The Issue of State Sovereignty in Cyberspace

Luidmila Terentieva

Associate professor, International Private Law Chair, Kutafin Moscow State Law University. Address: 9 Sadovaya-Kudrinskaya Str., Moscow 123242, Russian Federation. E-mail: terentevamila@mail.ru

Abstract

The author examines a special approach to establishing the sovereignty of the state in relation to cyberspace, the extraterritorial characteristics of which determine the question of the implementation of the territorial supremacy of the state. The author concludes that the understanding of the state's sovereignty in relation to cyberspace lies not in detailing a set of measures in the form of sovereign powers undertaken in this area, but in constructing the boundaries of cyberspace both in relation to the technical component of the network infrastructure that supports the smooth functioning of the Network, and in in relation to the virtual component of cyberspace. To achieve the goal of the study, the author proposed to combine social, technological and subjective approaches, understanding by cyberspace an artificial telecommunication environment for the implementation of public relations controlled by a wide range of subjects (states, intergovernmental organizations, non-governmental organizations, individuals, etc.), the functioning and maintenance of which is carried out by means of software-technical infrastructure in the form of its physical part (telecommunication networks, computers, servers, routers, processors, satellites, etc.) and a virtual part (operating systems, data transmission standards, hardware applications, software, etc.).

Keywords

cyberspace, sovereignty, Internet, software, digital rights, information.

Acknowledgements: The article was prepared thanks to the financial support of the Russian Foundation for Basic Research (RFFI) as a part of the RFFI's project "Internet Law: from a Concept to a Methodology of Regulating Trans-Border Relations" — project No. 18-29-16061; the funding was awarded based on the results of a competitive review of proposals for projects of interdisciplinary basic research (the competition's code is 26-816: "Transformation of Law in an Age of the Development of Digital Technologies").

For citation: Terentieva L.V. (2021) The Issue of State Sovereignty in Cyberspace. *Legal Issues in the Digital Age,* no 2, pp. 49–67.

DOI: 10.17323/2713-2749.2021.2.49.67

Introduction

The rise of a large-scale extraterritorial multi-site space of information and communication has not only positive aspects, such as interactive communication and the infusion of the principles of transparency and openness into the workings of the traditional societal and governmental institutions; it also carries certain risks — for instance, potentially threatening state sovereignty, which is based on such traditional characteristics as power and territory.

Because the vital qualities of the state, as well as the principles of international law, are deeply entrenched in the traditional concepts of territorial geography, the academe has had to address the following questions: is the system rooted in the 1648 Peace of Westphalia sufficiently well equipped to respond to modern challenges of a network society [Bethlehem D., 2014: 9–24].

The development of digital technologies gave rise to the theory of "digital libertarianism," which counterposes sovereignty of cyberspace to state sovereignty [Tulikov A.V., 2016: 235–243]. The difficulties of objectifying cyberspace through physical parameters have given rise to the argument that geographic territoriality in international law is ineffective and borders between states have been weakened [Anselmo E., 2006: 24–31]; [Malakhov V.C., 2007: 218]; [Benyekhlef K., Gelinas F., 2001:7]; [Kobrin S., 1997: 65–77]; that the concept of territory has changed significantly and borders of states do not coincide with borders of regions over which these states exercise authority [Adams J., Albakajai M., 2016: 256–265]; [Matusitz J., 2014: 713–724]; [Streltsov A., 2017: 88–106]; that territorial sovereigns cannot control cyberspace, which should be governed by its own jurisdiction (or several jurisdictions) specially created for the purpose [Johnson D., Post D., 1996]; and that sovereignty is a fiction [Ivanov V., 2009]. Some researchers have also suggested creating a legal system based on self-regulation since sovereigns cannot exercise their authority over cyberspace, which has no borders [Samarin A.A., 2016:13].

As M.N. Marchenko noted, the argument that state sovereignty is "historically exhaustible" and "susceptible to erosion" not only contributes to undermining the centuries-old school of thinking on sovereignty and its role for society and the state but also erodes the entire methodological foundation of the process of acquiring knowledge about the state and law [Marchenko M.N., 2011: 92–93].

Arguably, any stage of society's technological development accompanied by an acceleration of the pace of globalization can present a convenient opportunity to raise the question of possible elimination of sovereignty and a weakening of the power of state institutions. But despite all the radical ideas about the forthcoming end of geography and state borders, the magnitude of development of economic, political, and social relations in cyberspace calls for a discussion about limits of states' legal powers with regard to these relations.

