INTERNATIONAL SECURITY LAW

DOI: https://doi.org/10.24833/0869-0049-2020-1-44-53

Research article
Received 29 November 2019
Approved 2 March 2020

Andrey A. DANELYAN
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
53/2-1, ul. Ostozhenka, Moscow, Russian Federation, 119021
danel1@mail.ru
ORCID: 0000-0001-5771-0888

Elena E. GULYAEVA
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
53/2-1, ul. Ostozhenka, Moscow, Russian Federation, 119021
gulya-eva@yandex.ru
ORCID: 0000-0001-8376-7212

INTERNATIONAL LEGAL ASPECTS OF CYBERSECURITY

INTRODUCTION. *In the modern world, the number of crimes committed in cyberspace has significantly increased. New types of malware used to achieve illegal goals appear regularly. According to experts, the material damage to the global economy from crimes committed with the help of information and communication technologies amounts to trillions of US dollars. Such a scale requires effective means of legal regulation of relations in cyberspace. Cybersecurity is considered one of the most relevant topics of current international law, which is extremely important for ensuring the national security of states. Information and communication technologies can be used to negatively affect economic, social, cultural and political relations, to damage the economic, military, and defense potential of the state and society. In this regard, the international community is deeply interested in developing a multilateral legal framework for cooperation in the field of cybersecurity. However, a unified approach to solving this problem in the international arena has not yet been developed. Legal regulation of cyberspace is very complex due to the virtual interface characteristics of this area.*

MATERIALS AND METHODS. *The material for the study is the works of Russian and foreign researchers in the field of international law, international legal acts adopted in the framework of the UN and the European Union, draft UN conventions, national regulatory legal acts of the Russian Federation, the People's Republic of China and other states as well as judicial practice of international courts. The research methodology is based on general and specific scientific methods of cognition (the dialectical method, methods of analysis and synthesis, deduction and induction, comparative legal and historical legal methods).*

RESEARCH RESULTS. *The analysis showed that despite the applicability of the principles and rules of current international law to the information sphere, the universalization of the international legal regulation of cyberspace is required, taking into account its characteristics and in order to effectively combat the use of information and communication technologies for illegal purposes. The efforts of states to develop special rules of conduct in cyberspace are currently concentrated on a narrow sphere of issues related to human rights, data privacy, etc. Not all states are interested in creating a modern and effective mechanism for cooperation in cyberspace. Many states are openly opposing the development of new international legal instruments. For this reason, the Russian initiative to adopt the UN Convention on Cooperation in Combating Information Crimes has not been support-*

ed. This fact has entailed the absence of a full-fledged universal international legal framework for cooperation in the field of cyberspace.

DISCUSSION AND CONCLUSIONS. *Based on the analysis of doctrine and practice, the authors conclude that there is a need to create a universal international legal framework for cooperation in the field of cyberspace. In modern international law, cybersecurity is one of the most pressing problems directly related to state security. The difference in the approaches of states to the problem of ensuring cybersecurity at the present stage entails the absence of an effective multilateral legal framework for cooperation in this area.*

KEYWORDS: *cyberspace, cybercrime, cybersecurity, internet, information and communication technologies (ICT), information war, Tallinn Manual, Budapest Convention, international law*

FOR CITATION: Danelyan A.A., Gulyaeva E.E. International Legal Aspects of Cybersecurity. – *Moscow Journal of International Law.* 2020. No.1. P. 44–53. DOI: https://doi.org/10.24833/0869-0049-2020-1-44-53

The authors declare the absence of conflict of interests.

ПРАВО МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

DOI: https://doi.org/10.24833/0869-0049-2020-1-44-53

Исследовательская статья
Поступила в редакцию: 29.11.2019
Принята к публикации: 02.03.2020

Андрей Андреевич ДАНЕЛЬЯН
Дипломатическая академия МИД России
Остоженка ул., д. 53/2-1, Москва, 119021, Российская Федерация
danel1@mail.ru
ORCID: 0000-0001-5771-0888

Елена Евгеньевна ГУЛЯЕВА
Дипломатическая академия МИД России
Остоженка ул., д. 53/2-1, Москва, 119021, Российская Федерация
gulya-eva@yandex.ru
ORCID: 0000-0001-8376-7212

