DOI 10.52468/2542-1514.2022.6(4).32-44

THE CONCEPT OF CYBERSPACE IN INTERNATIONAL LAW

Ksenia A. Ivanova[1,2], Madi Zh. Myltykbaev[3], Daria D. Shtodina[3]

[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia*

[2] *University of Tyumen, Tyumen, Russia*

[3] *MGIMO University, Moscow, Russia*

Article info

Received –
2022 March 09
Accepted –
2022 September 20
Available online –
2022 December 20

Keywords

Cyberspace, international law, international information security, Internet, UN Group of Governmental Experts, ICT, cyber regulation in international law

The subject. The article is devoted to the analysis of approaches in the development of the concept of cyberspace in international law.

The purpose of this article is to try to highlight the attributes of cyberspace, which will allow to resolve existing gaps in the field of universal cyber regulation in international law.

The research presented in this article was conducted by combining various disciplinary approaches, including comparative law, comparative politics and international relations, political theory, and sociology. In addition, the study includes methods of dialectical logic, analysis and synthesis, as well as a formal-legal analysis of UN international legal acts.

The main results and scope of their application. As states pay increasing attention to cyberspace management as the technical architecture that powers the global Internet and governance in cyberspace, in terms of how states, corporations and users can use this technology, the role of international law in cyberspace is increasing, becoming more prominent, becoming more important. At the same time, note that international law has no specific rules for regulating cyberspace. Moreover, the technology is both new and dynamic. Thus, for several years there have been open questions as to whether existing international law applies at all to cyberspace. Cyberspace is now the backbone of global commerce, communication and defense systems, and is a key aspect of the critical infrastructure that sustains our modern civilization. Technology and information spread almost instantaneously, and the global economy and supply chains are integrated to a degree unprecedented in history.

Nevertheless, there is still no developed universal concept of cyberspace in international law, only approaches at the level of the UN, international organizations, including the First Committee of the UN General Assembly on Disarmament and International Security, the G20, the European Union, the Association of Southeast Asian Nations and the Organization of American States and doctrinal approaches are singled out.

Conclusions. The competition for strategic technology and the competition for advantage in the "information space" is growing, so far without the standard international rules of the road. Moreover, the future is likely to prove even more transformational. The potential threats are also extraordinary: autonomous weapons, cyber warfare, sophisticated disinformation campaigns and geopolitical instability. In such circumstances, it is crucial to develop a universal notion of cyberspace because of the persistent significant vulnerabilities and number of threats in global communications.

1. Introduction

Cyberspace is widely recognized as a fundamental fact of everyday life in the contemporary world. Until recently, it was believed that its political influence was linked to low political background conditions, routine processes, and decisions. However, now experts have begun to realize its impact on international policy, national security, major institutions, and processes of decision-making[1], the Latin expression «Hic sunt leones» («Lions live here») can be used[2], which referred to undiscovered land. Cyberspace can be attributed to a «land», which was actually «discovered» in the 20th century, but there are still discussions about the international legal regime that operates in it.

Considering the need to introduce a conceptual framework, it should be, however, borne in mind that there was no single definition of cyberspace. Carl Sagan (Carl Sagan) once said that modern society depends on science and technology, but hardly anyone has an idea of these two concepts.

It is generally believed that the term «cyberspace» first appeared in fiction, in the work of William Gibson («Neuromant» in 1984: «Cyberspace. Collective hallucination... graphic representation of data extracted from the memory banks of any computer in the human system... The light lines that contoured the apparent space of mind...». Since cyberspace has its own distinctive features, such as its virtuality, the idea of cyberspace at an early stage could only have formed in the literature.

Later, in the 1990s, there was t.n. «World Wide Web» (World Wide Web. WWW)[3], founded by Tim Berners-Lee (Tim Berners-Lee). Let us not dwell on the history of the «Internet» network, in detail the genesis of information and communication technologies, including the «Internet» network, is described in the first chapter of the first volume of «International information security: theory and practice»[4]. It can only be noted that the pioneer in this field is the US. By 1995 only 1% of the Earth's population had access to the «Internet»[5], by 2005, the figure exceeded 1 billion users worldwide, in 2010, two billion users, and in 2014, the figure reached a critical level of three billion people[6].

Cyberspace is a fundamentally new space that cannot be left unregulated by law, but in the enforcement process, legislators need to consider the debate about the applicability of the notion of state sovereignty therein, the absence of a universal international treaty that regulates the conduct of states in cyberspace, as well as a unified judicial system[7].