This problem was also broached in President Putin's decree of May 9, 2017, "On the Strategy of Development of Information Society in the Russian Federation for 2017–2030," in which it is noted in §17, that states have to adapt, practically "on the fly," state regulation in the area of information and information technologies in order to set in place international legal mechanisms that would protect states' sovereign right to regulate information space, including in national segments of the Internet[1].

Before proceeding to establish international legal mechanisms for regulating information space, the following question has to be addressed: is the present territorial concept of the state's sovereignty and jurisdiction is essentially exhausted in this space and do we need new approaches partly based on realities of cyberspace. And assessing the territorial principle of sovereignty and jurisdiction, we should look at a combination of extraterritorial information flows rather than at cyberspace's technological infrastructure, which, possessing certain physical parameters as it does, can be localized fairly easily,

There is a truth to the doctrinal argument that ensuring a state's sovereignty in information sphere and developing a global information society are two mutually exclusive objectives because it is difficult for the state to maintain control over its information policies when this state is strongly integrated into global information society [Abdrakhmanov D.V., 2016: 66–72]. This conflict of concepts, however, can not only produce the idea about a weakening of sovereignty in global information space — it can also give rise to a different approach, such as recognizing the need to take additional measures to strengthen the state's control over information space, as well as its information security.

It should be pointed out that as such, globalization, and information and communication flows, cannot affect sovereignty as an international legal

[1] Compendium of Laws of the Russian Federation [Sobranie zakonodatel'stva Rossiyskoy Federatsii]. 2017. No. 20. Article 2901.

principle. If we assume that they can, it would be tantamount to recognizing that sovereignty can be divided or abridged. If we recognize that the mentioned processes lead to an abridgment of sovereignty, it follows, then, that sovereignty consists of structural elements that can be taken away. State sovereignty, meanwhile, is a qualitative, static category: quantitative characteristics, such as size, volume, completeness or incompleteness, are not applicable to it.

Any abridgement of sovereignty as an international legal principle of sovereign equality of states, of supremacy and independence of a government inside the respective country and in relations with other governments can result in an erosion of the concept of sovereignty and put at risk the very existence of the state, because sovereignty can be transferred only in full (as when one state is incorporated into another as a unit of the federation), and not partially. So raising the question of restricting sovereignty when globalizing, integration and information processes are afoot appears inappropriate.

At the same time, taking into consideration the expansion of collective interests of governments and the entire international community at an age of globalization, scholars allow room for restricting the functions of sovereign states or delegating the state's rights inherent in the state's sovereignty as a primary subject of international law, but only when the concerned state voluntarily agrees to it for the purpose of achieving objectives of public importance [Galushko D.V., 2013: 366–374]; [Moiseyev A.A., 2007: 26].

Relying on the concept of transfer of sovereign rights, rather than of sovereignty itself, S.V.Chernichenko concludes that the principle of sovereign equality of states (including respect for state sovereignty) is not an obstacle to globalization [Chernichenko S.V., 2010: 25–31]. Besides, according to M.N.Marchenko, as states coexist and interact with each other working on global and local problems in today's realities, the social role and importance of state sovereignty, far from becoming weaker, only grows [Marchenko M.N., 2011:100].

The fact that states are bound by political, economic, social and other obligations both at home and internationally has an impact not on sovereignty as an international legal principle but on the realization of states' sovereign rights. The principle of sovereign equality of states meanwhile remains firmly in place.

In academic literature the concept of sovereignty is often represented as having different categories: economic, political, taxational, informational, etc. [Shakhmametiev A.A., 2013: 76–81]; [Khavanova I.A., 2013: 41–51];

[Izbulatov Kh.Kh., 2007: 139–141]; [Kirilenko V.P., Alexeyev G.V. 2016: 14–23]. As was noted by O.Ch.Reut, the application of these adjectives to sovereignty is not at odds with the concept of sovereignty and enables us to clarify one or another dimension of the concept [Reut O.Ch., 2007: 115–124]. At the same time, some thinkers suggest an inverse move — applying an indivisible concept of state sovereignty to one or another sphere [Bachilo I.L., 2016: 76–88]; [Talapina E.V., 2018: 60–67]; [Chernichenko S.V., 2010: 25]. S.V.Chernichenko argues that dividing state sovereignty into separate elements is inexpedient because it is difficult to compile an approximate list of types of sovereignty and define each of them [Chernichenko S.V., 2010: 31].

