Russian Journal of World Politics and Law of Nations. 2022. 1(1-2). P. 4–22 Research Article
DOI 10.24833/RJWPLN-2022-1-2-4-22

Political and Legal Framework of the International Information Security System: Russian Approaches and Initiatives[1]

Sergey M. Boyko

Office of the Security Council of the Russian Federation

Abstract. The present article covers the state policy of the Russian Federation in the field of international information security. The purpose of the study is to identify the key directions for strengthening international cooperation in the area of information security. The article examines the state of bilateral cooperation on international information security issues, in particular on the example of the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of International Information Security. The article analyses Russian initiatives put forward in regional and multilateral organizations. Thus, special attention is paid to cooperation within BRICS, the SCO, the CSTO and ASEAN. Regional and interregional interaction in this area increases the stability and security of the respective regions, taking the national interests of the parties involved into account. The article also studies Russian projects promoted at the global level, namely, the UN General Assembly resolutions proposed by the Russian Federation. Russia and its partners contributed to the adoption of a set of 13 international rules, principles and norms of responsible behaviour of states in the information space. The convocation of an Open-Ended Working Group, whose mandate has been extended until 2025, has become an important contribution of Russia to institutionalization of the discussion mechanism within the United Nations. The author concludes that Russian projects and cooperation agreements reached can foster the development of a political and legal framework of the international information security system. The focus on promoting the formation of such a system is confirmed by the updated Basic Principles of State Policy of the Russian Federation in the Field of International Information Security. However, these initiatives are not exhaustive. Therefore, the formation of such a system requires the efforts of the entire world community.

Keywords: international information security; foreign policy of the Russian Federation; state policy of the Russian Federation; international cooperation

[1] English translation from the Russian text: Boyko S.M. 2021. Politiko-pravovye predposylki sistemy mezhdunarodnoi informatsionnoi bezopasnosti. *Mezhdunarodnye protsessy* [International Trends]. Vol. 19, no. 4, p. 6-25. DOI: 10.17994/IT.2021.19.4.67.4. (In Russian).

Rapidly escalating threats in the information sphere require an adequate response from the state, society and citizens. The unlawful impact on the information infrastructure by states pursuing their destructive military-political, terrorist, extremist and criminal goals can only be countered through a comprehensive approach to building a system of international information security (IIS) at the bilateral, multilateral, regional and global levels.

It is a focus of Russia's state policy in the field of IIS to promote the development of such a system, the foundations of which were laid in 2021 in a strategic planning document devoted to the issue entitled "Basic Principles of State Policy of the Russian Federation in the Field of International Information Security."[2] The updated version of this document defines an "IIS system" as a set of international and national institutions that regulate activities in the global information space in order to prevent (minimize) threats to IIS.[3]

The problems of creating an IIS system and approaches to building international cooperation to form appropriate legal frameworks and develop practical measures have been addressed by a number of Russian and foreign authors.

Russian researchers have traditionally paid special attention to the political aspects of this problem, including the prospects for creating an international system of information security through the prism of Russian and US initiatives at the United Nations (Sebekin 2020); the formation of international regimes of information security at various levels (Zinovyeva 2019, 2021); the state and possibilities of developing a political and legal framework for cooperation in ensuring IIS (Krutskikh 2007, 2014); the applicability of international responsibility law to the behavior of states in cyberspace (Krasikov 2018); and potential areas of Russian–American cooperation in the field of IIS in the context of the progressive development of international law and its adaptation to the specifics of the ICT environment as a new area of international cooperation (Smirnov, Streltsov 2017).

In turn, authors outside of Russia put more emphasis on the legal component of the problems addressed. They tend to focus on issues of state responsibility for internationally unlawful acts in cyberspace and the development of rules for attributing such acts to a particular state (Antonopoulos 2015); analyse the principles of state responsibility and progress in the development of basic rules of behaviour in international law with regard to cyberspace (Jensen 2017); assess both the role of the United Nations in regulating cybersecurity issues and the need for further concerted action in general (Henderson 2015); consider the creation of norms of state behaviour to ensure stability in cyberspace[4]; and explore the legal status of cyberspace and its sovereignty and

[2] Basic Principals of State Policy of the Russian Federation in the Field of International Information Security. URL: http://publication.pravo.gov.ru/Document/View/0001202104120050. (In Russian).

[3] Ibid.

[4] Nye J. 2018. How Will New Cybersecurity Norms Develop? *Project Syndicate*. URL: https://www. project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03?barrier=accesspaylog (accessed: 01.01.2022); Nye J. 2019. Rules of the Cyber Road for America and Russia. *Project Syndicate*. URL: https://www.project-syndicate.org/commentary/cyber-rules-for-america-and-russia-by-joseph-s--nye-2019-03?barrier=accesspaylog (accessed: 01.01.2022).

the potential challenges in developing a comprehensive and globally negotiated treaty establishing rules of behaviour, prohibiting certain activities, and establishing rules of jurisdiction (Tsagourias 2016).

An analysis of the relevant literature shows that the studies on the problems of creating an IIS system carried out by Russian and foreign scholars and experts share a comprehensive approach, emphasizing the need for cooperation between stakeholders to counter the full range of challenges and threats in the information sphere.

If in the past, priority was given to the so-called triad of threats (threats to the use of information and communication technologies, or ICT, for destructive military and political purposes in order to to undermine the sovereignty and territorial integrity of states for terrorist and other criminal purposes), today, researchers in Russian and around the world more often focus on "new threats," which have been growing in recent years and directly affect the formation of the IIS system.