The development of the use of technologies in the modern world, led to a need to «demisthesize» cyberspace and to develop norms aimed at regulating its legal regime.

In order to define cyberspace in international law, it is necessary to consider the general definition of the term, as described above, in fiction. Cyberspace consists of two words: «cyber» related to electronic and computer information technologies, and «space» to the actual territory created by electronic technology to receive information through interconnected systems and related infrastructure. Cyberspace is a unique mode of physical and virtual objects, hardware (hardware) and software services (software), i.e. all computer networks in the world, including the «Internet» network and other networks, isolated or not connected to the «Internet». Cyberspace is much broader than the concept of the «Internet» network and therefore it is not limited to the use of «Internet».

Jacqueline Lipton [8] outlined the main features of cyberspace:

ISSN 2542-1514 (Print)

- global distribution of the «Internet» network;

- distinctive rules governing online behaviour as opposed to norms regulating behavior in the ordinary, «physical» world;

- the types of damage as a result of unfair conduct in an online environment.

In science, there are points of view, according to which it makes no sense to regulate cyberspace and consider the application of any norms in it, because this process is more like studying «the law of the horse» («Law of the horse»), since separate and unrelated rules are used, which cannot be harmonized for study[9].

Lawrence Lessig, by contrast, believes that cyberspace can protect all the basic values of humanity. Moreover, the law of cyberspace includes not only laws, precedents, statutes, but also all construction of the «Internet» network, non-binding norms, various standards applicable in this field[10].

There are twenty-eight definitions of the term «cyberspace» in international law due to the constant development of technology[1].

Professors Heike Krieger and George Nolte[11] note that the regulation of cyberspace in international law may pose certain challenges to the well-established international legal order.

There have already been similar problems in international law relating to the regulation of airspace and outer space. The main difficulty was the delimitation of these spaces, the elaboration of universal international treaties to regulate the conduct of states in airspace and outer space[12].

Is such a comparison applicable in the context of cyberspace? It is not possible to provide an unambiguous answer to this question.

François Delerue in his study[12] on the applicability of international law in cyberspace highlights the main points of discussion that should be considered when attempting to regulate this «territory» by international law:

- the term «cyberspace» first appeared in fiction, this concept was not developed by engineers or technicians;

- the question of considering the term as a territory where military action may take place remains unclear these days;

- given the lack of state sovereignty in cyberspace, the applicability of the concept of the common heritage of mankind remains a contentious issue.

We refute the thesis about cyberspace as the fifth dimension along with Earth space, water, air and space. Unlike the four existing spaces in international law, cyberspace has no territory in the classical view of the science of international law. On the contrary, all four existing spaces are already linked in one way or another to the use of virtual technologies, depending on them, for example, Earth Remote Sensing in space law. Any limitation of cyberspace is conditional and includes environment consisting of «Internet» network and other computers and telecommunication networks connected to «Internet» network or not. The «Internet» network is only one of many computer networks. Regarding the question of the applicability of international law to cyberspace, the answer would be positive, but in the twenty-first century, the major question for international law is not simply the applicability of existing international law, but

[1] Cyberspace as a Strategic Tool of Social Engineering. Report of the Center for System Initiatives expert M.V. Miguleva at the 5th International Scientific Conference «China and Russia: State Development Strategies», 28.05.2018, St. Petersburg. URL:https://center-si.com/analitics/m-v-migulyova-kiberprostranstvo-kak-strategicheskij-instrument-socialnoj-inzhenerii/ (Date views 17.02.2022).

ISSN 2658-4050 (Online)

the answer to another, highly controversial question of how to apply these norms.

The talk is about aspects that need to be explored to understand the nature of cyberspace, including the meaning of the term in international law that has already been considered; the question of sovereignty and its applicability; and sources of regulation; current problems and current regulatory trend.

2. Sovereignty in Cyberspace: Discussion Aspects

As was mentioned earlier, cyberspace cannot be equated with «Internet». «Cyberterritory» is transnational in nature, does not have a single control center and can be controlled only in certain areas[13]. No delimitation or demarcation acts are to be mentioned. The question of the sovereignty of states in cyberspace is a contentious one. Let us recall that the signs of the sovereignty of the state are: the supremacy of the state within its territory and autonomy in international relations. Element of sovereignty, territorial supremacy, i.e. extension of the supremacy of the state throughout the territory of the state[14]. Namely the particular territorial supremacy will be discussed. Cyberspace cannot be considered separately from the sovereignty of a state, as any critical information infrastructure located within a state could potentially pose a threat to other states, in case of interference with the operation of these facilities in the territory of other states. The establishment of sovereignty in this space could call into question the classical concept of state sovereignty, since it would involve the power of a state to control space beyond state borders[15].