As it appears, such notions as "political sovereignty," "economic sovereignty," "financial sovereignty" are rather abstract, meaning an autonomous, independent political course pursued by a state in one or another sphere. In each of the mentioned areas states are equally self-sustaining and independent.

A special approach can be applied to state's sovereignty in such specific sphere of information and communication space as cyberspace. As in the concepts of political, economic, financial sovereignty, the key here is the category of state sovereignty, denoting an immutable characteristic of the state's supremacy within its national borders and its independence in international affairs. The cardinal difference of sovereignty as applied to cyberspace, however, is the impossibility of reducing its borders to the state's physical borders, which raises the question of the principles of realization of the state's territorial supremacy in relation to this space.

In scholarship, the question of the workings of sovereignty in cyberspace is often raised by researchers of informational sovereignty. The concept of informational sovereignty originated yet before the birth of cyberspace; because of this, informational sovereignty in the scholarship is vested with a broader meaning — it stands for the state's supremacy and independence in shaping and carrying out its information policy, aimed at protecting the state's security in information space, information sphere, information segment [Yefremov A.A., 2017: 201–215]; [Kucheryavyi M. M., 2015: 11].

In some concepts of information sovereignty, spatial limits of sovereignty in information sphere are often represented as spatial limits of the state's supreme power over the respective national segment of telecommunications environment, first of all the Internet [Streltsov A., 2017: 88–106] or as virtual reality, which is cybernetic space [Polikarpov V.S., Polikarpova Ye.V., 2014: 279–284]. Such a view probably stems from equating cy-

berspace to information space and virtual space, an approach applied by some scholars [Vaganov P.A., 2006: 73–89].

In this case the spheres of sovereignty differ greatly in terms of volume, considering that cyberspace is just one of the elements — a significant one, but only one among other elements — of information space, which is quite wide and includes much more than cyberspace alone.

Some scholars also apply a more narrow approach, using it to conceptualize network sovereignty. Thus, some academics point to constitutive properties of network sovereignty such as the state's supreme power to shape and carry out a national policy aimed at controlling and regulating, within the state's territorial borders, operations of social network structures, as well as suppressing, within other nations' borders, activities of network structures aimed at undermining the state's constitutional basis and constitutional security [Sharifov M.S., 2009: 40–44].

This approach is vulnerable to criticism because it is not clear how social network structures can operate in the respective state. Do these researchers mean establishing sovereignty in relation to the network hardware that ensures a smooth functioning of these social network structures or in relation to information posted online on a site with one or another state's domain name?

What is also unclear is what exactly is meant by network structures: social networks, technological infrastructure or something else? It appears more appropriate, therefore, to talk not about sovereignty in relation to social network structures or the technological infrastructures supporting operations thereof but in relation to cyberspace, which includes all of the above-mentioned elements.

Non-Russian scholars argue that it is impossible to establish sovereignty in relation to cyberspace as such although it may be established in relation to an infrastructure situated within the state's territorial borders, as well as in relation to activities connected with this infrastructure, no matter whether it is publicly or privately owned [Schmitt M., 2013: 25].

Considering the territorial nature of state sovereignty and jurisdiction, it appears beyond doubt that a state can establish sovereignty in relation to cyberspace's technical component physically present on the respective state's territory.

Cyberspace, however, is not tantamount to an array of only material objects (computers, servers, routers, optical fiber cables, etc.), nor is it tantamount to a computerized network consisting of a multitude of com-

puterized subnetworks across the globe. In addition to the technological component, cyberspace includes a plethora of immaterial elements, such as information and software[2]. The main function of cyberspace is virtual: creating an interactive environment for a wide range of actors.

It appears more appropriate, therefore, to define sovereignty in cyberspace not only in relation to the technical component of the network infrastructure ensuring the network's smooth functioning but also in relation to the virtual component of cyberspace.

So, it is necessary to offer a definition of cyberspace in which technological and social approaches converge and to explore the relationship between the concepts of information space and cyberspace.

