitimacy in these matters (Zinovieva, 2009). Naturally, such proposals run counter to the principled approaches of the United States wishing to maintain control over the Network.

Russia and China have consistently advocated the internationalization of governance of the global Internet, increasing role of States in this process, as well as maintaining their sovereign right to regulate the national segment of the Internet (Krutskikh & Zinovieva, 2021). China is also actively involved in the adoption of universal standards in the field of 5G communication networks. On the part of China and Chinese companies, work is underway to develop new protocols for IP-addresses. All these actions are aimed at internationalizing international Internet governance and increasing the role of the global community in this process in order to make it inclusive and democratic (Tikk & Kerttunen, 2020). I repeat: the optimal institutional base for Internet governance is the ITU.

— **The United States has frozen cooperation with Russia on cybersecurity issues. Western countries accused Russia of harmful activities in the information space at a session of the UN Open-ended Working Group. How will the dialogue between Russia and the West continue developing in multilateral and bilateral formats to draw up convention on the provision of IIS?**

[17] Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence / ed. by M.N. Schmitt. Cambridge ; New York : Cambridge University Press, 2013. URL: https://assets.cambridge.org/97811070/24434/frontmatter/9781107024434_frontmatter.pdf (accessed: 01.04.2022).

[18] The Internet Corporation for Assigned Names and Numbers (ICANN). URL: https://www.icann.org/en (accessed: 01.04.2022).

[19] Public Technical Identifiers (PTI). URL: https://pti.icann.org/ (accessed: 01.04.2022).

[20] International Telecommunication Union. URL: https://www.itu.int/ru/Pages/default.aspx (accessed: 01.04.2022).

— Russia and the United States are countries that have a special responsibility for maintaining global peace and security. Our interaction took place in different ways, but with Russia's invariable attitude towards achieving practical results.

On September 25, 2020, the President of the Russian Federation Vladimir Putin presented a comprehensive program of practical measures to restore Russian-US cooperation in the field of IIS.[21] The program was focused on increasing the level of trust, resetting relations with the United States in order to prevent large-scale confrontation in the digital environment and included the following areas.

First. To restore a regular full-scale bilateral interagency high-level dialogue on the key issues of ensuring IIS.

Second. To maintain a continuous and effective functioning of the communication channels between competent agencies of our States through Nuclear Risk Reduction Centers, Computer Emergency Readiness Teams and high-level officials in charge of the issues of IIS within the bodies involved in ensuring national security, including that of information.

Third. To jointly develop and conclude a bilateral intergovernmental agreement on preventing incidents in the information space similarly to the Soviet-American Agreement on the Prevention of Incidents On and Over the High Seas in force since 25 May 1972.

Fourth. To exchange, in a mutually acceptable format, guarantees of non-intervention into internal affairs of each other, including into electoral processes, inter alia, by means of the ICTs and high-tech methods.

In addition, the President of the Russian Federation Vladimir Putin proposed to conclude reaching a global agreement on a political commitment of States on no-first-strike with the use of ICTs against each other. There was no substantive response to our proposal.

After the July 2021 summit in Geneva, a specialized expert dialogue was launched between Russia and the United States in "the Kremlin — White House" format under the auspices of the Office of the Security Council of the Russian Federation and the US National Security Council.[22] The exchange of operational information on cybercrime was established, the volume and quality of information on computer incidents transmitted between the National Coordination Center for Computer Incidents of Russia and the US Agency for Cybersecurity and Infrastructure Protection was increased. Bilateral cooperation between the Prosecutor General's Office of the Russian Federation and the US Department of Justice has intensified. Nevertheless, despite the positive experience of interaction in this area, in the spring of 2022, the White House unilaterally withdrew from the permanent channel of communication with the Kremlin. In addition, Washington refused to further discuss the security of critical information infrastructure. All joint work to stop the activities of cybercriminals was also stopped. The United States refused the Russian proposal to deanonymize the Internet and forced its allies not to support our initiative to adopt an international legally binding document regulating the activities of States in the information space.