Such relatively new threats include the use of ICTs to cause economic damage, including through destructive impact on the information infrastructure, as well as to promote extremism, terrorism and separatism, attracting new supporters to extremist and terrorist organizations. Scientists and experts point to the growing threat of using ICTs to interfere in the internal affairs of states, disrupt public order, incite ethnic, racial, and religious hatred, promote racist and xenophobic ideas and theories, destabilize the internal political and socio-economic situation, and disrupt the state governance system. The threat of the dissemination of information that is harmful to the socio-political and socio-economic system, and to the spiritual, moral, and cultural environment of states, is getting more and more serious.

The listed IIS threats are covered in detail in the works by Russian authors such as Yelena Batuyeva, Valery Vasenin, Yelena Zinovyeva, Oleg Kazarin, Vladimir Skiba, Rinat Sharyapov, Anatoly Kapustin, Anatoly Smirnov, and Andrei Krutskikh (Batuyeva 2014; Vasenin 2004; Zinovyeva 2019; Kazarin, Skiba, Sharyapov 2016; Kapustin 2015; 2017; Smirnov 2016; Krutskikh 2021). They are also covered in foreign publications (Ambos 2015; Buchan 2018; Weimann 2015; Jensen, Watts 2017; Kastner, Megret 2015; Kerschischnig 2012; Lewis, Stewart 2013; Saul, Heath 2014; Hua, Bapna 2013). The global nature of these threats and the scale of the possible consequences of their implementation necessitate the creation of a multi-level IIS system.

The legal basis for each level of this system can be provided by international treaties on cooperation in the field of IIS. Such treaties make it possible not only to fix the common approaches of cooperating parties, but also to guarantee their mutual security against threats in the information sphere. The format of treaties may vary, due to the peculiarities of the legal systems of the states that reach agreements on cooperation. For example, according to Federal Law No. 101-FZ "On International Treaties of the Russian Federation" dated July 15, 1995, international treaties shall be concluded with foreign states, international organizations and other entities on behalf of states (interstate treaties), governments (intergovernmental treaties) and government bodies or authorized organizations (interdepartmental treaties).[5] Russian law, as well as the laws of other states, provides for various types of international legal instruments: treaties, agreements, conventions, protocols, exchanges of letters or notes, and other types and names of international treaties.

When states with different legal systems reach agreements on cooperation in the field of ensuring IIS, such variability makes it possible to find mutually acceptable approaches to the legal frameworks for cooperation. In general, international treaties form a multilevel legal framework of interstate relations in the field of ensuring IIS, which contributes to the maintenance of peace, security and stability in the global information space, while also promoting international cooperation in accordance with the purposes and principles of the Charter of the United Nations.

Bilateral Cooperation at the Heart of IIS System

The legal framework at the bilateral level of the IIS system is formed by international treaties concluded between two states. Such treaties help establish practical cooperation between interested parties since they clearly outline the main areas of cooperation.

The Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in International Information Security dated May 8, 2015,[6] for example, provides for a mechanism of cooperation between authorized bodies to exchange and share information on existing and potential information security risks, threats and vulnerabilities. This includes identifying, assessing, studying, detailing, and preventing such phenomena. Measures related to the joint response to IIS threats and the creation of appropriate channels of communication and contact are of a more hands-on nature.

The practical side includes cooperation between the competent authorities of Russia and China in the field of critical information infrastructure security, technology exchange, and cooperation between authorized bodies in responding to computer incidents. Information sharing and collaboration in law enforcement in the investigation of cases involving the use of ICTs for terrorist and criminal purposes are of great importance to ensure protection against information threats.

The development and implementation of necessary joint confidence-building measures in this area, as well as interaction in the development and promotion of international law to ensure national and international information security are sub-

[5] Federal Law No. 101-FZ "On International Treaties of the Russian Federation" (amended and supplemented) dated July 15, 1995. URL: https://www.consultant.ru/cons/cgi/online.cgi9req=doc&base=LAW&n=370228&dst=1000000001%2C0#04556996730220404. (In Russian).

[6] Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of International Information Security dated May 8, 2015. URL: http://publication.pravo.gov.ru/Document/View/0001201608100001. (In Russian).

ordinate to the idea of creating an IIS system at the bilateral level. Key areas for cooperation include promoting scientific research, conducting joint research projects, training specialists, developing exchange programmes for students, graduate students and teachers at field-specific institutions of higher education. Along with solving the tasks set, great importance is attached to cooperation between Russia and China and coordination of their efforts within the framework of international organizations and forums, along with working meetings, conferences and seminars involving authorized representatives and experts. The above-mentioned areas of cooperation between Russia and China largely guarantee interaction between the parties in combating IIS threats.

Russia has similar intergovernmental agreements with Belarus, Brazil, Cuba, India, Indonesia, Iran, Kyrgyzstan, Nicaragua, Turkmenistan, South Africa, Uzbekistan, and Vietnam. Mutual agreements allow for effective systemic cooperation at the bilateral level. At the very least, the existing commitments guarantee information security from possible destructive influences on the part of the partner. The growing number of bilateral agreements forms an extensive web of security, providing the foundation for a global IIS system.

First, Russia has signed intergovernmental agreements with its allies in the Commonwealth of Independent States (CIS), the Shanghai Cooperation Organisation (SCO) and BRICS, as well as with its traditional partners and countries that share Russia's approach to building the IIS system. These are mostly framework agreements, setting out the main areas of cooperation between the parties and outlining procedural issues. Practical cooperation is based on specific plans for the implementation of these areas. The list of nations cooperating with Russia in this vital area is not limited to the countries mentioned above. Moreover, it is impossible to build this system on the basis of blocs alone: it is necessary to interact on a mutually beneficial basis without regard to political preferences and affiliation with this or that bloc.