In science of international law has been a long debated over the limitation of state sovereignty in cyberspace. Liberal scholars opposed any regulation by states and defended the right of the cyber system to domestic regulation. In their opinion, cyberspace is a classic example of «terra nullius» («no man's land»[2]) where application of state regulation is impossible. If the development of this idea is continued, it can be assumed that we will talk about some «superterritorial» space, but there are no rules in classical international law that could regulate it.

According to Pallavi Khanna, no state has recognized the «independent» sovereignty of cyberspace in an explicit form, which gives reason to consider the secondary, dependent nature of cyberspace from the primary, basic state sovereignty. The lack of territoriality of such space allows states to partially endow it with territoriality through the introduction of control mechanisms to ensure the security of information flows across states' borders. The article by Pallavi Khanna gives an example of a case involving Yahoo![3], which rejected the request from France to stop auctioning off the attributes of nazism, referring to free regulation of the «Internet» network. Later, a French court was able to prove that the american company did not conduct the auction in a legal vacuum, but spread advertising in France, where such actions to justify Nazism are prohibited by criminal law.

This example is essential for

[2] Applicability of International Law on Cyber Espionage Intrusions. Ella Shoshan thesis, Faculty of law Stockholm University, Stockholm, 2014. URL: www.diva-portal.org/smash/get/diva2:799485/FullTeXT01 (Date views 17.02.2022).

[3] LICRA v. Yahoo! (Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France), decided by the High Court of Paris (Tribunal de grande instance) in 2000. Also see Jon Henley, Yahoo! Cleared in Nazi Case. The Guardian, 12.02.2003. URL: www.theguardian.com/technology/2003/feb/12/newmedia.media (Date views 17.02.2022).

ISSN 2542-1514 (Print)

understanding the regulation of companies and states in cyberspace[16]. Of course, the application of the concept of classical territorial supremacy in this space is not expected, but the state acts in cyberspace through servers, its own infrastructure, located under the jurisdiction of the state, therefore, it will be held responsible for illegal acts.

Regarding the sovereignty of the state, the need to respect it was affirmed in the case of Nicaragua against the USA[17]. Based on this decision, it was recognized that all hostile cyber operations against cyberinfrastructure located in the territory of another state, implies a violation of the sovereignty of the affected state even if such operations do not entail harm or damage, since any hostile action is tantamount to unlawful interference through the exercise of supremacy over the territory of the affected state.

Realizing the danger of unlimited cyberspace and its removal from state control, some states have put forward an initiative to regulate the national segment of the network «Internet»[4]. Thus, China, North Korea advocate the complete isolation of the national segment of the network «Internet». The latter allows access only to the isolated national segment of the «Internet» network («Kwangmyeong»[5]). Despite attempts by a group of hackers in 2013 to connect the North Korean segment to the global network, it was not possible to do so because these draconian laws are often justified by the need to protect state sovereignty from cyberattacks by western states[6]. Now there is a realistic concept of sovereignty that allows states to exercise their jurisdiction on the basis of the principle of territoriality (i.e. the state has the right to regulate the transfer of information, along with the right to regulate the use of information by persons in cyberspace within the borders of the state). The sovereign has the right to control the hardware and software in its territory. Another principle of cyberspace regulation is the so-called «effects doctrine», which takes into account the consequences of unlawful acts that may have been committed in the territory of another state but caused injury to the former state. The US[7] National Cyber Security Strategy lists those actions that can be attributed to the violation of state sovereignty: attacks on network equipment, the use of such equipment and other hostile actions committed in cyberspace, which can threaten the peace and stability, civil liberties and the protection of privacy.

There is no prohibition under international law for a state to regulate its segment of cyber-infrastructure, but this right can only be realized if states comply with the principles of international law.

3. Sources of regulation of state behaviour in cyberspace

It should be noted that the lack of a universal convention to regulate the actions of

[4] 1680 VI. CYBERSPACE REGULATION AND THE DISCOURSE OF STATE SOVEREIGNTY. Harvard Law Review, 1999. URL: https://cyber.harvard.edu/property00/jurisdiction/hlr.html (Date views 17.02.2022).

[5] Kwangmyeong is the national intranet in North Korea. It was created in 2000 at the initiative of the Government of the DPRK and is one of the largest isolated from the «Internet». It has 1 to 5,500 sites.

[6] OpNorthKorea Text Release. Pastebin, 2013. URL: https://pastebin.com/ULEyQma4 (Date views 17.02.2022).