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ

ВВЕДЕНИЕ. *В современном мире существенно возросло количество преступлений, совершаемых в киберпространстве. Регулярно появляются новые виды вредоносного программного обеспечения, используемого для достижения незаконных целей. По оценкам экспертов, материальный ущерб мировой экономике от преступлений, совершаемых с помощью информационно-коммуникационных технологий, исчисляется триллионами долларов США. Такие масштабы требуют эффективных средств правового регулирования отношений, складывающихся в киберпространстве. Кибербезопасность считается одной из самых актуальных тем современного международного права, крайне важной для обеспечения национальной безопасности государств. Информационно-коммуникационные технологии могут быть*

использованы в целях негативного воздействия на экономические, социальные, культурные и политические отношения, нанести ущерб экономическому, военному, оборонному потенциалу государства и общества. В связи с этим международное сообщество проявляет серьезную заинтересованность в разработке многосторонней правовой основы сотрудничества в области кибербезопасности. Однако единый подход к решению данной задачи на международной арене пока так и не выработан, поскольку сложность правового регулирования киберпространства обусловлена виртуальной характеристикой складывающихся в этой сфере отношений.

МАТЕРИАЛЫ И МЕТОДЫ. *Материалом для исследования послужили труды российских и зарубежных исследователей в области международного права, международно-правовые акты, принятые в рамках ООН и Европейского Союза, проекты конвенций ООН, национальные нормативно-правовые акты Российской Федерации, Китайской Народной Республики и др. государств, а также материалы судебной практики международных судов. Методологическую основу исследования составили общенаучные и частно-научные методы познания (диалектический метод, методы анализа и синтеза, дедукции и индукции, сравнительно-правовой и историко-правовой методы).*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *Проведенный анализ показал, что несмотря на применимость принципов и норм современного международного права к информационной сфере, требуется универсализация существующего международно-правового регулирования применительно к киберпространству с учетом его определенной специфики и в целях эффективного правого противодействия использованию информационно-коммуникационных технологий в незаконных целях. Усилия государств по разработке специальных правил поведения в киберпространстве сконцентрированы в настоящее время на узкой сфере вопросов, касающихся прав человека, конфиденциальности данных и др. Далеко не все государства заинтересованы в создании современного и эффективного механизма сотрудничества в киберпространстве, открыто выступая против разработки новых международно-правовых инструментов. По этой причине российская инициатива о необходимости принятия Конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности» не нашла поддержки, что влечет за собою отсутствию полноценной универсальной международно-правовой базы сотрудничества в сфере киберпространства.*

ОБСУЖДЕНИЯ И ВЫВОДЫ. *В статье на основании анализа доктрины и практики обосновывается вывод о необходимости создания универсальной международно-правовой базы сотрудничества в сфере киберпространства. В современном международном праве кибербезопасность является одной из самых актуальных проблем, непосредственно связанной с безопасностью государства. Различие подходов государств к проблеме обеспечения кибербезопасности на современном этапе влечет за собою отсутствие эффективной многосторонней правовой основы сотрудничества в данной сфере.*

КЛЮЧЕВЫЕ СЛОВА: *киберпространство, киберпреступность, кибербезопасность, интернет, информационно-коммуникационные технологии (ИКТ), информационная война, «Таллинское руководство», «Будапештская конвенция», международное право*

ДЛЯ ЦИТИРОВАНИЯ: Данельян А.А., Гуляева Е.Е. 2020. Международно-правовые аспекты кибербезопасности. – *Московский журнал международного права.* №1. С. 44-53. DOI: https://doi.org/10.24833/0869-0049-2020-1-44-53

Авторы заявляют об отсутствии конфликта интересов.

1. Introduction

The term cyberspace has appeared fairly recently. The majority of experts believe that it was initially used by a speculative fiction writer W. Gibson in 1981.[1] Etymologically, the word is derived from the word *cybernetics* – the science that deals with general principles of operation procedures and information transfer in machines, living organisms, and human society [Wiener 1948:14].