Definition of cyberspace

In Annex 1 to the Agreement on Cooperation in the Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization (Yekaterinburg, June 16, 2009) "'information space' means a field of activities related to the formation, generation, transformation, transmission, use, storage of information that [has] an impact, among other things[,] on individual and social consciousness, information infrastructure and information itself"[3].

Information infrastructure is defined in Annex I to the Agreement as "a range of technical tools and systems for formation, generation, transformation, transmission, use and storage of information"[4].

The definition of information resources in the Agreement is not very good either — the resources are conceptualized through information infrastructure as well as information as such and its flows, rather than as an autonomous concept[5].

Russian law has adopted a technological approach to conceptualizing information space, informed by the current state of information and communications technologies.

[2] At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. May 13, 2014. Pp. 8–9. Available at: https://www.nap.edu/read/18749/chapter/3. (accessed: January 12, 2021)

[3] Byulleten' mezhdunarodnykh dogovorov. 2012. No. 1.

[4] Ibid.

[5] Ibid.

Such technological approach is applied in the Russian Presidential decree of May 9, 2017 "On Strategy of Development of Information Society in the Russian Federation for 2017–2030" (hereinafter referred as to the 2017 Presidential decree) — in this document information space is conceptualized as a combination of information resources created by subjects of information sphere, tools by which the subjects interact, the subjects' information systems, and the requisite information infrastructure.

Scholars, too, often apply the technological approach to conceptualizing information space, which they define as a combination of information resources and infrastructural facilities comprising national and cross-border computerized networks, telecommunication systems and public use networks, data bases and data banks, other trans-border information transmission channels [Girich V.L., 2007]; [Kopylov V.A., 2002: 234]; [Prosvirnin Yu.G., 2000: 64].

It is easy to notice that the quoted definitions are somewhat circuitous, with one concept defined through another. Thus, the definition of information space contained in the Presidential decree of May 9, 2017, includes quite a lot of terms that are either authoritatively explained in other regulatory documents or have been doctrinally interpreted in the absence of a definition in law.

Thus, the concept of information system is entrenched in Federal Law 2 "On Information, Informational Technologies, and Protection of Information," adopted in 2006: according to the text of the law, an information system is the combination of information in data bases and information technologies, hardware and software employed to process it[6].

The concept of information resources was contained in §2 of the now repealed Federal Law 24 "On Information, Informatization and Protection of Information" (approved in 1995): the definition included individual documents and individual arrays of documents, as well as documents and arrays of documents in information systems (libraries, archives, funds, data banks, other information systems)[7].Academics categorize information resources as an element of information systems, conceptualizing these resources as a combination of documented information covered by special

[6] Federal Law No. 149-FZ July 27, 2006 On Information, Information Technologies, and Protection of Information // Compendium of Laws of the Russian Federation. 2006. No. 31 (part I). Article 3448.

[7] Federal Law No. 24-FZ February 20, 1995 On Information, Informatization, and Protection of Information // Compendium of Laws of the Russian Federation. 1995. No. 8. Article 609 (now repealed).

rules, as set out in law or other regulatory instruments, with respect to creation and documentation of information items, categories of information included into an information resource, procedures and conditions for provision, usage, dissemination, etc. [Amelin R.V., 2018].

Yet another component of information space — "information infrastructure" — is conceptualized in the 2016 Presidential decree "The Doctrine of Information Security" (hereinafter referred to as the Information Security Doctrine)[8], where it is defined as "a combination of informatization objects, information systems, Internet websites and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or used under international treaties signed by the Russian Federation."

It should be noted that the above mentioned definitions, contained in the presidential decrees and federal laws, are somewhat difficult to grasp. For instance, the term "information systems" is in fact referenced twice — first, in the concept of information space presented in the 2017 presidential decree, and second, as an element in the concepts of information infrastructure and information sphere, which are elaborated in the 2016 Information Security Doctrine. Besides, as it references Internet websites, the definition of information infrastructure is practically a carbon copy of the definition of information resources from the definition of information space, because websites can be categorized as arrays of documents in information systems.

At the same time, the above concept of information infrastructure in the context of cyberspace highlights the combination of material and non-material infrastructures of cyberspace, which include material equipment, such as communication networks and informatization objects (telecomunication networks, servers, routers, processors, satellites, cables, etc.), and non-material assets, such as information resources and websites.