[7] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Executive Office of the President of the United States, 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Date views 17.02.2022).

states in cyberspace is considered to be the main problem to date. The main regulatory area of cyberspace is cybersecurity[18]. According to terminology compiled by the International Telecommunication Union (ITU), cybersecurity includes various means[8] aimed at protecting cyberspace as a «cyber environment», protecting the organization of its work, and protecting the persons included in it. According to Professor Joseph Nye[19], the issue of cybersecurity should be divided into four basic threats: espionage, crime, cyberwarfare, cyberterrorism. The reasons for these threats may be the shortcomings in the system of the «Internet» network, hardware and software, and the attempts of states and companies to move many objects of critical infrastructure into the sphere of online[20]. Let us consider only some of the sources aimed at regulating cybersecurity.

To describe the sources of international law governing cyberspace, it is necessary to give examples of three approaches to the regulation of this space in international law: «cyberinstitutionalist», «cyberlibertarian» and the approach of «state officials». Cyberinstitutionalists (Tim Wu[21]) advocate the institutionalization and adoption of international legal norms that would regulate cyber environment. Cyberlibertarians (John Barlow[9]), by contrast, refuse to apply any norms in cyberspace, referring to freedom in the «Internet». «Sovereigns» (James Lewis[22]) are confident that in this situation, only states, as primary subjects of international law, could make efforts to create the necessary universal norms to regulate cyberspace[23].

The Statute of the International Court of Justice (article 38) lists the sources of international law[10]:

a) International conventions, both general and special, establishing rules expressly recognized by the disputing states;

b) International custom as evidence of a general practice recognized as law...

There are currently no universal international conventions aimed at regulating the conduct of states in cyberspace. States cannot agree on the possibility of limiting sovereignty, the creation of a universal judicial body empowered to deal with cases in cyberspace, etc. The question of the emergence of new actors, including the Russian Federation, remains important who act in cyberspace on their own behalf and dictate the rules of the game in this area[24]. Next, briefly consider the contradictions of states and new initiatives to regulate cybersecurity, including from global giants in the cyber industry such as Microsoft[11].

To begin with, I propose to address the discussion on the applicability of customary international law in cyberspace. Had there been any customary international law that could be accepted by all states?

Gary Brown and Keira Polet in their article «Customary International Law in Cyberspace»[25] analyzed the applicability of international custom in the «fifth dimension». When discussing the applicability of custom, one should keep in mind the two essential

[8] UN ITU-T Recommendation X.1205 (04/08): Overview of cybersecurity. The International Telecommunication Union, 2008. URL: www.itu.int/rec/T-REC-X.1205-200804-I (Date views 17.02.2022).

[9] A Declaration of the Independence of Cyberspace. J.P. Barlow, Electronic Frontier Foundation, 1996. URL: www.eff.org/cyberspace-independence (Date views 17.02.2022).

[10] Statute of the International Court of Justice. The United Nations, 1945. URL: www.icj-cij.org/en/statute (Date views 17.02.2022).

[11] 'Digital Peace Now' launches this weekend. Kate O'Sullivan, Microsoft, 2018. URL: https://blogs.microsoft.com/on-the-issues/2018/09/28/digital-peace-now-launches-this-weekend/ (Date views 17.02.2022).

ISSN 2542-1514 (Print)

elements of custom, «objective» («general practice») and subjective («recognition of it as a right»). According to them, the first cyber-attack took place in the Soviet Union in 1982[26] when an explosion occurred on the Trans-Siberian Railway gas pipeline. It was reported that the explosion was due to the launch of a malware program and was the result of a special CIA operation. Later, cyber attacks began to appear in the US, examples being Moonlight Maze (1998-2001), Code Red (2001), Mountain View (2001). In 2010, Google reported on Chinese hackers attempting to steal the company's intellectual property. Hackers installed malware and hacked the data of the owners of Google Mail accounts, which defended human rights[27]. As a result, Google was forced to limit the conduct of business in this state. However, in this context, we are not talking about the emergence of an international legal custom, because for its emergence it is necessary to have an actor who performs these actions, for the appearance of «opinion juris» as, for example, in the case of the first satellite launch in the USSR and in the future, the emergence of the principle of non-appropriation of outer space.