In research literature, cyberspace is often mistakenly associated with the Internet. One of the reasons for this mistake is the absence of a commonly accepted definition of what *cyberspace* means. According to an American expert F.D. Kramer, the Western scientific doctrine includes about 28 definitions of the term *cyberspace*[2]. A French professor S.I. Laurent notes that cyberspace is a social and technical reality, which is closely related to the political context[3]. D.E. Dobrinskaya suggests that cyberspace is a product of any information and communication technologies (ICT), including the Internet [Dobrinskaya 2018:58]. The US Congressional Research Service perceives cyberspace as a comprehensive multiplicity of connections among people that are based on computers and telecommunications, regardless of their physical and geographic location [Makarenko 217:237]. At the same time, according to the US Department of Defense, cyberspace is a sphere of radio electronic means, i.e. the means of radio detection, location, navigation, automatization, control, and guidance. They are used for receiving, transferring, processing, storing, and transforming information. On top of that, cyberspace is a part of the information structure of the armed forces[4]. In China, a law on cybersecurity came into force on June 1, 2017. It covers the work of network resources providers as well as the services related to gathering, storing, and processing of user data. The law also has sections about the way the security of the information infrastructure must be provided in strategically important branches. It is claimed to protect national «cybersovereignty» of the People's Republic of China[5]. The Russian Federation has no current internal legal acts with the word *cyberspace*[6]. However, the Decree of the President of the Russian Federation of December 5, 2016 has approved the Doctrine of Information Security of the Russian Federation in which the information sphere is understood as a complex of software, IT systems, Internet websites, communication networks, and information technologies. It also includes persons who produce and process information alongside with developing and using the abovementioned technologies. The tools for controlling the corresponding social relations are on the list too[7].

Cyberspace is a combination of computers, mobile devices, and users that interact at a distance. The Internet, in its turn, is used to connect these computers and mobile devices. Cyberspace is wider than the Internet because the Internet is included into cyberspace. In modern conditions, cyberspace is becoming the main channel for distributing and storing information.

---

[1] For the first time, Canadian-American science-fiction writer William Gibson used the concept of «cyberspace» in 1982 in his short story «Burning Chrome», and then popularized it in 1984 in the novel «Neuromancer». In the novel «Neuromancer», the author described cyberspace as a «consensual hallucination», which is difficult to distinguish from reality and in which computer systems are a kind of substitute for the real world that exists only in the memory of computers and the minds of its users.

[2] See: Miguleva M.V. Kiberprostranstvo kak strategicheskii instrument sotsial'noi inzhenerii. Doklad na V mezhdunarodnoi nauchnoi konferentsii «Kitai i Rossiya: gosudarstvennye strategii razvitiya» [Cyberspace as a strategic tool of social engineering. Report at the 5th International Scientific Conference "China and Russia: State Development Strategies"]. – *Whatisgood.ru.* October 10, 2018. (In Russ.). URL: https://whatisgood.ru/theory/analytics/kiberprostranstvo-kak-strategicheskiy-instrument/ (accessed 10.09.2019).

[3] Ibid.

[4] See: Cover Sheet for Air Force Doctrine Document (AFDD) 3-13. Information Operations. URL: https://fas.org/irp/doddir/usaf/afdd3-13.pdf (accessed 10.09.2019).

[5] The Law on Cybersecurity of the People's Republic of China. (In Chinese). URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (accessed 10.09.2019).

[6] Except the Draft of the Concept of the Cybersecurity Strategy of the Russian Federation, prepared by the Council of the Federation of the Federal Assembly of the Russian Federation. See: Kontseptsiya strategii kiberbezopasnosti Rossiiskoi Federatsii. Proekt [Draft of the Concept of the Cybersecurity Strategy of the Russian Federation]. (In Russ.). URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (accessed 10.09.2019).

[7] Ukaz Prezidenta RF ot 05.12.2016 No. 646 "Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii"[Decree of the President of the Russian Federation dated December 5, 2016 No. 646 «On approval of the Doctrine of Information Security of the Russian Federation»]. – *Sobranie zakonodatel'stva Rossiiskoi Federatsii* [Collection of the Legislation of the Russian Federation]. December 12, 2016. No. 50. Art. 7074. (In Russ.).

We support the valid point raised in research literature that the problems of cyberspace in general and cybersecurity in particular became urgent during the Gulf War of 1990-1991. In that conflict, the latest military technical achievements were combined with powerful information campaign and press coverage.

After this event, scientists and politicians began to rethink the concepts of *information war* and *cyberwar*. Cyberspace is now seen as the «fifth space»[8] used to achieve political goals through ICT [Warden 1995].

These new circumstances provoked the international need to resolve the issue of applicability of the existing international legal rules and principles to the information sphere. It is also necessary to work out special rules of conduct in cyberspace to rightfully combat the use of ICT for illegal purposes.

2. Analysis of doctrinal approaches and modern international legal regulation of cyberspace

In recent years, this issue has been the subject of research done by many experts in Russian and foreign doctrines of international law, but solutions have not yet been found[9].

The scientific community has long been discussing the question: is it possible to apply existing international legal rules to cyberspace, or would it be better to develop new rules for regulating this sphere of relations?

