Expert report

UN Security Council

«Threats to Peace and Security Posed by Information and Communication Technologies»

PRCIMUN-2022

Precaspian International Model United Nations

МОДЕЛЬ ООН

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

АБСОЛЮТНАЯ ГАРАНТИЯ УСПЕХА

1932

1. KEY POINTS

The exchange of information and the possibility of its dissemination can be considered as the basis for the existence and functioning of any type of society.

Several turning points associated with the emergence of new forms of an information exchange, known as ‘information revolutions’, can be marked out throughout the historical development of society. The first such revolution happened due to the invention of writing and alphabet, which made it possible to record information and store knowledge of the surrounding world and events. The second information revolution is related to the emergence and development of printing, which greatly facilitated the process of recording the knowledge, and increased the speed of information dissemination. The third information revolution, far greater and more rapid in its scope and consequences, was triggered by technological changes – the discovery of electricity and subsequent invention of telegraphy, telephone, radio and television, which significantly increased the speed of information dissemination and made information available for a wide range of users. At the current stage of development, society is experiencing the fourth information revolution, unparalleled in its nature and scope[1]. Since the middle of the 21st century, the international community has entered a new phase of development – the post-industrial, or information society. Computing machines, first computers and subsequent creation of the Internet as the most important achievement of the technological revolution have been introduced since 1960s. All of this has led to the transition to the new type of a society – an information society, the core element of which is an almost unlimited access to information and knowledge, its dissemination and use as a base resource. The global technological infrastructure of the Internet determines a cross-border nature of its functioning and use, which transcends time, space and political boundaries.

To date, it can be said that the massive spread of the ICT in the world, in combination with the transnational communication network of Internet, has created the conditions for the establishment of a Global Information Society (GIS). At the same time, the process of GIS emergence and the development of a legal framework of its functioning and structure took a certain amount of time and evolved in several stages. The first significant milestone was the ITU Plenipotentiary Conference, where the idea of a World Summit on Information Society under the aegis of the International Telecommunication Union was put forward and supported. Then G8 adopted the Okinawa Charter on Global Information Society[2]. This document proposed a number of important ideas, formulated complementary political, economic and social goals and identified specific work areas, including economic and structural reforms, sustainable macroeconomic management, development of international networks and human resources, active use of

[1] Rassolov I.M. Law and cybernetic space. Monograph. - 2nd ed. - M: Moscow Bureau for Human Rights, 2016, pp. 7-10

[2] Okinawa Charter on Global Information Society, July 21 , 2000 http://www.kremlin.ru/supplement/3170

ICT in the public sector. The Plenipotentiary Conference of ITU adopted the Marrakesh Agreements in 2002[3], which established the principles of building a global information society – ensuring the right to information and knowledge, promoting universal access to them, strengthening the international cooperation and enhancing the security of information and communication networks. The World Summit on the Information Society (WSIS) was held in two steps – in Geneva (2003) and Tunis (2005)[4]. This meeting was the first international platform where the discussion of the issues related to global informatization was raised to the highest political level and took place on such a broad geopolitical scope in dialogue with the representatives of businesses and civil society. The summit brought together more than 11,000 participants from 176 countries, including the representatives of international organizations. At the meeting, information security was in the focus of international concern. The issues of trust and security in the use of information and telecommunication technologies were among the main issues discussed at the World Summit. The point was made that the full benefits of information and telecommunication technologies could be taken only if technologies and networks are reliable, secure and are not used in purposes that are incompatible with the objectives of ensuring international stability and security. The World Summit participants expressed their concern that information and telecommunication technologies could have a negative impact on the security of states and recognized the need to prevent the use of information technologies for criminal and terrorist purposes. Participants identified the reviewing of existing and potential threats for the security of information and communication networks as one of the measures that could be proposed to address international security issues. The most important outcome of the first round was the adoption of two documents subsequently endorsed by the UN General Assembly – Declaration of Principles on the Information Society[5] and Plan of Actions of the World Summit on the Information Society[6].