It is this approach of Russia, a state with strong ICT capabilities that ranks high on the global "table of ranks" that drives the desire of many states to build pragmatic bilateral relations with Russia. The priorities for Russia's partners include ensuring information security, cooperating in the most sensitive areas related to the protection of critical infrastructure, and preventing the use of ICTs for criminal purposes. In some cases, political divisions and different approaches do not prevent many Western countries, including the United States, France, Germany, the Netherlands, South Korea and Japan, from engaging in a dialogue with Russia. Regular interagency consultations help reach a better understanding, bridge positions, increase confidence, and resolve potentially dangerous situations.

The practical result of such cooperation is the reduction in the number of computer attacks on the information resources of cooperating parties and the coordination of joint efforts in the fight against cybercriminals.

A good example of how these approaches are put into practice is the Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building of 17 June 2013,[7] which gave a start to cooperation between relevant Russian and US agencies. The heads of state also agreed to establish a bilateral working group on threats to ICT and their use in the context of international security to hold regular consultations on issues of mutual interest and concern.

Eight years later, in June 2021, a similar process was launched by Russian and US leaders at a summit in Geneva. A regular dialogue at the top government level involving information security experts helped to enhance cooperation between the parties in combating the criminal use of ICT.

Thus, the development of bilateral interaction on a pragmatic basis has already become a trend in this area.

Multilateralism as a Sign of a Common Approach and the Willingness to Act Together

Above the bilateral foundation lies the next level of the IIS system – the level of multilateral cooperation that brings together a number of countries sharing common approaches to addressing threats in the information sphere.

An example of such interaction is the Shanghai Cooperation Organisation, which has laid both political and legal foundations for cooperation in ensuring IIS.

The first step was the Statement of the Heads of the Shanghai Cooperation Organisation Member States on International Information Security dated June 15, 2006,[8] in which the leaders expressed their concern about the emerging real danger of the use of ICT for purposes that can seriously harm the security of individuals, society and the state in violation of the fundamental principles of equality and mutual respect, non-interference in the internal affairs of sovereign states, peaceful settlement of conflicts, non-use of force, and respect for human rights. Attention was also drawn to the fact that threats to use ICT for criminal, terrorist and politico-military purposes incompatible with ensuring international security can be realized both in the civil and military spheres, causing grave political and socio-economic consequences in individual countries and regions – and the world as a whole – and destabilizing the social life of states. In this regard, the heads of the SCO member states agreed to take coordinated and complementary measures to adequately respond to today's challenges and threats to information security.

The key point was the decision to create a core group of experts to develop an action plan to ensure IIS and identify possible ways and means of solving current prob-

[7] Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building of June 17, 2013. URL: http://www.kremlin.ru/supplement/1479. (In Russian).

[8] Statement of the Heads of the Shanghai Cooperation Organisation Member States on International Information Security dated June 15, 2006. URL: http://www.infoshos.ru/ru/?id=94. (In Russian).

lems in this area within the SCO. Since 2006, this expert group has been actively involved in the creation of a political and legal framework for cooperation between the Organization's member states on a multilateral basis. Three years of work by the expert team produced a draft intergovernmental cooperation agreement that was signed in Yekaterinburg on June 16, 2009.

The Agreement between the governments of the SCO member states on cooperation in the field of IIS was the world's first multilateral agreement in this area.[9] The signing of this agreement confirmed the possibility of reaching cooperation agreements between countries with significant differences in their national legislations and the respective terminology. These differences, however, were not an obstacle to signing the document, because the approaches to ensuring national information security and the creation of the IIS system were based on the common principles shared by all signatory countries.

What distinguishes cooperation in the SCO is its concrete and hands-on approach. The countries aim to identify, coordinate and implement joint measures to ensure IIS, create a system of monitoring and joint response to emerging threats, ensure information security of critical facilities, and counter the threats of using ICT for terrorist activities and information crime. The agreement provides for the exchange of experience, training of specialists, working meetings, conferences, seminars and forums involving authorized representatives and experts in the field of information security.

One of the main areas of cooperation aimed at harmonizing the parties' approaches to the unification of the relevant national legislations is the exchange of information on legislative regulation. Cooperation on legal issues involves improving the international legal framework and implementing practical mechanisms of cooperation in ensuring IIS. In this regard, a specific task is to work out joint measures to develop international law on limiting the spread and use of information weapons threatening defence capabilities and national and public security. Promoting the secure and stable functioning and internationalized management of the global internet is also of great importance.

For more than 12 years, efforts in this area have been coordinated by the core group of experts of the Shanghai Cooperation Organisation member states. Its work has resulted in concerted action by the SCO's members in various international arenas, most notably the United Nations, as evidenced by Resolution A/RES/73/27 "Developments in the Field of Information and Telecommunications in the Context of International Security" adopted on December 5, 2018 at the 73rd session of the UN General Assembly.[10] This document outlines a set of international rules, norms, and principles

[9] Agreement between the governments of the Shanghai Cooperation Organization member states on cooperation in the field of International Information Security. URL: https://base.garant.ru/2571379/. (In Russian).

[10] Resolution A/RES/73/27 "Developments in the Field of Information and Telecommunications in the Context of International Security." Adopted by the UN General Assembly on December 5, 2018. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement.

of responsible state behaviour that was previously enshrined in the 2013[11] and 2015[12] reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

These rules, norms and principles are based not only on the results of studies by the relevant groups of the UN governmental experts, but also on the Rules of Conduct in the Field of International Information Security, which the SCO member states introduced as official documents at the 66th (A/66/359)[13] and 69th (A/69/723)[14] sessions of the UN General Assembly on September 12, 2011 and January 9, 2015, respectively.