If we assume that international legal obligations of various states, including international treaties, are not applicable to cyberspace, we would have to conclude that there is no legal regulation in this sphere. Consequently, states are free from any international legal obligations when cyberspace is in question. In other words, we would face a legal gap and be very skeptical about state sovereignty in cyberspace. At the same time, it would make it necessary to adopt rules for cyberspace, and these rules would not be based on the principles of the UN Charter. For this reason, it is unacceptable for us to assume that cyberspace is not legally regulated by the rules of current international law. But the question arises: which of the existing rules of international law are applicable to cyberspace?

According to A. Streltsov, the main sources of law in this area are the UN Charter and international treaties, stemming from the UN Charter provisions on ensuring international peace and security. Among those are international treaties on humanitarian aspects of warfare, and decisions of the International Court of Justice, in which the provisions of international law on the use of force are interpreted[10].

We believe that such principles and rules of international law as non-use of force and threat of force, non-interference in matters within the internal competence of states, the obligation of states to cooperate with each other, the sovereign equality of states, respect for human rights and fundamental freedoms, etc. are applicable to cyberspace.

However, cyberspace is rather specific due to the virtual interface characteristics of the global information space. It is an object of law where distance does not matter. In this respect, not all generally recognized principles and rules of international law can be applied to cyberspace by a simple extrapolation of concepts. For example, such concepts as *act of aggression, use of force,* and *armed attack* cannot be applied to a cyber attack. The concept of *information war* used by political scientists and the media cannot be applied to the concept of war in its international legal sense. Some obligations of states can be fulfilled in cyberspace according to the *mutatis mutandis* principle, with changes based on the special nature of cyberspace. We also should admit that it is sometimes difficult to adapt conceptual foundations of the international rule of law to the threats that arise in cyberspace.

In contrast to our view, the drafters of the Tallinn Manual on the International Law Applicable to Cyber Warfare[11] proceed from the assumption that cyberspace does not differ from other fields of relations, and it does not require special approaches to its legal regulation. In their opinion, the basic principles of international law and international humanitarian law are applicable to what people do in cyberspace. Thus, according to the Tallinn Manual,

[8] Along with land, sea, air space and outer space.

[9] See: [Gelbstein, Kurbalija 2005; Malcolm 2008; Batueva 2009:15-22; Mathiason 2009; Bedritsky 2010:25:40; Knake 2010; Mueller 2010; Kasenova 2012:18-24; Mansell 2012; Kasenova, Yakushev 2013; Kasenova 2013:43-64; Determann, Guttenberg 2014:875-902; Krutskikh, Strel'tsov 2014: 20-34].

[10] Strel'tsov A. O problemakh adaptatsii mezhdunarodnogo prava k informatsionnym konfliktam [On the problems of adapting international law to information conflicts]. – *Digital.Report.* July 24, 2015. (In Russ.). URL: https://digital.report/problemyi-adaptatsii-mezhdunarodnogo-prava-k-informatsionnyim-konfliktam/ (accessed 12.09.2019).

[11] Not legally binding.

the term weapon is applicable to cyber technologies. Large-scale cyber attacks can be considered as armed attacks, under Article 51 of the UN Charter.

In its essence, the Tallinn Manual covers two main aspects: the *jus ad bellum* principle, which determines the conditions for the use of force by a state in international relations, and the *jus in bello* principle, which is about humanitarian points of a conflict. The main source of *jus ad bellum* law is the UN Charter, and the main sources of *jus in bello* law are the Hague Conventions, the Geneva Conventions, and other international treaties, which have stemmed from their provisions and ideas.

A number of research articles written by Russian and foreign experts in international law address adaptation of international law of armed conflict to cyberspace. A. Streltsov notes that Article 41 and Article 42 of the UN Charter distinguish two main types of *force*: the force related to the use of weapons and the force that has nothing to do with weapons. He stresses that malicious use of ICT is mainly regulated by the rules of Article 2 (4) of the UN Charter. Article 2 (4) requires that member-states refrain from the threat or use of force in international relations, including the ones in cyberspace[12]. According to A. Streltsov, despite the obvious possibility of using ICT for military purposes, almost all experts believe that ICT are not weapons [13].

However, in accordance with the advisory opinion of the International Court of Justice on legality of the threat or use of nuclear weapons (1996), implementation of the right to self-defense does not depend on the type of weapons being used to attack. The fact of use of force is enough [14].