The Tunis Commitment on the Information Society and Tunis Agenda for the Information Society were adopted at the second stage[7]. The papers outlined a common understanding of the fact that the use of ICT should come with the respect for the universally recognized human rights, and should not undermine the freedom of access to information; activities, aimed at the bridging of digital gaps, become particularly important, thus enabling the developing countries to assert their right to access the modern ICT.

Regional conferences were organized with WSIS activities, with a number of declarations on the information society being

[3] The Ministry of Communication of the Russian Federation, STATE TELECOMMUNICATION COMMISSION,
Decision No. 49 "On the outcomes of the ITU Plenipotentiary Conference (Marrakesh, 2002) and the work of the Russian Communications Administration on it" dated December 25, 2002 https://docs.cntd.ru/document/901858785

[4] **World Summit on the Information Society** https://www.un.org/ru/events/pastevents/wsis.shtml

[5] Document WSIS/GENEVA/DOC/4-R dated December 12, 2003 Original: English. Declaration of Principles on building the information society: a global challenge in the new millennium https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf

[6] Document WSIS/GENEVA/DOC/5-R dated December 12, 2003 Original: English. Plan of Action https://www.un.org/ru/events/pastevents/pdf/plan_wsis.pdf

[7] Document WSIS-05/TUNIS/DOC/6(Rev.1)-R dated November 15, 2005 Original: English. Chair of the Preparatory Committee for the Tunis phase TUNIS AGENDA FOR THE INFORMATION SOCIETY https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

adopted. Thus, one of the principles of the information society, enshrined in the **Bucharest Declaration** of the Pan-European Conference[8], was the principle of building trust and security in the use of information and telecommunication technologies. It implies the development of a global culture of cybersecurity which should be ensured through the adoption of preventive measures and supported by the whole society while preserving the freedom of communication. The states that participated in the Bucharest Conference came to an understanding of the fact that "information and telecommunication technologies can be used for purposes incompatible with the objectives of ensuring international stability and security, as well as have a negative impact on the integrity of infrastructure in individual states, breaching their security".

The Asian Conference was held in 2003 in Tokyo and resulted in the formulation of the **Tokyo Declaration**. The document, which was adopted by representatives of 47 countries, 22 international and 116 non-governmental organizations, as well as the officials of 54 private companies, highlighted "priority areas of action" in the field of information and telecommunication technologies. The security of information technologies and means is an important issue among these areas. Recognizing the principle of a just, equal and adequate access to information and telecommunication technologies for all countries, the parties consider it necessary to pay particular attention to the threat of a potential military use of ICT. The Member States also agreed on the need to strengthen regional and international cooperation for the purpose of enhancing the security of the information sector. It was the first time an opinion had been expressed that the effective provision of information security could be achieved not only technologically, but also institutionally, and that would require the efforts to ensure legal regulation of the issue and the development of respective national policies.

It means that in conditions of the global information revolution, information and communication technologies become not only a tool but also the most important element in constructing the global information society. At the same time, the first attempts to discuss and understand the role of ICT revealed potential challenges and dangers to information security of individual users, national public security, and ultimately, to international security. Global information revolution created a new field in which international law and order are being formed, which has led to changes in the structure of international security and creation of a separate **International Information Security (IIS)**. In this regard, the issue of development and improvement of an international legal framework in the field of information security and adoption of special laws and rules directly regulating ICT becomes especially relevant. Actions to form the basis of an international framework in the field of IIS are taken at various forums and in different formats of diplomatic activity, including bilateral, regional and universal international platforms.

2. UN ACTIONS IN THE CONTEXT OF INTERNARHIONAL INFORMATION SECURITY.

The UN platform will discuss the global issue of providing international

[8] Document WSIS/PC-2/DOC/5-R dated January 15, 2003 Original: English. Note by the WSIS Executive Secretariat REPORT OF THE WSIS PAN-EUROPEAN REGIONAL CONFERENCE (Bucharest, November 7-9, 2002) https://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-R.pdf

information security in various aspects, including the use of ICT in military field, possibilities of using ICT for criminal or terrorist purposes, importance of respecting human rights and freedoms in the field of using ICT, and issues of determining the status and management of the Internet space.