Espionage could be seen as an example of the emergence of a customary rule of international law in cyberspace, but here again it is difficult to apply custom as understood in article 38 of the Statute. There is no customary international law against espionage in peacetime. States may have laws at the national level prohibiting such actions. One example is the United States, where espionage is punishable by death[12]. As a general rule, espionage is not prohibited by international law. Speaking about actions in cyberspace, it is necessary to attribute them by their nature not to military actions, but to espionage, because the malware is introduced into the systems of state bodies and actually «collect and accumulate» accumulated information. Just like classic espionage in international law, cyberespionage is subject to a permissive regime in which states themselves, on the basis of international law, decide on the legality of an action. On the one hand, cyberattacks and other unlawful actions may, like an armed attack on the territory of another state,[28] lead to specific physical consequences (explosion, damage, disablement). On the other hand, assuming that such actions are related to combat, what to do if the program temporarily disables the power grid? There was no fighting in this example, but the network was temporarily shut down. In such a case, the attack is of a "near-combat" type and also falls under the definition of an armed attack[29]. In order to regulate customary international law, it is necessary to form the position of states on the consideration of these cases either on the basis of the notion of "espionage" (authorization regime) or on the basis of the concept of "armed attack" (prohibition regime in international law).

In 2011, the U.S.[13] developed the United States National Security Strategy, which attempted to influence the development of conventional norms in cyberspace. The paper emphasized that the creation of such rules did not require a review of customary international law, international law as a whole. All existing international legal norms will apply both in peacetime and in wartime. Of course, the rules

[12] 18 U.S.C pt.1, chap. 37 "Espionage and Cencorship", para. 793-98. The United States Code. URL: www.law.cornell.edu/uscode/text/18/part-I/chapter-37 (Date views 17.02.2022).

[13] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Executive Office of the President of the United States, 2011. URL:https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Date views 17.02.2022).

contained in the document could not be considered customary rules of international law, but they could create the conditions for state cooperation in view of the reluctance to accept primary sources of international law and universal international treaties. It seems an overly short-sighted approach to considering cyberespionage on the basis of a permissive order, which could lead to massive cyberattacks in the future.

An important step towards addressing the issue of cybersecurity and the regulation of state behaviour in cyberspace would be the adoption of a convention that includes basic definitions and norms. To date, the only instrument regulating cybercrime is the 2001[14] Budapest Convention, but it has been adopted in the Council of Europe and has a regional character, although non-European states are also parties to the Convention.

Both European and non-European states must make efforts to adapt existing international law to cyberspace to some extent, but in practice this requirement is unlikely to materialize any time soon. So, in 2013 and 2015 the Group of Governmental Experts prepared reports which recognized and confirmed the application of the provisions of international law and, in particular, of the 1945 UN Charter to cyberspace[15]. In 2017, the GGE discussed the possibility of applying all branches of international law in cyber-territory, for instance, the possibility of applying all norms of international humanitarian law in cyberspace[16], the possibility of using countermeasures, the right to self-defence. Three states: China, Cuba and the Russian Federation, have consistently advocated the need not to apply the above-mentioned regimes, but to respect all other branches of international law. Russia's position is explained by the fact that the lack of special rules for the regulation of cyberspace can serve as a trigger mechanism for launching an arms race in the «fifth dimension». A.V. Krutskikh [17]declares that the militarization of cyberspace is inadmissible, the use of force is prohibited, and respect for state sovereignty, human rights and freedoms is respected. In his view, the main features of cyberspace and the resulting problem of identifying the source of the cyber attack are not taken into account. For the United States[18] and the United Kingdom[19], on

[14] Convention on Cybercrime. Council of Europe, 2001. URL https://rm.coe.int/1680081561 (Date views 17.02.2022).

[15] UN Doc A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly of the United Nations, 2013. URL: https://undocs.org/A/68/98 (Date views 17.02.2022).

UN Doc A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly of the United Nations, 2015. URL:, https://undocs.org/en/A/70/174 (Date views 17.02.2022).

[16] UN GGE on Cybersecurity: The End of an Era? E. Korzak, The Diplomat, 2017. URL: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (Date views 17.02.2022).

[17] Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere. A. Krutskikh, The Ministry of Foreign Affairs of the Russian Federation, 2017. URL: https://archive.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/%20content/id/2804288 (Date views 17.02.2022).

[18] Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental

ISSN 2542-1514 (Print)

the contrary, while the question of the application of general law is clear, according to the position of these states, there is no need to develop new norms of international law to regulate cyberspace and thus to call into question the existing international legal order, which in the future will lead to inevitable revision of the entire framework of existing international legal norms. On the other hand, if no special rules were adopted, it would not be possible to reach consensus on the positions of states, while the level of uncertainty would increase and development of the presumably new industry of international law would be halted. Differences in terminology at the national level also remain relevant. So, if for most states it is about the regulation of cybersecurity ("cybersecurity")[30], where the emphasis is on security in understanding the science of international law, for Russia and China the focus is on "information security within the state" ("information security") and on the protection of state sovereignty[31].