Analysis of current practice shows that interpretations of the *weapons* concept are expanding. For example, the terrorist attack with the use of captured aircrafts on September 11, 2001 was de facto equated to an *armed attack* under Article 51 of the UN Charter. In this case, the civilian aircrafts, which were not weapons by nature, were turned into the attack instrument. The United States, with the support of the international community, declared its right to individual and collective self-defense.

W.M. Stahl holds a slightly different opinion. He thinks that provisions of the UN Charter do not allow us to clearly equate a hacker attack by one state on another to an armed attack, which gives the nation the right to use force. In addition, the *use of force* concept in the UN Charter does not cover terrorists and other non-state actors who are often behind hacker attacks. Since cybernetic aggressions are out of traditional classifications used for internationally recognized rules of warfare, it is generally accepted that states should treat hacker attacks as a type of crime[15].

To clarify the abovementioned viewpoint, a number of experts ask the following questions: What situations are covered by the *armed conflict* concept in the information sphere? What is the range of individuals protected by law in such conflicts? Where is the line beyond which a non-international informational armed conflict becomes an international one? What rules of law (international or domestic) regulate the actions of belligerents in such conflicts? [Kozik 2008].

Customary international law presumes that not every use of force can be considered as an armed attack. The decision of the International Court of Justice in the case concerning military and paramilitary activities in and against Nicaragua of 27 June 1986 set out a scale criterion for an armed attack by one state on another. Subsequently, the *scale criterion* was confirmed in a number of other decisions of the International Court of Justice[16].

In the context of the use of ICT, the scale criterion can theoretically be considered met when a cyber attack goes beyond minor incidents. For example, the collapse of infrastructure, which cannot be fixed quickly enough. It blocks the state's ability to act or ruins the basic living conditions of the population. Thus, if the consequences of a cyber attack can be equated to an attack by regular armed forces, the scale criterion can be considered met.

---

[12] Strel'tsov A. Op. cit.

[13] Ibid.

[14] «These provisions do not apply to specific weapons. They app1y to any use of force, regardless of the weapons employed». International Court of Justice: Legality of the threat of use of nuclear weapons. ICJ Advisory Opinion. July 8,1996. Para 39. URL: https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (accessed 13.09.2019).

[15] Stahl W.M. Kiberbezopasnost' i mezhdunarodnoe parvo [Cybersecurity and International Law]. – *Interlaws.Ru.* February 26, 2017. (In Russ.). URL: https://interlaws.ru/kiberbezopasnost-i-mezhdunarodnoe-pravo/ (accessed 10.09.2019).

[16] See: International Court of Justice: Case concerning oil platforms. Judgement. November 6, 2003. Paras 51, 62. URL: https://www.icj-cij.org/files/case-related/90/090-20031106-JUD-01-00-EN.pdf(accessed 10.09.2019); Eritrea-Ethiopia Claims Commission - Partial Award: Jus Ad Bellum - Ethiopia's Claims 1-8. December 19, 2005. – *Reports of International Arbitral Awards.* 2009. Vol. XXVI. P. 457-469. URL: https://legal.un.org/riaa/cases/vol_XXVI/457-469.pdf(accessed 10.09.2019).

It should be noted that the scale criterion is not recognized by all states. For example, the US State Department objected to the fact that the International Court of Justice used the scale criterion in decisions on Nicaragua and oil platforms.

The traditional requirements for justifying a state's response to an armed attack, i.e. implementation of the right to self-defense under Article 51 of the UN Charter, are necessity and proportionality. These requirements are not directly enshrined in the UN Charter, but they reflect the international custom in this area[17].

Under current international law, for justifying the use of force in response to an armed attack, it must be determined that another state is responsible for the attack. When cyberspace is in question, it is quite difficult to identify the attackers and determine if they are operating under the control of the state. While the location of the attack target is obvious, the location of the attackers is often undetectable.

So, there are certain difficulties in applying the rules of current international law to cyberspace. In our opinion, solutions for many problems could be facilitated by discussing them with technical specialists in the field of ICT, including military purposes.

To facilitate practical implementation of the right to self-defense under Article 51 of the UN Charter, the international community should develop clear categories that would allow defining a cyber attack as the use of force or the act of aggression. It is also necessary to work out appropriate criteria for qualifying ICT as weapons. Anyway, it is not an easy task to do.

Unfortunately, if we turn to the issue of creating new rules for regulating cyberspace, the efforts of states are currently focused on a narrow area of problems related to human rights, data privacy, etc. Moreover, not all states are interested in creating an effective mechanism for cooperation. Many states are openly opposing the development of new international legal instruments. For this reason, there is no comprehensive international legal environment for cyberspace.