S.A. Dementiev is right arguing that when information space is approached only in terms of technology, such approach emphasizes only a method for achieving information space and the information person, ignoring the substance of such space and such person [Dementiev S.A., 2017: 145–149].

In the humanities it is barely possibly, and hardly necessary, to formulate concepts of information space through an exhaustive description of technological characteristics referenced therein. Formulating the respec-

[8] Decree of the President of Russian Federation of December 5, 2016. No. 646. // Compendium of Laws of the Russian Federation. 2016. No. 50. Article 7074.

tive concepts, one should rather use a non-deterministic approach reflecting these concepts' substantive characteristics (communicativeness, decentralization, extraterritoriality, etc.).

It follows from the above that information space should be conceptualized as an environment where information is created, relayed, consumed and used, without an emphasis on channels by which it is transmitted and received. Technologies are undoubtedly one of the key factors in information space's functioning. It is worth noting though that, firstly, when a particular period's technological context is ignored, the argument about the absence of information space at that period appears futile. Secondly, law influences not methods by which technological infrastructures are formed but results of these infrastructures' impact.

The definition at issue should be centered on the environment in which social interactions, governed by law, occur, whereas organizational and technical aspects of information space should be referenced in the definition only inasmuch as they reflect the manner in which the respective environment is formed.

Considering that the specifics of cyberspace are conditioned by its technological characteristics, the academic community has to provide a definition of cyberspace that would reflect a combination of its technical, social, and institutional elements.

The technology-oriented definitions of cyberspace emphasize technological infrastructures, and arrays of methods used to store, change, and utilize information.

In National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) 2008 cyberspace is defined as "the independent network of information technology infrastructures, [which] includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries"[9].

In the U.S. Department of Defense's National Military Strategy for Cyberspace Operations (p.3), cyberspace is defined as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[10]

[9] Available at: https://fas.org/irp/offdocs/nspd/nspd-54.pdf (accessed: January 25, 2021)

[10] Available at: https: hsdl.org (accessed: January 25, 2021)

The Western scholarship has provided definitions of cyberspace as "a domain characterized by the use of computers and other electronic devices to store, modify, and exchange data via networked systems and associated physical infrastructures." [Schaap A. , 2009: 126].

Another definition of cyberspace is that of "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures." Some researchers came up with a social definition of cyberspace, probably taking into consideration the word's etymology — it consists of two elements, first, "cyber," originating from the Greek word *kybernao/kybernan*, meaning "to govern," "to control," [Kuehl D., 2009] and "space".

Social scientists and philosophers define cyberspace as a socio-cultural factor having an impact on development of the network society [Khutornoi S.N., 2003: 9–10]. Sometimes cyberspace is defined through a metaphorical abstraction, used for describing objects typical for computer networks — for instance, a website is described as located in cyberspace and network communication, as "communication in cyberspace." [Baryshev R.A., 2009: 9–10]; [Volov A.G., 2011: 49–54].

Identifying characteristics of cyberspace, scholars usually refer to this space's indivisibility, the fact that it cannot be reduced to borders of a physical space [Voinikanis Ye.A., 2013], fluidity and variability of cyberspace's borders [Dobrinskaya D. Ye., 2018: 52-70], geographic indeterminacy, a trans-border character [Fedotov M.A., 2016: 164-182], multidimensionality, and the absence of linearity, length, physical parameters [Anselmo E., 2006: 25]. Theoreticians also point to continuous variability of cyberspace's structure — the result of birth and death of information resources, changes in the directions of information flows, and creation of new technologies of processing and transmitting information [Bondarenko S.V., 2002: 61–64].

What makes cyberspace unique and distinctive is its global character — its universal accessibility and trans-border nature, allowing unlimited numbers of users to interact across national borders.

M.S. Dashyan approaches cyberspace as a social domain, identifying some of its essential properties, such as convergence (a mixture of traditional phenomenons and processes within one open system — the Internet); a hierarchical order, decentralization, extraterritoriality (the Internet forms a new information space — cyberspace, outside the limits of real world, so it cannot be measured with physical and chemical measuring tools); a democratic character [Dashyan M.S., 2007].