Both of these reports rightly stressed the input of the SCO. In 2013, the Group noted document A/66/359, circulated by the UN Secretary General at the request of the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan, containing a Rules of Conduct in the Field of International Information Security, with Kazakhstan and Kyrgyzstan subsequently joining as sponsors.[15] In 2015, the Group took the Rules of Conduct in the Field of International Information Security proposed by China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan under advisement.[16]

The common approaches of the SCO countries to ensuring IIS and their readiness to consolidate efforts against threats in the information sphere were once again confirmed in the statement of the Council of Heads of State of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security dated November 10, 2020.[17] The document clearly outlines the commitment of the SCO's member states to improve mechanisms and measures aimed at preventing inter-state conflicts and overcoming the lack of trust between nations that may stem from the unlawful use of ICT.

The key message of the leaders' statement was an appeal to the international community for close cooperation, including in the prevention of conflicts arising from the use of ICT, ensuring their use in the interests of social and economic development and

[11] 2013 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement.

[12] 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.

[13] Rules of Conduct in the Field of International Information Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement.

[14] Rules of Conduct in the Field of International Information Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement.

[15] 2013 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement.

[16] 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.

[17] Statement of the Council of Heads of State of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security dated November 10, 2020. URL: http://ru.china-embassy.org/rus/zgxw/t1831178.htm (In Russian).

the wellbeing of peoples. The main goal is to build a common future in the information space based on international cooperation in the field of information security by stepping up efforts at the national, bilateral and multilateral levels.

The political will of the heads of the SCO member states to create a legal framework for the IIS system can be seen in the focus on the development of rules, norms and principles of responsible state behaviour in the information space, the elaboration of universal legally binding instruments under the aegis of the UN, the improvement of internet governance, ensuring equal rights of states, and strengthening the role of the International Telecommunication Union in this context.

The agreements reached within the SCO have helped to establish effective cooperation in the field of information security, making it possible to significantly reduce the number of computer attacks on the critical information infrastructure of the member states and to enhance their national security in the information sphere.

Cooperation among the BRICS member states is developing in a multilateral format. A Working group of experts on security in the use of ICTs has been set up to coordinate countries' efforts in this area and promote cooperation within BRICS, including by considering relevant initiatives and implementing the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs.

With regard to establishing an IIS system, the XII BRICS Summit Moscow Declaration dated November 17, 2020 emphasizes the leading role of the United Nations in promoting a dialogue to achieve a common understanding of ICT security and use, as well as the development under the auspices of the Organization of universally recognized norms, rules and principles of responsible state behaviour in the field of ICT.[18]

The determination of the leaders of Brazil, Russia, India, China and South Africa to cooperate multilaterally is reflected in their consideration and preparation of proposals for a BRICS intergovernmental agreement on security cooperation in the use of ICT, as well as bilateral agreements between the BRICS nations.

Multilateral cooperation thus helps to harmonize the national approaches of cooperating states and strengthen the IIS system.

Regional Cooperation to Achieve Common IIS Goals

The third level of the IIS system is represented by regional organizations such as the Collective Security Treaty Organization (CSTO) and the Commonwealth of Independent States (CIS), both of which operate in the post-Soviet space.

The legal basis for interaction at this level is provided by the relevant cooperation agreements. Such cooperation, as a rule, is very practical and covers a whole range of areas that require active interaction between the parties.

[18] XII BRICS Summit Moscow Declaration dated November 17, 2020. URL: https://eng.brics-russia2020.ru/images/114/81/1148126.pdf.

For example, the Agreement on Cooperation of the Member States of the Collective Security Treaty Organization in the Field of Information Security, dated 30 November 2017,[19] provides for the development of a regional information security system based on interstate cooperation and stronger interagency cooperation. The focus is on improving mechanisms for countering threats in the information sphere, taking joint action to enhance information security and combat illicit activities in the information space of member states, and providing mutual assistance in developing the technological basis to ensure the Organization's information security, while also identifying, preventing and neutralizing threats to information security. The priority tasks include planning and carrying out coordinated steps to ensure information security and cooperation in protecting critical facilities, as well as combating destructive information influence, illegal activities in the information space and the creation and distribution of malicious software, and developing criteria for identifying, detecting and blocking information resources used for illegal purposes.

Priority is given to preventing third parties from using the territory and/or information infrastructure under the jurisdiction of a CSTO member state to exert destructive information influence, including computer attacks, on another CSTO state. This brings to the fore the identification of the source of computer attacks conducted from their territory, countering these attacks and eliminating their consequences.

A prerequisite for coordinated action by the parties was training in the field of information security, which was identified as a separate area of cooperation within the association.

Since CSTO members are aware of the need to integrate the regional component into the emerging global system, the countries aim to develop a coordinated position on ensuring IIS and promote this position on the international arena.

This list of action-oriented areas of cooperation suggests that the regional component of the multilevel IIS system plays an important role in ensuring its stable and sustainable functioning. At the same time, in order to further develop the global IIS system, it is necessary to ensure both the sustainable functioning of the levels of interaction noted above and the development of integration processes that help unite the efforts of various regional associations or establish their cooperation with individual leading states (groups of states) that are champions in the field of information security

Such interaction is generally based on political statements at the highest level, as well as other formats for expressing the will of stakeholders. For example, on November 14, 2018, Russia and the Association of Southeast Asian Nations (ASEAN) issued the Statement on Cooperation in the Field of Security of and in the Use of Information

[19] Agreement on Cooperation of the Member States of the Collective Security Treaty Organization in the Field of Information Security, dated November 30, 2017. URL: http://docs.cntd.ru/document/542645728. (In Russian).

and Communication Technologies, which serves as a catalyst for the consolidation of stakeholder efforts.[20]

The statement confirmed the proximity of the approaches adopted by Russia and the ASEAN countries in shaping the IIS system, noting that the cooperation and coordination of efforts of states at the bilateral, regional and international levels are essential for responding to threats and challenges posed by the use of ICT in a timely and effective manner, with due account of their cross-border nature. The document emphasizes the practical aspect of cooperation between Russia and the ASEAN member states, the importance of stepping up efforts to bridge the digital divide, and the need for measures to build national capacities and launch educational and training programmes on ICT security and the use of ICT. Particular attention is paid to strengthening practical cooperation in such areas as combating the use of ICT for terrorist purposes and other criminal activities.