The only multilateral treaty dealing with criminal activities in the field of information technologies is the Convention on Cybercrime, adopted on 23 November 2001 in Budapest[18].

The Convention has five main objectives: 1) harmonization of substantive criminal law to combat cybercrime; 2) harmonization of criminal procedure law; 3) promotion of mutual legal assistance; 4) codification of international law with an emphasis on jurisdictional rules based on territoriality; 5) providing a legal framework to promote understanding of issues related to cybercrime.

The Convention has articles on crimes against confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices); computer-related offenses (computer-related forgery, computer-related fraud); offenses related to child pornography; offences related to infringement of copyright and related rights.

It should be taken into account that this Convention was drafted at the time when the level of ICT was low and many types of network threats were not yet known[19]. For this reason, Articles of the Convention do not even mention *botnets, phishing, spam,* and other tools used by hackers.

However, the approach laid down in paragraph "b" of Article 32 of the Budapest Convention is unacceptable for Russia and many other countries. This rule deserves to be quoted in full: «A Party may, without the authorization of another Party: … b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system»[20]. As you can see this provision makes it possible for a state party to obtain trans-border access to information, the source of which is located in another state. It can be done without notifying the relevant authorities of the state where the source of information is located. In our opinion, this way the Budapest Convention establishes a loophole for a violation of the state sovereignty principle in the information space. It is unacceptable.

It is important that paragraph 32 (b) of the Budapest Convention provides fertile ground for violating

[17] In addition to the Judgments for Nicaragua and the Oil Platforms of the International Court of Justice of the United Nations, as well as the Advisory Opinion on the Use of Nuclear Weapons, Judgment of the International Court of Justice of the United Nations concerning Military and Paramilitary Activities in Congo can be cited.

[18] Council of Europe: Convention on Cybercrime. Budapest. November 23, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed 11.09.2019).

[19] The Convention was developed since 1997 and was open for signature in 2001.

[20] Council of Europe: Convention on Cybercrime. Budapest. November 23, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed 11.09.2019)

fundamental human rights and freedoms in the digital sphere, the right to privacy in particular.

There are also some other regional and bilateral tools for combating cybercrime, but they do not contribute to common understanding of the key aspects of countering illegal behavior in cyberspace.

3. Russian initiatives in the field of cyberspace regulation

In this context, the Russian Federation highlights the need to develop a universal international legal framework for cooperation and common cyber vocabulary. Russian experts have worked out and distributed a Draft United Nations Convention on Cooperation in Combating Information Crimes[21] for review in international forums[22].

Article 1 of the Convention sets out its three main objectives: a) to promote and strengthen measures aimed at effectively preventing and combating crimes and other unlawful acts in the field of ICT; b) to prevent action directed against the confidentiality, integrity and availability of ICT as well as the misuse of ICT by providing for the punishability of such acts, as described in this Convention, and by providing powers sufficient for effectively combating such crimes and other unlawful acts, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by developing arrangements for international cooperation; c) to improve the efficiency and develop international cooperation, including in the context of training and providing technical assistance in preventing and combating ICT crimes[23].

The Convention includes lots of old and relatively new concepts: *botnet, malicious software, child pornography, information and communication technologies (ICT), information, critical infrastructure facilities, spam, ICT device,* etc. For example, botnet means «two or more ICT devices with malicious software downloaded which is managed centrally and without users' knowledge»[24]. *ICT* refers to a set of methods, production processes, and software-and-hardware facilities combined to generate, transform, transmit, use, and store information[25]. *Spam* is defined as «delivery of electronic messages on the address list (data base) to those who do not communicate the sending party their addresses for message delivery and do not give their consent to be sent such messages and are unable to deny the delivery of such messages from the sending party»[26].

The Convention also presumes technical assistance, mutual legal assistance at the pre-trial stage, including cases of emergency, and the mechanism to implement its provisions.

Chapter II of the Convention establishes liability for: unauthorized access to electronic information; unauthorized interception; unauthorized impact on data; disruption of ICT operation; creation, utilization and distribution of malicious software; distribution of spam; creation and utilization of botnets; offenses related to child pornography; phishing-related offenses, etc.

Extradition of persons suspected of committing crimes is governed by Article 48 of the Convention. This article provides for one of the fundamental principles of international criminal law cooperation – *aut dedere aut judicare* (extradite or prosecute).