At the same time, some researchers argue that defining cyberspace is a difficult task [Hitsevich N., 2015: 16], which probably explains the emergence of somewhat fanciful descriptions of it — for instance, an electronic nervous system of our society that lends a dynamic structure to cyberspace [Manuel C., 2003: 36]. An academic inquiry into cyberspace through the lens of engineering and social scientists produced, in Russia and elsewhere, bipartite and tripartite definitions of cyberspace. Thus, cyberspace is explored both as a physical entity and a virtual one. "The physical part is the millions of networked information and communication technologies that create and enable it: computers, servers, routers, processors, satellites, switches, and cables. The virtual part is formed by electronic connections and by the data sent between and stored in the pieces of its physical infrastructure." [Spade C., 2012: 6]. Changes in cyberspace are caused by changes in, and development of, new hardware and software.

D. Clemente in his study identifies already three layers of cyberspace: "the physical layer (i.e. hardware such as submarine and ethernet cables, routers and switching devices), the logical layer (i.e. software or lines of code that allows the hardware to function and communicate), and the social layer (i.e. interaction between online personas that represent people or, increasingly, machines)." [Clemente D., 2013: 5].

There can be little doubt that cyberspace's main function is embedded in virtual reality — it consists in providing an environment where users across the globe can interact. And this function is activated by physical elements (telecommunication networks, computer systems, servers, routers, processors, satellites, switchboards, and cables) and non-physical elements (applications, software, etc.) of cyberspace alike.

The communicative and technological properties of cyberspace are reflected in the international standard ISO/IEC 27032: 2012 Information technology Security techniques. Guidelines-for cybersecurity, issued by the International Organization for Standardization (ISO) (hereinafter referred to as ISO/IEC 27032: 2012). In the document's §4.21 cyberspace is defined as "a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks."[11]

[11] Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (accessed: March 23, 2021)

Cyberspace, therefore, can be regarded both as a virtual communications environment and as certain electronic carriers providing access to this environment.

In Russian scholarship, likewise, two approaches to cyberspace — technological and social — coexist [Vagin O.A., Goriainov K.K. et al, 2018].

In the technological theoretical framework, cyberspace is an information and telecommunication instrument for transmitting, processing and storing information (principles of organization of hardware networked environment, selection of networking protocols, organization of address spaces, etc.). From the vantage point of social sciences, cyberspace is a complex socio-cultural phenomenon that influences many facets of society's life and forms a special environment in which certain types of activity and specific social relations occur[12].

Defining cyberspace, one should take into consideration subject-oriented approach as well. Management of cyberspace consists in coordinating the processes of distribution of address spaces, exploitation of root servers, creating and administering systems of domain names and internet addresses, etc. Managers of cyberspace include not only national governments and intergovernmental organizations, but also certain national and international non-governmental organizations: Internet Society (ISOC), Internet Corporation for Assigned Names and Numbers (ICANN), etc., as well as open communities, such as Internet Engineering Task Force (IETF). The Working Group of Internet Governance (WGIG) at its meetings in 2004–2005, too, referenced a large group of entities managing the Internet: governments, private businesses, civic society, intergovernmental and non-governmental international organizations, as well as other forums[13].

It is this type of management by a large group of stakeholders (governments, non-governmental organizations, private persons, etc.) that defines certain features of cyberspace, which, unlike terrestrial, aerial, cosmic and marine spaces, that is the realms traditionally governed by international law, does not have a "natural" origin and is a product of human creativity. Cyberspace is an artificial environment for creating, transmitting and using information.

[12] Ibid.

[13] Background Report. World Summit on the Information Society. Available at: http://www.itu.int/wsis/wgig/docs/wgig-background-report.pdf (accessed: January 20, 2019)

Conclusion

So, defining cyberspace, one should take into account not only its technological and social elements, but also its subject-oriented component.

It should be noted that although the above mentioned 2017 Presidential decree provides definitions of such modern phenomena as internet of things, cloud computing, big data processing, etc., it does not contain a definition of cyberspace. As for international documents, the term "cyberspace," without a definition, comes up in the 2000 Okinawa Charter on Global Information Society[14] and the 2001 Convention on Cybercrime[15].

Although the Russian legislation does not have a definition of cyberspace, attempts to conceptualize it were made by the authors of the Draft of the Concept of Cybersecurity Strategy in the Russian Federation[16]. In the Draft cyberspace is a particular element of information space with clear boundaries, and also a type of operations in information space, which are brought about by a combination of communication channels of the Internet and other telecommunication networks, technological infrastructure enabling their functioning, and all forms of human activities (by individuals, organizations, governments) carried out via them.