The commitment of the parties to the Statement to strengthen and optimize existing regional security mechanisms in the use of ICT, as well as the support of the Russian initiative to establish a Russia–ASEAN dialogue on security issues, demonstrate the resolve of the ASEAN nations to create, in cooperation with Russia, a qualitatively new regional level of the IIS system.

An important element of this interaction is the development of bilateral relations between Russia and the ASEAN countries and the creation of an essential legal framework for cooperation in ensuring security in the use of ICT. Russia signed an intergovernmental cooperation agreement with Vietnam in this area in 2018,[21] and a similar agreement with Indonesia in 2021.[22] The dialogue with Singapore and Malaysia in this field is developing constructively and rapidly. Thailand and Cambodia have also confirmed their commitment to bilateral cooperation with Russia.

Such regional cooperation, as well as intra- and inter-regional agreements, including bilateral accords, help strengthen the regional level of the IIS system – the guarantor of stability and security in the information sphere for all stakeholders.

The development of normative legal and political frameworks for cooperation at the above levels cannot fully prevent threats in the information sphere. However, such

[20] Statement of ASEAN and the Russian Federation on Cooperation in the Field of Security of and in the Use of Information and communications technologies dated November 14, 2018. URL: https://asean.org/statement-of-asean-and-the-russian-federation-on-cooperation-in-the-field-of-security-of-and-in-the-use-of-information-and-communication-technologies/.

[21] Agreement between the Government of the Russian Federation and the Government of the Socialist Republic of Vietnam on Cooperation in the Field of International Information Security dated September 6, 2018. URL: http://docs.cntd.ru/document/554398783. (In Russian).

[22] Decree No. 2984-r of the Government of the Russian Federation "On the Signing the Agreement between the Government of the Russian Federation and the Government of the Republic of Indonesia on Cooperation in the Field of International Information Security dated December 28, 2018. URL: http:/docs.cntd.ru/document/552051443. (In Russian); Russia and Indonesia Sign an Intergovernmental Agreement on Cooperation in International Information Security. *Security Council of the Russian Federation*. December 14, 2021. URL: http://www.scrf.gov.ru/news/allnews/3151/. (In Russian).

cooperation and political will greatly reduce the number of new challenges and threats and, most importantly, the scale of their consequences.

Global level of the system to ensure IIS

The apex of the IIS system pyramid is the global level – the interaction of states on the basis of international legal instruments adopted under the auspices of the United Nations that regulate activities in the information space.

The first step towards creating a political and legal framework at this level was the adoption of Resolution A/RES/73/27 "Developments in the Field of Information and Telecommunications in the Context of International Security." The Russia-sponsored document was adopted by the 73rd session of the UN General Assembly on December 5, 2018, for the first time establishing a set of 13 international rules, norms and principles of responsible state behaviour.[23]

In conjunction with this resolution, an open-ended working group was set up in 2019 to ensure a more democratic, inclusive, and transparent negotiation process on security in the use of ICTs, with a priority to further develop these norms, rules, and principles of responsible behaviour by states.

The resolution, supported by a majority of UN member states, launched a regular institutional dialogue with a wide range of participants under the auspices of the organization, providing a new format of expert discussion of key IIS issues by all stakeholders, including business, non-governmental organizations and academia.

At Russia's initiative, Resolution A/RES/75/240 "Developments in the Field of Information and Telecommunications in the Context of International Security" was adopted onDecember 31, 2020 by majority vote at the 75th session of the UN General Assembly.[24] Among other things, it set up a new Open-Ended Working Group for 2021–2025 on security in the use of ICT. Thus, the United Nations has maintained the continuity of a democratic, inclusive, and transparent security negotiation process.

The new Open-Ended Working Group launched in June 2021 will continue to develop the norms, rules and principles of responsible state behaviour and ways to implement them and modify or formulate additional rules to them, if necessary.

For the first time, the platform will be used to review initiatives designed to ensure security in the use of ICT, providing an opportunity to discuss problems in this area comprehensively and look for ways to solve them, including through possible joint measures to prevent and counter existing and potential threats in the sphere of information security.

[23] Resolution A/RES/73/27 "Developments in the Field of Information and Telecommunications in the Context of International Security". URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement.

[24] Resolution A/RES/73/27 "Developments in the Field of Information and Telecommunications in the Context of International Security. Adopted by the UN General Assembly on December 31, 2020. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement.

Despite the fact that the reports of the Open-Ended Working Group and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2010, 2013, 2015) are advisory in nature, the provisions set out in them may ultimately become the basis for the preparation, under the auspices of the United Nations, of the relevant legal instruments governing relations in the IIS sphere.