Since 1998, the long-term and extremely intense discussion of various aspects of IIS has been under way for 23 years at the UN General Assembly. The Russian Federation takes an active role in this process being the author of many initiatives and drafts of UN resolutions on the agenda entitled *Developments in the Field of Information and Telecommunications in the Context of International Security*.

In 1998, a special message on the international information security of the Russian foreign minister was sent to the UN Secretary-General. Particular emphasis there was placed on the need to prevent the emergence of a conceptually new informational area of confrontation and conceptually new military conflicts. The resolution entitled *Developments in the Field of Information and Telecommunications in the Context of International Security*, proposed by Russia during the 53rd session of the UN General Assembly and adopted as Resolution A/RES/53/70[9] on December 4, 1998, became a practical development of the Russian initiative. The resolution suggests that the UN member states keep discussing the issues of information security, determine specific threats, provide particular assessment of the threats, including the development of international principles of ensuring security of global information systems. The UN Secretary-General, who was assigned to report thereon at the next session of the UN General Assembly, must be informed by UN Member States about the results of their assessment [2]. The report was published on August 10, 1999 (A/54/213)[10] and included assessment from such countries as Australia, Belarus, Brunei, Cuba, Oman, Qatar, Russia, Saudi Arabia, the UK and the USA. The common point of these assessments was to recognize the existence of challenges for information security provision, but there were significant differences in prioritizing (of military, legal, humanitarian and other aspects) as well as in the methods of its consideration and solution.

The next Resolutions of the UN General Assembly 54/49[11], 55/28[12] largely confirmed the content of the Resolution 53/70, expanding it with important provisions admitting the possibility of a negative impact of ICT and the use of it against the security of Member States not only in civilian, but also in military sphere. This is how a triad of threats (using ICT for military, terrorism and criminal purposes)[13] was first outlined by the Russian Ministry of Foreign Affairs. The Resolution 54/49 confirms once again the need to develop international principles and rules in the sphere of ICT security and the fight against cybercrimes. The Resolution A/RES/55/28 states that the objective to limit the threats in

[9] Resolution A/RES/53/70 of the UN General Assembly dated December 4, 1998 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760..

[10] Developments in the Field of Information and Telecommunications in the Context of International Security: report by the Secretary-General A/54/213 | 1998-08-10 https://digitallibrary.un.org/record/286090?ln=ru

[11] Resolution A/RES/54/49 of the UN General Assembly dated December 1, 1999 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElemen

[12] Resolution A/RES/55/28 of the UN General Assembly dated December, 20 2000 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561..

[13]

the sphere of information security would be in the line with "examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems".

The resolution A/RES/56/19 dated November 29, 2001[14], enshrines a decision to establish a group of governmental experts (GGE) to work on a comprehensive study on the issue of international information security. The functions of this group include consideration of existing and potential threats in the field of information security and possible measures to limit the threats emerging in this field, as well as consideration of international concepts aimed at strengthening the security of global information and telecommunications systems. The start of UN GGE activities in 2004 opened a new phase of the long-term work of the UN by laying the first institutional unit which remained the main discussion platform on the issues of international information security over the course of several sessions. Six meetings of GGE were convened (GGE 1 in 2004, established under A/RES/56/19; GGE 2 in 2009, established under A/RES/60/45; GGE 3 in 2012, established under A/RES/65/41; GGE 4 in 2014, established under A/RES 68/243; GGE 5 in 2016, established under A/RES/70/237; GGE 6 in 2019, established under A/RES/73/266) up until 2021. The mandate of the group expanded and included such areas as the development of norms, rules and principles of responsible behavior of the states and actions to strengthen trust and develop capacity, as well as consideration of issues of using ICT in conflicts and the ways the countries apply the international law in their using of ICT. It is important to mention that only three GGEs formalized the results of their work in final reports (2010, 2013, 2015) which were agreed and approved by consensus. The work of other groups allowed to have a full exchange of views, best practices and documents on the issue of developments in the field of international information security but did not result in a consensus on a final report.

The Resolution A/RES/57/53[15] of the UN General Assembly on international information security advances the provisions of the previous resolutions and points to the inadmissibility of the use of information and telecommunication technologies to affect the infrastructure of countries or destabilize the situation in a particular region.