To ensure the provision of immediate assistance for the purpose of investigations, prosecutions or judicial proceedings concerning criminal offences related to computer systems and data, or for electronic evidence-gathering of criminal offences, Article 57 of the Convention states that each state party must designate a point of contact available on a twenty-four hour, seven-day-a-week basis (24/7 Network).

---

[21] Draft United Nations Convention on Cooperation in Combating Information Crimes. URL: https://www.rusemb.org.uk/fnapr/6394 (accessed13.09.2019).

[22] The document was distributed during presentations at the XV Meeting of the Heads of special services, security agencies and law enforcement agencies of foreign states - partners of the FSB of Russia (St. Petersburg, July 27-28, 2016), The Eighth International Meeting of High Representatives in charge of Security (Varaksino, Tver Oblast, May 23-25, 2017), "on the sidelines" of the 26th session of the Commission on Crime Prevention and Criminal Justice (Vienna, May 22-26 2017), IV World Conference on the Internet (Wuzhen, PRC, December 3-5, 2017). On December 28, 2017, the Russian draft was circulated as an official document of the UN General Assembly under agenda item 107 of its 72nd session «Crime Prevention and Criminal Justice» (No. A / C.3 / 72/12 of October 16, 2017). This document was translated from Russian into all the official languages of the Organization and electronically posted on the official websites of the UN and the Russian Foreign Ministry.

[23] Draft United Nations Convention on Cooperation in Combating Information Crimes. URL: https://www.rusemb.org.uk/fnapr/6394 (accessed 13.09.2019).

[24] Ibid.

[25] Ibid.

[26] Ibid.

The Convention specifies the main areas of activities for the development and improvement of special training programs for the personnel responsible at the national level for preventing and combating ICT crimes. The aim is to trigger the development and planning of strategic policies to combat ICT crimes.

To implement its provisions, the Convention establishes a Conference of states parties to enhance their corresponding opportunities and cooperation among them.

It is proposed that the Conference of the state parties establish an International Technical Commission as a permanent body to combat ICT crimes and to increase the degree of coordination between the state parties to the Convention.

As we have noted above, the Draft United Nations Convention on Cooperation in Combating Information Crimes was distributed in different international forums. On December 28, 2017 it was presented as an official document of the UN General Assembly under item 107 of the 72nd session agenda «Strengthening the United Nations crime prevention and criminal justice program, in particular its technical cooperation capacity». The document has been translated from Russian into all official languages of the United Nations and is available on the official websites of the United Nations and of the Russian Ministry of Foreign Affairs.

However, some delegations are opposing this Draft Convention as well as the development of any new international legal tools in this area. They insist that the existing international legal instrument, namely the Budapest Convention, is sufficient to successfully combat crime in cyberspace.

4. Conclusion

Thus, though the principles and rules of current international law are applicable to the information sphere, it is necessary to universalize the existing international legal regulation of cyberspace, taking into account its specific characteristics and in order to effectively combat the use of ICT for illegal purposes.

The efforts of states are currently focused on a narrow area of problems related to human rights, data privacy, etc. Not all states are interested in creating an effective mechanism for cooperation. Many states are opposing the development of new international legal instruments. That is why the Russian initiative on the UN Convention on Cooperation in Combating Information Crimes has not been supported. This fact has entailed the absence of a full-fledged universal international legal framework for cooperation in the field of cyberspace.