Potential major regulatory acts include the UN Convention on Ensuring International Information Security, the concept of which was introduced by Russia in September 2011 at an international meeting of high representatives in charge of security issues.[25] This document, as conceived by its drafters, could form the basis of a fundamental multilateral treaty involving all UN member states, open to wider international participation and aimed at addressing the need, proclaimed in the UN Millennium Declaration of September 8, 2000, to strengthen the international rule of law, including in the information sphere.[26]

In 2011, the purpose of this convention was set out – to counter the use of ICTs to disrupt international peace and security, and to establish measures to ensure that the activities of states in the information space: (1) contribute to overall social and economic development; (2) are conducted in a manner that is compatible with the objectives of maintaining international peace and security; (3) comply with the generally recognized principles and norms of international law, including the principles of the peaceful settlement of disputes and conflicts, the non-use of force, non-interference in internal affairs, and respect for human rights and fundamental freedoms; (4) are compatible with the right of everyone to seek, receive and impart information and ideas as set forth in UN documents, bearing in mind that this right may be limited by law to protect national and public security interests of each state, and to prevent misuse of information resources; and (5) guarantee the freedom of technological exchange and the free exchange of information, taking respect for the sovereignty of states and their political, historical and cultural specificities into account.[27]

Over the decade since the concept was first introduced, certain changes have taken place that have prompted a review of the current state of the information space, existing and potential threats to IIS, and possible measures to counter them. These changes are reflected in the updated version of the above-mentioned concept of the UN Convention, which was presented in July 2021.[28]

[25] Concept of the UN Convention on International Information Security (2021). *Security Council of the Russian Federation*. URL: http://www.scrf.gov.ru/security/information/Concept_en/.

[26] United Nations Millennium Declaration. Adopted by United Nations General Assembly resolution 55/2 of September 8, 2000. URL: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_55_2.pdf.

[27] Concept of the UN Convention on International Information Security (2021). *Security Council of the Russian Federation*. URL: http://www.scrf.gov.ru/security/information/Concept_en/.

[28] Ibid.

The main goal of the document is defined as the promotion of an IIS system able to counter threats to international peace, security and stability in the information sphere. This system must facilitate: (a) equitable strategic partnership in global information space on the basis of sovereign equality of States; (b) overall social and economic development on the basis of equal and secure access of all States to modern ICT developments; (c) implementation of universally recognized principles and norms of international law, including principles of peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs, and respect for human rights and fundamental freedoms; (d) Exercise of everyone's right to seek, receive and impart information and ideas of all kinds, taking into account that this right may be subject to certain restrictions established by law and necessary for respect of the rights or reputations of others, as well as for the protection of national security, public order, public health or morals; (e) free exchange of technology and information with respect for the sovereignty of States and their existing political, legal, historical and cultural specificities.[29]

Despite the update, the basic approaches to the creation of the IIS system, which were established in 2011, remained unchanged.

However, the Russian initiative to develop this Convention was not supported by Western countries, which prefer non-binding rules and norms of responsible state behaviour. A similar position can also be found in the works of some foreign scholars. In particular, Joseph S. Nye notes that "a binding international legal treaty would be premature as the next step. Norms of expected behaviour can provide a flexible middle ground between rigid treaties and taking no action at all"[30].

And there are also other scholars who, on the one hand, confirm the difficulties currently facing Russia in advancing its initiative and, on the other hand, assess the need for comprehensive arrangements.

According to Nicholas Tsagourias, cyberspace is a domain that offers possibilities but also contains risks and dangers, a regulatory system based on common values, principles and rules of conduct is needed to foster cooperation and good citizenship in cyberspace. This may require a comprehensive and globally negotiated treaty to establish rules of behaviour and jurisdiction. Yet agreement on a comprehensive legal framework for cyberspace faces huge challenges. Tsagourias believes that the prospects for such an all-encompassing regime are rather bleak. However, he concludes that international law defines the behaviour and interests of states in cyberspace and perhaps rationalizes them (Tsagourias 2016).

The Russian initiative to get the Convention on International Information Security adopted by the United Nations is not the only one at the global level. The explosive

[29] Ibid.

[30] Nye J. 2019. Eight Norms for Stability in Cyberspace. *Project Syndicate.* URL: https://www.project-syndicate.org/commentary/eight-norms-for-stable-cyberspace-by-joseph-s-nye-2019-12?barrier=accesspaylog (accessed: 01.01.2022).

growth of the unlawful use of ICT has heightened the need to address this problem. Russia believes that a comprehensive international convention on combating the use of information and communications technologies for criminal purposes could serve as a legal basis for consolidating the efforts of the global community under the aegis of the UN.

UN General Assembly Resolution A/RES/74/247 "Countering the use of Information and Communications Technologies for Criminal Purposes" dated December 27, 2019, established an ad hoc open-ended intergovernmental committee of experts representing all regions of the world to develop this convention.[31]

Existing international legal instruments and efforts at the national, regional and international levels to combat the use of ICT for criminal purposes will be taken into account when preparing the convention, as will the work of the Open-Ended Intergovernmental Expert Group to conduct a comprehensive study on cybercrime.[32]

A key document in this regard could be the draft UN Convention on Cooperation in Combating Information Crime introduced at Russia's initiative and circulated at the United Nations in October 2017 as a document of the 72nd session of the General Assembly (under agenda item 107 "Crime Prevention and Criminal Justice").[33]

This draft, which takes into account current realities and is based on the principles of sovereign equality of parties and non-interference in the internal affairs of other states, is the result of the years-long efforts by experts to create a universal, comprehensive document aimed at countering crimes in the use of ICT.

A clear advantage of the document is that its developers drew on the experience of similar international legal instruments. These include the UN Convention against Corruption of October 31,2003,[34] the UN Convention against Transnational Organized Crime of 15 November 2000,[35] the Council of Europe Convention on Cybercrime (ETS No. 185) of November 23, 2001 (the so-called Budapest Convention on Cybercrime),[36] and universal anti-terrorist conventions of the United Nations.

An updated draft of the UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes[37] was submitted by Russia

[31] Resolution A/RES/74/247 "Countering the Use of Information and Communications Technologies for Criminal Purposes" dated December 27, 2019. URL: https://undocs.org/ru/A/RES/74/247.