4. Current problems and current regulatory trends

Being aware of the complexity of a unified view on many issues, states are moving towards regional cooperation. The United Nations, the EU, the CIS, ASEAN, the OAS are developing numerous norms to regulate cybersecurity and many other aspects of cooperation,[32] but the increased production of norms cannot lead to uniform application in international law.

In cyberspace the main subjects are considered not only the state, but also companies: Google, Facebook, Microsoft, etc. In 2018, Microsoft launched the «Digital Peace Now»[20] initiative to adopt the digital Geneva Convention or the so-called «Geneva Convention 5.0», which would protect the rights of citizens from cyberattacks in peacetime with the help of specialized companies, that is, a «jus contra bellum» was used, aimed at preventing an active response from states[12].

It is obvious that cyberspace cannot remain a «law-free zone» («law-free zone»), so Harold Honnju Koh proposes to use the US approach to this problem caused by a lack of regulatory sources. The US position is that all the principles of international law are applicable in cyberspace, i.e. cyber-attack may fall under Article 2, paragraph 4, of the UN Charter and the actions themselves should be qualified as use of force if the following conditions are met: the existence of an appropriate context, subject, actions, objectives, location, consequences, intent. In his view, self-protection measures for affected states can and should be applied in the cyberenvironment, and it is also necessary to use «jus in bello» on the basis of necessity and proportionality. States would be required to review the conventional weapons and to include new types of cyberweapons.

Attribution to the state must be addressed in order to qualify the act, but the

Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. United States Mission to the United Nations, 23.06.2017. URL: https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/ (Date views 17.02.2022).

[19] Cyber and International Law in the 21st Century. J. Wright, speech of the UK Attorney General, 23.05.2018. www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (Date views 17.02.2022).

[20] Digital Peace Now. Global movement of digital citizens from over 170 countries, launched by Microsoft in 2018. URL: https://digitalpeacenow.org/ (Date views 17.02.2022).

ISSN 2658-4050 (Online)

issue is practically impossible to resolve in practice because cyber weapons can be acquired not only by states but also by non-objects of international law. An attempt to equate states with different levels of technological capabilities in cyberspace is also unlikely to succeed. Thus, there may be fragmentation of international law: functional (different rules and regimes governing the conduct of states in cyberspace) and geographical (an increase in regional treaties and agreements) that do not facilitate the harmonization of states' positions.

Various initiatives, centres and non-governmental organizations are also involved in the process of stabilizing the international legal order in the cyber environment. Thus, the Global Commission on the Stability of Cyberspace, consisting of 26 eminent persons specializing in cyberspace[21], plays an important role.

Within the framework of such a specialized agency of the United Nations as ITU, definitions of basic terms, initiatives in the field of cyberlaw are being developed. Thus, in 2014, an initiative was launched to introduce the Global Cybersecurity Index to track its level in the world[22]. In 2020, Russia took the fifth place in this ranking and the USA took the first[23].

The last point I would like to make is the current trends in the regulation of cyberspace in international law. A report on the applicability of international law in cyberspace[24] was prepared by the United Nations Group of Governmental Experts on 28 May 2021. The United Nations Office on Drugs and Crime was established on 28 May 2002. It is noteworthy that, for the first time since 2017, the parties have managed to reach consensus on the many issues on the agenda. Individual states: Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan and China proposed the adoption of an International Code of Conduct on Information Security. The confirmation of the industry's application to cyberspace during armed conflict was a critical step towards addressing the current challenges in the application of international humanitarian law. The application of all fundamental principles of international law was reaffirmed. States in this situation are required to cooperate and share practices to resolve cyber disputes, as described above.

However, even with these advances, it remains unclear when States will be able to develop a convention that would regulate cyberspace in accordance with existing norms. It would be possible to assume that in time the issue will be solved in one way or another, as in the case of outer space, in the exploration of which Russia and the United States participated, however it is not the states that play an important role and dictate rules of conduct in cyberspace, but private companies, including

[21] About – Global Commission on the Stability of Cyberspace (GCSC). Global Commission on the Stability of Cyberspace. URL: https://cyberstability.org/about/ (Date views 17.02.2022).

[22] Global Cybersecurity Index 2020. International Telecommunication Union, 2021. URL: www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (Date views 17.02.2022).

[23] Global Cybersecurity Index 2020 REPORT. International Telecommunication Union, 2021. URL: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (Date views 17.02.2022).