The Resolution A/RES/58/32[16] of the UN General Assembly dated December 8, 2003 expresses a concern about the possible use of ICT for the purposes that do not provide international stability and security and may have a critical influence on the countries' unity mechanism by breaching their security in civilian and military spheres.

The UN Resolution A/RES/66/24[17] should be mentioned among the resolutions under the title *Developments in the Field of Information and Telecommunications in the Context of International Security*. This resolution established norms, rules and

[14] Resolution A/RES/56/19 of the UN General Assembly dated November 29, 2001 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476..

[15] Resolution A/RES/57/53 of the UN General Assembly dated November 22, 2002 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/541..

[16] Resolution A/RES/58/32 of the UN General Assembly dated December, 8 2003 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485.pdf?OpenElement

[17] Resolution A/RES/66/24 of the UN General Assembly dated December 2, 2011 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/460/28/PDF/N1146028.pdf?OpenElement

principles of the countries' responsible behaviour in the field of IIS that have been elaborated by the Russian Federation in liaison with its partners from the Shanghai Cooperation Organization (SCO). The 73rd session of the UN General Assembly was a breakthrough, since two Russian draft resolutions were adopted there – A/RES/73/27[18] (it finally approved a set of 13 rules of the countries' behaviour in the field of international information security) and A/RES/73/187[19] (*Countering the Use of Information and Communications Technologies for Criminal Purposes*, which includes the previously presented Russian draft of the UN universal convention on cooperation in countering information crime). The Russian initiative to establish a new institutional mechanism in 2019 should be also mentioned. This initiative includes the development of an Open-ended Working Group which operates on the basis of consensus aimed to make the negotiations in this sphere more democratic, inclusive and transparent (A/RES/73/27). A fundamentally new provision here is that any UN member state can participate in the group's work, rather than a limited number of representatives from 15 to 25 members of the Group of Governmental Experts. The OEWG mandate is quite wide and includes the whole range of issues for discussion in the context of IIS, including further work on norms, rules and principles of the countries' responsible behavior, the issue of applicability of the international law to the use of ICT by states, trust-building measures and capacity-building in the field of ICT, assessment of current and potential threats, and organization of a regular institutional dialogue with a wide range of participants under the auspices of the United Nations. Russia's position, reflected in the Resolutions A/RES/74/29[20], A/RES/75/240[21] *Developments in the Field of Information and Telecommunications in the Context of International Security*, elaborates the OEWG idea in 2019 and the extension of its mandate for 2021-2025.

The U.S. initiatives in the field of IIS are reflected in the Resolutions A/RES/73/266[22], A/RES/74/28[23], A/RES/75/32[24] *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, mention the ongoing work of the GGE of the 6th convocation in 2019-2021 but do not introduce any provisions or additions to the Group's mandate and to the issue of IIS in general, leaving this to the UN General Assembly's consideration at subsequent sessions after

[18] Resolution A/RES/73/27 of the UN General Assembly dated December 5, 2018 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement

[19] Resolution A/RES/73/187 of the UN General Assembly dated December 17, 2018 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/56/PDF/N1845056.pdf?OpenElement

[20] Resolution A/RES/74/29 of the UN General Assembly dated December 12, 2019 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/10/PDF/N1941010.pdf?OpenElement

[21] Resolution A/RES/75/240 of the UN General Assembly dated December 31, 2020 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement

[22] Resolution A/RES/73/266 of the UN General Assembly dated December 22, 2018. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/04/PDF/N1846504.pdf?OpenElement

[23] Resolution A/RES/74/28 of the UN General Assembly dated December 12, 2019. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/03/PDF/N1941003.pdf?OpenElement

[24] Resolution A/RES/75/32 of the UN General Assembly dated December 7, 2020. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/354/02/PDF/N2035402.pdf?OpenElement

examining the results of the work of GGE and OEWG.

Analysis of the results of the work done in the field of ensuring IIS allows to talk of the development of international information law. Therefore, the current situation is marked by the appearance of a new measurement of the international security system.