[32] Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector (draft, February 2013). URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf.

[33] Draft United Nations Convention on Cooperation in Combating Information Crime. Letter dated October 11, 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. A/C.3/72/12 of October 16, 2017. URL: http://www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступности+с+правками+секр+ООН.pdf/c93e68c9-9994-4769-951d-057c4881b8fd. (In Russian).

[34] United Nations Convention against Corruption. Adopted by UN General Assembly resolution 58/4 of October 31, 2003. URL: https://www.unodc.org/unodc/en/treaties/CAC/.

[35] United Nations Convention against Transnational Organized Crime. Adopted by UN General Assembly Resolution 55/25 of November 15, 2000. URL: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

[36] Convention on Cybercrime (ETS No. 185) (Budapest, November 23, 2001). URL: https://rm.coe.int/1680081561.

[37] United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (draft). URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf.

to an intergovernmental ad hoc committee in July 2021. The final draft is scheduled to be completed in 2023–2024 during the 78th session of the UN General Assembly.

Another important step in creating a global IIS system could be the adoption by the United Nations of a convention document in the field of internet security. The Russian concept of the convention (the concept of the safe operation and development of the internet) presented in April 2017 could serve as the basis for such a document.[38]

The concept's key ideas are to promote the further development of the internet, improve its security and guarantee the rights and freedoms of users, while also establishing a regime of equal international cooperation in managing the network, increasing its efficiency and effectiveness.

The implementation of Russia's initiative will enable each state to protect its national segment of the global network, including critical information infrastructure, and also guarantee the rights and freedoms of users and the protection of citizens on the internet. It also eliminates the possibility of interfering with the internet and manipulating network access to influence other sovereign states.

The concept is based on the Tunis Agenda for the Information Society of December 15, 2005,[39] and the 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 of December 16, 2015.[40] The Russian concept reflects the key message of these basic instruments: each state has the sovereign right to independently decide the issues of public policy on the internet.

This approach has both supporters and opponents, who see Russia's initiative as an attempt to take control of the global information network and infringe on the rights of its users. In this context, it seems appropriate to recall the provisions of Article 19 of the 1966 International Covenant on Civil and Political Rights: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers […] The exercise of the rights […] carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (ordre public), or of public health or morals.[41]

[38] Ministry of Communications Presents draft New UN Convention Concept. *Ministry of Digital Development, Communications and Mass Media of the Russian Federation*. April 14, 2017. URL: https://digital.gov.ru/ru/events/36739/. (In Russian).

[39] Tunis Agenda for the Information Society. Document WSIS-05/TUNIS/DOC/6(Rev.1)-R dated November 15, 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[40] 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. Adopted by UN General Assembly Resolution A/70/125 of December 16, 2015. URL: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96090.pdf.

[41] International Covenant on Civil and Political Rights. Adopted by UN General Assembly Resolution 2200 A (XXI) of December 16, 1966, https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf.

* * *

The creation of the IIS system at all the levels discussed above is a complex and multifaceted process that must involve states, non-state actors, the scientific and expert community, business, and ordinary citizens. However, responsibility for information security and protection from new challenges and threats rests with the states themselves. The future of the world community, socio-political stability and the wellbeing of the population depend on their activity in this area.

Understanding the complexity of these processes and the scale of the possible consequences of destructive activities in the information space has predetermined the content of Russia's approaches and initiatives aimed at promoting the formation of the IIS system at all levels, from bilateral to global.

The above list of Russia's initiatives to build the IIS system is not exhaustive and is not sufficient to meet this global challenge. This process will involve overcoming many differences, converging approaches to key issues, building mutual understanding and trust in this area, collaborating at various levels and in various formats to ensure IIS, and, lastly, reaching cooperative agreements to consolidate the efforts of the global community to counter the rapidly growing challenges and threats in the information sphere.

In the context of the search for strategic solutions to these problems, the Russian approaches and initiatives discussed in this article can guide the creation of the necessary political and legal framework for the creation of an IIS system – a guarantee of stability and equitable strategic partnership in the global information space.

About the Author:

Sergey M. Boyko – Head of the Department for Security Issues in the Information Sphere, Office of the Security Council of the Russian Federation. Moscow, 103132, Russia. E-mail: boiko_sm@gov.ru.

Conflict of interests:
The author declares the absence of any conflict of interests.

References:

Ambos K. 2015. International Criminal Responsibility in Cyberspace. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace.* St. Louis: Edward Elgar. P. 152-181.

Antonopoulos C. 2015. State Responsibility in Cyberspace. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace.* St. Louis: Edward Elgar. P. 130-151.

Batueva E.V. 2014. *Amerikanskaya kontseptsiya ugroz informatsionnoj bezopasnosti i ee mezhdunarodno- politicheskaya sostavlyayushchaya. Dissertatsiya na soiskanie uchenoj stepeni kandidata politicheskikh nauk* [American Concept of Threats to Information Security and Its International Political Dimension. PhD in Political Science Thesis]. Moscow. 207 p. (In Russian).

Buchan R. 2018. Cyber Espionage and International Law. Oxford. 248 p.

Henderson C. 2015. The United Nations and the Regulation of Cybersecurity. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace.* St. Louis: Edward Elgar. P. 582-614.

Jensen E.T., Watts S. 2017. A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? *Texas Law Review.* Vol. 19, p. 1555-1577.

Jian H., Bapna S. 2013. The Economic Impact of Cyber Terrorism. *The Journal of Strategic Information Systems.* Vol. 22. No. 2. P. 175-186.