[24] Letter of transmittal of the report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. Chair of the Group Guilherme de Aguiar Patriota, 28.05.2021. URL: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf (Date views 17.02.2022).

ISSN 2542-1514 (Print)

individuals, corporations, which in turn cannot be considered subjects of international law. Furthermore, the anonymity of cyber behaviour and the resulting problem of attribution remain unresolved. At the international level (UN), there is no progress in the process of solving the problems, many norms are «soft law» rather than «hard law», which leads to duplication of norms and uncoordinated practice of the conduct of states.

Michael P. Fischerkeller[25] offers a seemingly ambiguous solution. He suggested that the approach to non-interference in the use of coercion in favour of the exploitation (use of information) of cyberspace should be reconsidered. Not all coercive measures in international law can be considered unlawful, nor can all exploitative measures be considered illegal. The principle of exploitation will allow states to list those actions that will be considered as interference in the «national sector» of cyberspace (for example, a state, as the US has done, may attribute exploitation of intellectual property to a wrongful act). Exploitation is classically defined as an illegal act committed in cyberspace for the purpose of obtaining information, but the author disagrees with such a narrow and one-sided notion of exploitation. Instead, it would be appropriate to view the term as one state's use of technology to benefit from the imperfections of another state's cyberspace in order to gain a competitive advantage.

Such measures would not change existing gaps in universal cyber-regulation in international law. One step towards international law-making could be: an international summit with the participation of states, international organizations and representatives of companies to agree on a draft future convention; review of the existing soft law framework with a view to identifying uniform rules; move away from information security to cyber security; initiate work by the UN International Law Commission to present a draft convention.

[25] Current International Law Is Not an Adequate Regime for Cyberspace. M.P. Fischerkeller, Lawfare, 22.04.2021. URL: www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace (Date views 17.02.2022).

REFERENCES

1. Choucri N. *Cyberpolitics in International Relations*. The MIT Press, 2012. 320 p. DOI: 10.7551/mitpress/7736.001.0001.

2. Roscini M. World Wide Warfare – Jus ad bellum and the Use of Cyber Force, in: Bogdandy A. Von, Wolfrum R., Philipp C.E. (eds.). *Max Planck Yearbook of United Nations Law*. Leiden, Martinus Nijhoff Publ., 2010, vol. 14, pp. 85–130.

3. Kahin B., Keller J.H. *Coordinating the Internet*. The MIT Press, 1997. 510 p. DOI: 10.7551/mitpress/2170.001.0001.

4. Krutskikh A.V. *International information security: theory and practice*, in 3 volumes, 2nd ed. Moscow, Aspekt Press Publ., 2021. Vol. 1. 384 p. (In Russ.).

5. Ceruzzi P.E. *Computing: A Concise History*. The MIT Press, 2012. 199 p. DOI: 10.7551/mitpress/9426.001.0001.

6. Srinivasan R. *Beyond the Valley: How Innovators around the World are Overcoming Inequality and Creating the Technologies of Tomorrow*. The MIT Press, 2019. 424 p. DOI: 10.7551/mitpress/11894.001.0001.

7. Biegler S. *Beyond Our Control?: Confronting the Limits of Our Legal System in the Age of Cyberspace*. The MIT Press, 2003. 472 p. DOI: 10.7551/mitpress/1583.001.0001.

8. Lipton J. *Rethinking Cyberlaw: A New Vision for Internet Law*. Edward Elgar Publishing LTD, 2015. 176 p.

9. Frank H.E. Cyberspace and the Law of the Horse, in: *University of Chicago Legal Forum*, 1996, pp. 207–216

10. Lessig L. *Code and Other Laws of Cyberspace*. New York, Basic Books Publ., 1999. 320 p.

11. Krieger H., Nolte G., Zimmermann A. *The International Rule of Law: Rise or Decline?* Oxford, Oxford University Press, 2019. 378 p. DOI: 10.1093/oso/9780198843603.001.0001.

12. Delerue F. *Cyber Operations and International Law*. Cambridge, Cambridge University Press, 2020. 549 p. DOI: 10.1017/9781108780605.

13. Khanna P. State Sovereignty and Self-Defence in Cyberspace. *BRICS Law Journal*, 2018, vol. 5, no 4, pp. 139–154. DOI: 10.21684/2412-2343-2018-5-4-139-154.

14. Vylegzhanin A.N. (ed.). *International law*, Textbook for universities, in 2 parts. Moscow, Yurait Publ., 2021. Pt. 1. 329 p. (In Russ.).