Meanwhile, threats to international peace and security posed by ICT have not been put for discussion at the Security Council as a separate point of the agenda. The Security Council, being a universal platform for discussion of current threats to international peace and security, can put the military and political aspects of IIS for discussion. In the meantime, the military and political use of ICT is one of the most politicized issues, affecting the development of the global information society. This situation is largely due to the difference in Russian and the U.S. views on assessment of threats to information security and the key question of whether it would be possible to classify the use of ICT for military and political purposes as such threats, as well as regulatory approaches to the information space and the principles on which it will function.

Meanwhile, the Security Council, countering terrorist threats quite actively, adopted a range of resolutions that touch upon the issue of using ICT, including the Internet, for facilitating terrorism.

For example, the UNSC Resolution 1373 (2001)[25] calls on the Member States to accelerate the exchange of information on the use of ICT by terrorist groups and to suppress recruitment for terrorism; UNSC Resolution 1624 (2005)[26] on the prohibition of terrorist activity which also can be carried out with the use of the Internet, namely propaganda, incitement and justification for terrorism; UNSC Resolution 2129 (2013)[27] notes the relationship between terrorism and the development of ICT, particularly the Internet, the use of such technologies to commit terrorist attacks and also facilitate terrorist activity by incitement, recruitment, funding and planning of terrorist attacks with the use of the Internet and social media; UNSC Resolution 2178 (2014)[28] on foreign terrorist fighters calls on the Member States to act together in undertaking national measures to prevent terrorists from using technology, communications and sources for incitement of terrorist support. In 2017, the Security Council adopted the Resolution 2341 (2017)[29] on the protection of critical infrastructure facilities, expanding the states' capabilities to prevent terrorist attacks. The resolution suggests that the Member States consider possible preventive measures in undertaking national strategies and cybersecurity policies. The protection measures cover a wide range of issues, including planning, coordination and exchange of operational and intelligence information, screening, search, detection, cybersecurity, etc. The resolution mentions

[25] UNSC Resolution S/RES/1373 (2001) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/45/PDF/N0155745.pdf?OpenElement

[26] UNSC Resolution S/RES/1624 (2005) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/54/PDF/N0551054.pdf?OpenElement

[27] UNSC Resolution S/RES/2129 (2013) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/624/39/PDF/N1362439.pdf?OpenElement

[28] UNSC Resolution S/RES/2178 (2014) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/548/01/PDF/N1454801.pdf?OpenElement

[29] UNSC Resolution S/RES/2341 (2017) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf?OpenElement

such critical infrastructure facilities as the ones that are used “for the production, transmission and distribution of air, land and sea transport and for the provision of banking and financial services, water supply, food distribution and public health”. The Member States again stress the need for bringing together public and private sectors by organizing substantive consultations, cooperation with critical infrastructure operators, law enforcement and security officials, private business owners, including through joint training activities and application or creation of appropriate communication networks or emergency notification (pt. 5). The resolution calls on the Member States to introduce provisions on criminal responsibility for terrorist attacks on critical infrastructure facilities, as well as for planning, funding and logistical support of such attacks.

3. CURRENT THREATS TO INTERNATIONAL INFORMATION SECURITY.

The experts in international information security distinguish “a triad of threats” (the use of ICT for military, terrorist and criminal purposes)[30]. These three levels require different regulatory approaches and have different consequences for global information security:

– the issue of prevention of cyberwarfare should be classified as the level of public international law and intergovernmental relations;

– cyberterrorism is first of all politically motivated and aimed against governments, public authorities and society as a whole;

– cybercrime is a crime committed by citizens and the Internet users in the cyberspace, infringing on the security of information data, resources and systems.

Over the past five years, there have been negative trends associated with an increase in the scale and negative consequences of these threats. This demonstrates the need to take measures against the illegal use of ICT and to prevent them from being used to undermine international security. It should be noted that in practical terms, there is a mixture of the three categories of cyber-attacks, as there are difficulties both in terms of user identification, attribution (determination of the authorship of destructive actions in the information space and responsibility for their commitment), and in determining clear terminological, conceptual, and subsequently normative purviews. The military and political use of ICT remains a sensitive issue for a number of countries, and it is not always included in the multilateral international cooperation agenda.