Kapustin A.Y. 2015. Ugrozy mezhdunarodnoj informatsionnoj bezopasnosti: formirovanie kontseptual'nykh podkhodov [Threats to International Information Security: Formation of Conceptual Approaches]. *Zhurnal rossiiskogo prava.* No. 8. P. 89-100. (In Russian).

Kapustin A.Y. 2017. K voprosu o mezhdunarodno-pravovoj kontseptsii ugroz mezhdunarodnoj informatsionnoj bezopasnosti [With Regard to the International Legal Concept of Threats to International Information Security]. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya.* No. 6. P. 44-51. (In Russian).

Kastner P., Megret F. 2015. International legal dimensions of cybercrime. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace.* St. Louis: Edward Elgar. P. 253-270.

Kazarin O.V., Skiba V.Y., Sharyapov R.A. 2016. Novye raznovidnosti ugroz mezhdunarodnoj informatsionnoj bezopasnosti [New Kinds of Threats to International Information Security]. *Istoriya i arkhivy.* No. 1. P. 54-72. (In Russian).

Kerschischnig G. 2012. *Cyberthreats and International Law.* 344 p.

Krasikov D.V. 2018. Mezhdunarodno-pravovaya otvetstvennost' gosudarstv v kiberprostranstve [International Legal Responsibility of States in Cyberspace]. In: Alferova E.V., Lovtsov D.A. (eds). *Gosudarstvo i parvo v novoj informatsionnoj real'nosti: Sbornik nauchnykh trudov.* Moscow: INION. P. 235-247. (In Russian).

Krasikov D.V. 2018. Territorial'nyi suverenitet i delimitatsiya yurisdiktsij v kiberprostranstve [Territorial Sovereignty and Delimitation of Jurisdictions in Cyberspace]. In: Alferova E.V., Lovtsov D.A. (eds). *Gosudarstvo i parvo v novoj informatsionnoj real'nosti: Sbornik nauchnykh trudov.* Moscow: INION. P. 99-111. (In Russian).

Krutskikh A.V. 2007. K politiko-pravovym osnovaniyam global'noj informatsionnoj bezopasnosti [Towards the Political and Legal Foundations of Global Information Security]. *Mezhdunarodnye protsessy.* 5(1): 28-37. (In Russian).

Krutskikh A.V. (ed.) 2021a. *Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika: V trekh tomakh. Tom 1* [International Information Security: Theory and Practice: In three volumes. Volume 1]. 2nd ed. Moscow: Aspekt Press. 384 p. (In Russian).

Krutskikh A.V. (ed.) 2021b. *Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika: V trekh tomakh. Tom 2: Sbornik dokumentov* [International Information Security: Theory and Practice: In three volumes. Volume 2: Collection of documents]. Moscow: Aspekt Press. 784 p. (In Russian).

Krutskikh A.V., Biryukov A.V. 2017. Novaya geopolitika mezhdunarodnykh nauchno-tekhnologicheskikh otnoshenij [New Geopolitics of International Scientific and Technological Relations]. *Mezhdunarodnye protsessy.* 15(2): 6-26. (In Russian).

Lewis J.A., Stewart B. 2013. The Economic Impact of Cybercrime and Cyber Espionage. Report, *Center for Strategic and International Studies.* URL: https://apo.org.au/node/35084 (accessed: 01.01.2022).

Saul B., Heath K. 2014. *Cyber Terrorism.* Sydney Law School Legal Studies Research Paper. No. 14/11. URL: https://ssrn.com/abstract=2387206 (accessed: 01.01.2022).

Sebekin S.A. 2020. Budushchee mezhdunarodnoj sistemy informatsionnoj bezopasnosti v usloviyakh krizisa arkhitektury strategicheskoj stabil'nosti [The Future of International Information Security System in Crisis of Strategic Stability Architecture]. *Russian International Affairs Council.* URL: https://russiancouncil.ru/analytics- and-comments/columns/cybercolumn/budushchee-mezhdunarodnoy-sistemy-informatsionnoy- bezopasnosti-v-usloviyakh-krizisa-arkhitektury-str/ (accessed: 01.01.2022). (In Russian).

Smirnov A.I., Strel'tsov A.A. 2017. Rossijsko-amerikanskoe sotrudnichestvo v oblasti mezhdunarodnoj informatsionnoj bezopasnosti: predlozheniya po prioritetnym napravleniyam [Russian-American Cooperation in the Field of International Information Security: Proposals in Priority Areas]. *Mezhdunarodnaya zhizn'.* No. 11. P. 72—81. (In Russian).

Tsagourias N. 2016. The legal status of cyberspace. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace.* St. Louis: Edward Elgar Publ. P. 13—29.

Vasenin V.A. 2004. Informatsionnaya bezopasnost' i komp'yuternyj terrorizm [Information Security and Computer Terrorism]. In: Sherstyuk V.P. (ed.) *Nauchnye imetodologicheskieproblemyinformatsionnoj bezopasnosti.* Moscow: MTsNMO. P. 67—83. (In Russian).

Weimann G. 2015. *Terrorism in Cyberspace: The next Generation*. New York. 344 p.

Zinovieva E.S. 2021. *Mezhdunarodnaya informatsionnaya bezopasnost': problemy dvustoronnego i mnogostoronnego sotrudnichestva* [International Information Security: Issues of Bilateral and Multilateral Cooperation]. Moscow: MGIMO University. 250 p. (In Russian).

Zinovieva E.S. 2019. *Mezhdunarodnoe sotrudnichestvo po obespecheniyu informatsionnoj bezopasnosti: sub"ekty i tendentsii evolyutsii. Dissertatsiya na soiskanie uchenoj stepeni doktora politicheskikh nauk.* [International Cooperation in the Field of Information Security: Actors and Trends of Evolution. Doctor of Political Science Thesis]. Moscow. 362 p. (In Russian).