15. Kahin B., Nesson C. *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*. The MIT Press, 1997. 374 p. DOI: 10.7551/mitpress/1648.001.0001.

16. Jørgensen R.F. *Human Rights in the Age of Platforms*. The MIT Press, 2019. 392 p. DOI: 10.7551/mitpress/11304.001.0001.

17. Schmitt M.N. The Law of Cyber Warfare: Quo Vadis? *Stanford Law & Policy Review*, 2014, Vol. 25, iss. 2, pp. 269–299.

18. Wolff J. *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. The MIT Press, 2018. 336 p. DOI: 10.7551/mitpress/11336.001.0001.

19. Nye J.S. *Cyber Power.* Belfer Center for Science and International Affairs, Harvard Kennedy School, May, 2010. 24 p.

20. Coleman S., Shane P.M. *Connecting Democracy: Online Consultation and the Flow of Political Communication*. The MIT Press, 2011. 416 p. DOI: 10.7551/mitpress/9006.001.0001.

21. Wu T.S. Cyberspace Sovereignty? The Internet and the International System. *Harvard Journal of Law & Technology*, 1997, vol. 10, no. 3, pp. 647–666.

22. Lewis J. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*, 2010, vol. 16, iss. 2, pp. 55–65.

23. Adonis A.A. International Law on Cyber Security in the Age of Digital Sovereignty. *E-International Relations*, Mar 14 2020, available at: https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/.

24. Rheingold H. *The Virtual Community: Homesteading on the Electronic Frontier*. The MIT Press, 2000. 447 p. DOI: 10.7551/mitpress/7105.001.0001.

25. Brown G., Poellet K. The Customary International Law of Cyberspace. *Strategic Studies Quarterly*, 2012, vol. 6, iss. 3, pp. 126–145.

26. Barassi V. *Child Data Citizen: How Tech Companies Are Profiling Us from Before Birth*. The MIT Press, 2020.

ISSN 2542-1514 (Print)

232 p. DOI: 10.7551/mitpress/12415.001.0001.

27. Webb M. *Coding Democracy: How Hackers Are Disrupting Power, Surveillance, and Authoritarianism*. The MIT Press, 2020. 416 p. DOI: 10.7551/mitpress/11669.001.0001.

28. Schmitt M.N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 1999. 1998–1999, vol. 3, pp. 885–937.

29. Landau S. *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. The MIT Press, 2011. 383 p. DOI: 10.7551/mitpress/8623.001.0001.

30. Henriksen A. The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, 2019, vol. 5, iss. 1, pp. 1–9. DOI: 10.1093/cybsec/tyy009.

31. Jemielniak D., Przegalinska A. *Collaborative Society*. The MIT Press, 2020. 256 p. DOI: 10.7551/mitpress/11587.001.0001.

32. Koh H. H. International Law in Cyberspace. *Harvard International Law Journal Online*, 2012, vol. 54, pp. 1–12, available at: https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf (accessed date: 22.11.2022).

INFORMATION ABOUT AUTHORS

Ksenia A. Ivanova – PhD in Law; [1] Director, Center of Local Authorities of the Institute of Management and Regional Development; [2] Associate Professor, Department of Constitutional and Municipal Law
[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA)*
[2] *University of Tyumen*
[1] 84, Vernadskogo pr., Moscow, 119571, Russia
[2] 6, Volodarskogo ul., Tyumen, 625003, Russia E-mail: ivanova-ka@ranepa.ru
RSCI SPIN-code: 6610-9218; AuthorID: 695216

Madi Zh. Myltykbaev – Post-graduate student, International Law Department
MGIMO University
76, Vernadskogo pr., Moscow, 119454, Russia E-mail: myltykbaev@my.mgimo.ru
ORCID: 0000-0003-3261-9927
ResearcherID: AAA-3864-2019
RSCI SPIN-code: 6952-1510; AuthorID: 1028441

Daria D. Shtodina – Post-graduate student, International Law Department
MGIMO University
76, Vernadskogo pr., Moscow, 119454, Russia E-mail: dashashtodina96@gmail.com
ORCID: 0000-0003-4730-9614
ResearcherID: AAE-5310-2022
RSCI SPIN-code: 3795-6159; AuthorID: 1136990

BIBLIOGRAPHIC DESCRIPTION

Ivanova K.A., Myltykbaev M.Zh., Shtodina D.D. The concept of cyberspace in international law. *Pravoprimenenie = Law Enforcement Review*, 2022, vol. 6, no. 4, pp. 32–44. DOI: 10.52468/2542-1514.2022.6(4).32-44. (In Russ.).

ISSN 2658-4050 (Online)