Meanwhile, the global information space has provided opportunities for cross-border influence in violation of national state sovereignty and the principle of non-interference in the internal affairs of states. This creates new challenges in the system of international relations, which require an immediate response. The concept of digital sovereignty of states emerges and develops in this very context. State sovereignty in the ICT environment means its supremacy in the space of computing and information resources. The concept of digital sovereignty

[30] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime. Vienna, February 25-28, 2013.https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf; https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf

of states is supported by most countries of the world. Nevertheless, a number of states that oppose this concept argue that the establishment of State control over the national segment of the Internet and the content of the information space, due to its global and cross-border nature, may entail violation of the rights of foreign users to free access to information, freedom to seek, receive and impart information and ideas by any means and regardless of state borders (Article 19 of the Universal Declaration of Human Rights[31], Article 19, Paragraph 3 of the International Covenant on Civil and Political Rights[32]).

As for the military and political use of ICT, it is also worth noting that international law has not developed universally accepted concepts of war and armed struggle in the information space yet. However, such definitions appear in some international acts (Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, 2010[33]). Meanwhile, such definitions are necessary because the use of ICT in armed conflicts has a number of features that make its legal regulation difficult. These include, in particular, the absence of a prewar period and, as a consequence, the impossibility to determine the beginning of military force actions, as well as the possibility of carrying out aggressive actions using ICT without violating the borders of the State which such actions are aimed against. Besides, ICT are not weapons as such. All of this makes it difficult to qualify an information impact as an act of aggression. That is why it is important to develop a definition of "information weapons". The following questions are also subject to study: Can we consider national information infrastructure as a military object against which traditional weapons can be used in the event of a cyber-conflict? Which information infrastructure facilities need to be protected from the possible misuse of ICT on humanitarian grounds? Can the use of ICT to disturb the stability and order in another State be considered interference in internal affairs? These and other questions are raised by experts and scientists when considering a set of modernization issues of the current international law.

Practical examples of cyber-attacks on ICT networks and infrastructure include the use of Stuxnet, Duqu, Flame and Gauss viruses against information infrastructure in countries of the Middle East, attacks on servers of government agencies and private companies in Estonia in 2007 and Georgia in 2008, etc. They are interpreted by some experts as information war episodes[34].

Analysis of the international legal regulation of international information security shows that there is an intense debate on the international platform of interaction, primarily in the UN, which reflects the countries' attempts to find effective

[31] **Universal Declaration of Human Rights**
Adopted by UN General Assembly Resolution 217 A (III) on 10 December 10, 1948
https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

[32] **International Covenant on Civil and Political Rights**
Adopted by General Assembly resolution 2200 A (XXI) on 16 December,16 1966
https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[33] Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization (Yekaterinburg, June 16, 2009) https://base.garant.ru/2571379/

[34] Oleg Demidov. ENSURING INTERNATIONAL INFORMATION SECURITY AND RUSSIAN NATIONAL INTERESTS https://mail.pircenter.org/media/content/files/10/13559089230.pdf

international legal mechanisms to counter the challenges and threats in the information cyber space. It proves the relevance of putting this issue on the agenda of the coming model meeting of the UN Security Council within the framework of the Caspian International Model UN 2022.

4. REFERNCES

1. UN Security Council Resolution S/RES/1373 (2001) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/45/PDF/N0155745.pdf?OpenElement

2. UN Security Council Resolution S/RES/1624 (2005) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/54/PDF/N0551054.pdf?OpenElement

3. UN Security Council Resolution S/RES/2129 (2013) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/624/39/PDF/N1362439.pdf?OpenElement

4. UN Security Council Resolution S/RES/2178 (2014) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/548/01/PDF/N1454801.pdf?OpenElement

5. UN Security Council Resolution S/RES/2341 (2017) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf?OpenElement

6. Resolution A/RES/53/70 of the UN General Assembly dated December, 4 1998. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement

7. Resolution A/RES/54/49 of the UN General Assembly dated December 1, 1999. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElement

8. Resolution A/RES/55/28 of the UN General Assembly dated December 20, 2000. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/09/PDF/N0056109.pdf?OpenElement

9. Resolution A/RES/56/19 of the UN General Assembly dated November 29, 2001. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement

10. Resolution A/RES/57/53 of the UN General Assembly dated November 22, 2002. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/541/47/PDF/N0254147.pdf?OpenElement

11. Resolution A/RES/58/32 of the UN General Assembly dated December 8, 2003. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485.pdf?OpenElement

12. Resolution A/RES/66/24 of the UN General Assembly dated December 2, 2011. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/460/28/PDF/N1146028.pdf?OpenElemen t

13. Resolution A/RES/73/27 of the UN General Assembly dated December 5, 2018. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement

14. Resolution A/RES/73/187 of the UN General Assembly dated December 17, 2018. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/56/PDF/N1845056.pdf?OpenElement

15. Resolution A/RES/74/29 of the UN General Assembly dated December 12, 2019. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/10/PDF/N1941010.pdf?OpenElement

16. Resolution A/RES/75/240 of the UN General Assembly dated December 31, 2020. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement

17. Resolution A/RES/73/266 of the UN General Assembly dated December 22, 2018. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/04/PDF/N1846504.pdf?OpenElement

18. Resolution A/RES/74/28 of the UN General Assembly dated December 12, 2019. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/03/PDF/N1941003.pdf?OpenElement

19. Resolution A/RES/75/32 of the UN General Assembly dated December 7, 2020. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/354/02/PDF/N2035402.pdf?OpenElement

20. Universal Declaration of Human Rights

Adopted by UN General Assembly Resolution 217 A (III) on December 10, 1948 https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

21. International Covenant on Civil and Political Rights

Adopted by UN General Assembly resolution 2200 A (XXI) on December 16, 1966 https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

22. Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization (Yekaterinburg, June 16, 2009) https://base.garant.ru/2571379/

23. Developments in the Field of Information and Telecommunications in the Context of International Security: Report by the Secretary-General A/54/213 | 1999-08-10 https://digitallibrary.un.org/record/286090?ln=ru

24. World Summit on the Information Society

https://www.un.org/ru/events/pastevents/wsis.shtml

25. Okinawa Charter on the Global Information Society

July 21, 2000 http://www.kremlin.ru/supplement/3170

26. Document WSIS-03/GENEVA/DOC/4-R dated December 12, 2003, Original: English. Declaration of Principles Building the Information Society - a global challenge in the New Millennium https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf

27. Document WSIS-03/GENEVA/DOC/5-R dated December 12, 2003, Original: English. Plan of Action https://www.un.org/ru/events/pastevents/pdf/plan_wsis.pdf

28. Document WSIS-05/TUNIS/DOC/6(Rev.1)-R dated November 15, 2005, Original: English. Chair of the Preparatory Committee for the Tunis Phase TUNIS AGENDA FOR THE INFORMATION SOCIETY https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

29. Document WSIS/PC-2/DOC/5-R dated January 15, 2003, Original: English. Note by the WSIS Executive Secretariat REPORT OF THE WSIS PAN-EUROPEAN REGIONAL CONFERENCE (Bucharest, November 7-9, 2002) https://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-R.pdf

30. Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime. Vienna, 25-28 February 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf; https://www.unodc.org/documents/organized-

crime/cybercrime/Cybercrime_Study_Russian.pdf

31. The Ministry of Communications of the Russian Federation, STATE TELECOMMUNICATION COMMISSION DECISION No. 49 “On the outcomes of the ITU Plenipotentiary Conference (Marrakesh, 2002) and work of the Russian Communications Administration on it” dated December 25, 2002 https://docs.cntd.ru/document/901858785

32. Rassolov I.M. Law and cybernetic space. Monograph. - 2nd ed. - Moscow: Moscow Bureau for Human Rights, 2016, pp.7-10

33. Demidov Oleg. ENSURING INTERNATIONAL INFORMATION SECURITY AND RUSSIAN NATIONAL INTERESTS https://mail.pircenter.org/media/content/files/10/13559089230.pdf

34. SECURITY INDEX No. 1 (104), Vol. 19