Due to the one-sided and destructive position of the collective West, the overall level of information security in the world is declining. The number of cyberattacks has been on the rise in recent years. Since the beginning of 2022, Western countries have repeatedly

[21] Statement by Vladimir Putin on a Comprehensive Program of Measures to Restore Russian-American Cooperation in the Field of International Information Security [Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности] // President of Russia. September 25, 2020. (In Russian). URL: http://kremlin.ru/events/president/news/64086 (accessed: 01.04.2022).

[22] The White House and the Kremlin Agreed That Dialogue Is the Best Way to De-escalate [Белый дом и Кремль согласились, что диалог — лучший способ деэскалации] // Interfax. December 31, 2021. (In Russian). URL: https://www.interfax.ru/world/813561 (accessed: 01.04.2022).

increased attacks on our country — up to a million a week.

On May 20, 2022, under the chairmanship of the President of the Russian Federation Vladimir Putin, a meeting of Security Council of the Russian Federation was held, where the issues of information security were discussed.[23] The President of Russia noted that targeted attempts to disable online resources of critical information infrastructure in Russia have been detected. Media outlets, financial institutions and widely used public websites and networks have been hit the hardest. In addition, one of the tools of sanctions' pressure on Russia involved restrictions on foreign IT products and software. A number of Western tech companies unilaterally cut off Russia from technical support services for their equipment. Incidents where their products became limited or blocked have become more frequent.[24] But even today it can be said that the cyber aggression against Russia, as well as the sanctions attack on Russia in general, failed. In general, we were ready for this attack, and this is the result of the systematic work that has been carried out over the past years.[25]

Regardless of the geopolitical situation, Russia remains open to dialogue and cooperation on the principles of mutual trust and respect for national interests with all States, and the United States is no exception in this sense.

As for the Convention on International Information Security, the idea was first introduced by Russia at a meeting of high representatives in charge of security issues in Yekaterinburg in 2011. At that time, 52 States acted as co-authors of the Russian draft.[26] Russia submitted an updated draft of the Convention in 2021. Today, OEWG is the key platform for discussing the provisions of the future Convention. In order to maintain strategic stability and ensure protection against cyber threats, it is not enough to have norms that are voluntary and recommendatory in nature; we need the legal consolidation of the "rules of the road" in the ICTs environment.

— In your opinion, will the process of technological decoupling between the West adhering to the cybersecurity paradigm, and non-Western countries, advocating the concept of international information security and sovereign control of the internal segment of the Internet be accelerated in the future?

— The tendencies of recent years, and especially months, testify to the fact that the split of the world community into the West and non-Western continues.

The goal of the United States and NATO is to restore and consolidate forever their dominance in international affairs in favour of their selfish goals to the detriment of the national interests of other members of the international community. They promote the notorious "rules-based world order," which in practice means the consolidation of "the right of the strongest" in world affairs, which contradict the traditional understanding of the international law.

Russia and like-minded countries stand for the development of comprehensive cooperation in the field of IIS, taking into account the interests of all States. The primary task is to develop the international legal framework

[23] Vladimir Putin Chaired a Meeting of the Security Council of the Russian Federation via Videoconference [Под председательством Владимира Путина в режиме видеоконференции состоялось заседание Совета Безопасности Российской Федерации] // Security Council of the Russian Federation. May 20, 2022. (In Russian). URL: http://www.scrf.gov.ru/news/allnews/3240/ (accessed: 21.05.2022).

[24] Vladimir Putin Chaired a Meeting of the Security Council of the Russian Federation via Videoconference [Под председательством Владимира Путина в режиме видеоконференции состоялось заседание Совета Безопасности Российской Федерации] // Security Council of the Russian Federation. May 20, 2022. (In Russian). URL: http://www.scrf.gov.ru/news/allnews/3240/ (accessed: 21.05.2022).

[25] Security Council Meeting [Заседание Совета Безопасности] // President of Russia. May 20, 2022. (In Russian). URL: http://kremlin.ru/events/president/news/68451 (accessed: 21.05.2022).