References

1. Batueva E.V. Politicheskii dialog po voprosam upravleniya Internetom [Political Dialogue on Internet Governance Issues]. – *Mirovaya politika: novye problemy i napravleniya: sbornik nauchnykh statei.* Pod red. M.M. Lebedevoi [World Politics: new problems and directions: collection of scientific articles. Ed. by M.M. Lebedeva]. Moscow: MGIMO-Universitet Publ. 2009. P. 15-22. (In Russ.)
2. Bedritsky A.B. Amerikanskaya politika kontrolya nad kiberneticheskim prostranstvom [American Policy of Control over Cyber Space]. – *Problemy natsional'noi strategii.* 2010. No. 2. P. 25-40. (In Russ.)
3. Determann L., Guttenberg K.T. On War and Peace in Cyberspace: Security, Privacy, Jurisdiction. – *Hastings Constitutional Law Quarterly.* 2014. Vol. 14. No. 1. P. 875-902.
4. Dobrinskaya D.E. Kiberprostranstvo: territoriya sovremennoi zhizni [Cyberspace: territory of contemporary life]. – *Vestnik Moskovskogo universiteta.* Seriya 18. Sotsiologiya i politologiya. 2018. Vol. 24. No.1. P. 52-70. (In Russ.). DOI: https://doi.org/10.24290/1029-3736-2018-24-1-52-70
5. Gelbstein E., Kurbalija J. *Internet Governance: issues, actors and divides*. Msida: Diplo Foundation. 2005. 144 p.
6. Kasenova M. B., Yakushev M. V. *Upravlenie internetom. Dokumenty i materialy* [Internet Governance. Documents and Materials]. Saint Petersburg: Tsentr Gumanitarnykh Initsiativ Publ. 2013. 395 p. (In Russ.)
7. Kasenova M.B. Global''noe upravlenie Internetom v kontekste sovremennogo mezhdunarodnogo prava [Global Internet Governance in the Context of Modern International Law]. – *Indeks bezopasnosti.* 2013. Vol. 19. No. 1. P. 43-64. (In Russ.)
8. Kasenova M.B. Internet i mezhdunarodnoe publichnoe pravo: retrospektiva doktrinal'nykh podkhodov [The Internet and International Public Law: A Retrospective of Doctrinal Approaches]. – *Mezhdunarodnoe chastnoe i publichnoe parvo.* 2012. No. 2. P. 18-24. (In Russ.)
9. Knake R. I*nternet Governance in the Age of Cyber Insecurity.* New York: Council on Foreign Relations. 2010. 43 p
10. Kozik A. L. Razvitie informatsionnykh tekhnologii i pravovoe regulirovanie obshchestvennykh otnoshenii [The Development of Information Technology and the Legal Regulation of Public Relations]. – *Studii Juridice Universitare.* 2008. No. 3–4. P. 142–152. (In Russ.)
11. Krutskikh A.V., Strel'tsov A.A. Mezhdunarodnoe pravo i problema obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti [International Law and the Problem of Ensuring International Information Security]. – *Mezhdunarodnaya zhizn'.* 2014. No.11. P.20-34. (In Russ.)
12. Makarenko S.I. *Informatsionnoe protivoborstvo i radioelektronnaya bor'ba v setetsentricheskikh voinakh nachala XXI veka. Monografiy*a [Information Confrontation and Electronic Warfare in Network-centric Wars at

the Beginning of the XXI Century. A Monograph]. Saint Petersburg: Naukoemkie tekhnologii Publ. 2017. 546 p. (In Russ.)
13. Malcolm J. *Multi-stakeholder Governance and the Internet Governance Forum.* Perth: Terminus Press. 2008. 611 p.
14. Mansell R. *Imagining the Internet: Communication, Innovation, and Governance.* Oxford: Oxford University Press. 2012. 289 p.
15. Mathiason J. *Internet Governance: the New Frontier of Global Institutions.* New York: Routledge. 2009. 178 p.
16. Mueller M.L. *Networks and States: the Global Politics of Internet Governance.* Cambridge, Mass: MIT Press. 2010. 313 p.
17. Warden J. A. The Enemy as a System. – *Airpower Journal.* 1995. Vol. 9. No. 1. P. 41-55.
18. Wiener N. *Cybernetics or Control and Communication in the Animal and the Machine.* Cambridge, Mass.: The Technology Press. 1948. 194 p.

About the Authors

Andrey A. Danelyan,
Doctor of Juridical Sciences, Professor, Head of the Department of International Law, Diplomatic Academy of the Ministry of Foreign Affairs of Russia

53/2-1, ul. Ostozhenka, Moscow, Russian Federation, 119021

danel1@mail.ru
ORCID: 0000-0001-5771-0888

Elena E. Gulyaeva,
Cand. Sci. (Law), Associate Professor at the Department of European Studies, Diplomatic Academy of the Ministry of Foreign Affairs of Russia

53/2-1, ul. Ostozhenka, Moscow, Russian Federation, 119021

gulya-eva@yandex.ru
ORCID: 0000-0001-8376-7212

Информация об авторах

Андрей Андреевич Данельян,
доктор юридических наук, профессор, заведующий кафедрой международного права, Дипломатическая академия МИД России

119021, Российская Федерация, Москва, Остоженка ул., д. 53/2-1

danel1@mail.ru
ORCID: 0000-0001-5771-0888

Гуляева Елена Евгеньевна,
кандидат юридических наук, доцент кафедры европейского права Дипломатическая академия МИД России

119021, Российская Федерация, Москва, Остоженка ул., д. 53/2-1

gulya-eva@yandex.ru
ORCID: 0000-0001-8376-7212