[26] Russia Has Indicated a Solution for the Internet [Россия указала выход для Интернета] // Kommersant. September 23, 2011. (In Russian). URL: https://www.kommersant.ru/doc/1779208 (accessed: 01.04.2022).

for the activities of countries, as well as non-governmental entities in the field of ICTs.

The current situation in the global arena is hardly conducive to optimistic forecasts. However, security in the cyber sphere requires international agreements. The stakes are too high to rely on a game without rules.

It is impossible to have a cyber world order where individual States seek to strengthen their security at the expense of the security of others. It is necessary for the entire global community to work out norms aimed at preventing conflicts in the information space, promoting the peaceful use of ICTs, preventing their use for criminal and terrorist purposes, as well as continuing relevant negotiations with the central role of the UN. Otherwise, as Sergey Lavrov declared, the world is threatened with cyberanarchy.[27]

[27] Speech by the Minister of Foreign Affairs of the Russian Federation S.V. Lavrov at the Plenary Session "International Relations in the Context of Digitalization of Public Life" of the International Scientific and Practical Conference "Digital International Relations 2022", Moscow, April 14, 2022 [Выступление Министра иностранных дел Российской Федерации С.В. Лаврова на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» международной научно-практической конференции «Цифровые международные отношения 2022», Москва, 14 апреля 2022 года] // Russian Ministry of Foreign Affairs. April 14, 2022. (In Russian). URL: https://www.mid.ru/ru/foreign_policy/news/1809294/ (accessed: 01.05.2022).

Interviewed by D.A. Piskunov / Интервью провел Д.А. Пискунов

Received / Поступила в редакцию: 10.05.2022

References

Biryukov, A. V., & Alborova, M. B. (2019). *Socio-humanitarian dimension of international information security.* Moscow: Aspekt Press publ. (In Russian).

Creemers, R. (2022). *China's cybersecurity regime: Securing the smart State*. Leiden University. P. 1—38. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070682

Krutskikh, A. & Zinovieva, E. (Eds.). (2021). *International information security: Russia's approaches*. Moscow.

Krutskikh, A. V. (Ed.). (2019). *International information security: Theory and practice* : in 3 volumes. Moscow: Aspekt Press publ. (In Russian).

Krutskikh, A. V. (Ed.). (2021). *International information security: Theory and practice* : in 3 volumes. Moscow: Aspekt Press publ. (In Russian).

Krutskikh, A., & Biryukov, A. (2017). International science and technology relations as a new geopolitical reality. *International Trends*, (2), 6—26.

Li, Zhi, & Tang, Runhua. (2020). Duo li yi you guan fang mo shi : gou jian quan qiu hu lian wang zhi li ti xi de lu jing yan jiu [Multistakeholder model: Pathway to a global Internet governance system]. *Chuan mei guan cha [Media Observer]*, 444(12), 21—28. (In Chinese).

Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity*. Routledge.

Wang, Zheng. (2020). Lian he guo "shuang gui zhi" xia quan qiu wang luo kong jian gui ze zhi ding xin tai shi [Global internet governance towards a digital Cold war or digital commons]. *Zhong guo xin xi an quan [Information security of China],* 20(1), 40—43. (In Chinese).

Xu, Peixi. (2021). 2020 shu zi leng zhan yuan nian: wang luo kong jian quan qiu zhi li de liang zhong lu xian zhi zheng [Year of the digital Cold war 2020: The battle of the two paths of global governance in cyberspace]. *Xin xi an quan yu tong xin bao mi [Information Security and Communication Confidentiality]*, 21(3), 16—23. (In Chinese).

Yan, Xuetong. (2020). Bipolar rivalry in the early digital age. *The Chinese Journal of International Politics*, 13(3), 313—341. https://doi.org/10.1093/cjip/poaa007

Zinovieva, E. S. (2009). *International internet governance: Conflict and cooperation*. Moscow: MGIMO publ. (In Russian).

Zinovieva, E. S. (2020). *International information security: Problems of multilateral and bilateral cooperation*. Moscow: MGIMO publ. (In Russian).