The definition of cyberspace in the 2016 Information Security Doctrine, too, stresses technological characteristics, defining cyberspace as information systems and sites in the information and telecommunications system Internet. "The Internet" and "cyberspace," however, are not synonymous. The Internet is just one type of computer networks among others.

Cyberspace includes, but is not limited to, the Internet. Technology-wise, cyberspace includes computers that can be either plugged into or unplugged from the Internet, as well as networks, which can or cannot be a part of the Internet[17].

As was noted by Yu. V. Anokhin and M. P. Baranov, a computer unplugged from the Internet can process information and create a virtual space for a user working on it, while also influencing this user's mind. They add that activating a software — for instance, a computer game — users

[14] Okinawa Charter on Global Information Society, July 22, 2000. Diplomaticheskiy vestnik. 2000, no 8, p. 52.

[15] The Convention came into force on July 1, 2004. The Russian Federation is not party to it.

[16] Available at: URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (accessed: February 21, 2020)

[17] At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues…

enter in an indirect relationship with this game's creators, falling under the sway of images and symbols programmed by the creators [Anokhin Yu.V., Baranov M.P., 2019: 14–24].

Because cyberspace comprises ordinary in-house computer networks ("extranets"), as well as virtual networks connecting private networks of different companies ("intranets"), one can definitely conclude that cyberspace as an idea is broader than the "Internet network." And considering that cyberspace includes a wide range of communication networks, it is precisely the notion of cyberspace that should be employed determining what state should have jurisdiction over a matter.

ISO/IEC 27032: 2012, defining cyberspace as "a complex environment resulting from the interaction of people, …supported by …communications technology," conceptualizes the Internet, in §4.29, in a more technological vein, as "a global system of inter-connected networks in the public domain"[18].

Cyberspace thus is one of the elements of information space, which is an environment of social interactions whose functioning is supported by a combination of telecommunication networks and by a technological infrastructure. And social interactions among different subjects of law can be carried out without a connection to the geographic territory of a particular state.

If we are to converge social, technological and subject-oriented approaches, here is what appears to be the most apt definition of cyberspace: an artificial telecommunications environment in which social interactions occur, which is managed by a wide range of subjects of private and public law, and the functioning and maintenance of which are carried out via the software-and-hardware infrastructure consisting of material elements (telecommunication networks, computers, servers, routers, satellites, etc.) and non-material elements (software, data transfer standards, applications, software, etc.).

References

Abdrakhmanov D.V. (2016) State sovereignty and information society: mutual connection and mutual dependence. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta,* no 4, pp. 66–72 (in Russian)_

[18] Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (accessed: March 23, 2021)

Adams J., Albakajai M. (2016) Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, no 6, pp. 256–265.

Amelin R.V. (2018) Federal and Municipal Information Systems in the Russian Information Legislation: A Theoretical Legal Analysis. Garant.ru (in Russian)

Anokhin Yu.V., Baranov M.P. (2019) Doctrinal characteristic of the ideological function of the state in virtual space. *Zhurnal rossiyskogo prava*, no 8, pp. 14–24 (in Russian)

Anselmo E. (2006) Cyberspace in international law: does the rise of the Internet give the lie to the territorial principle in international law? *Ekonomicheskie strategii*, no 2, pp. 24–31 (in Russian)

Bachilo I.L. (2016) Conceptual framework of information law and the information security system. *Trudy Instituta gosudarstva i prava RAN,* no 3, pp. 76–88 (in Russian)

Baryshev R.A. (2009) Cyberspace and Alienation. Candidate of Philosophical Sciences Summary. Moscow, pp. 9–10 (in Russian)

Benyekhlef K., Gelinas F. (2001) The International Experience in regard to Procedures for Settling Conflicts relating to Copyright in the Digital Environment. *UNESCO Copyright Bulletin*, no 4, pp. 3–19.

Bethlehem D. (2014) The End of Geography: The Changing Nature of the International System and the Challenge to International Law. *European Journal of International Law*, no 1, pp. 9–24.

Bondarenko S.V. (2002) Social community of cyberspace. *Informationnoye obschestvo*, no 4, pp. 61–64 (in Russian)

Chernichenko S.V. (2010) Is state sovereignty divisible? *Yevraziyskiy yuridicheskiy zhurnal*, no 12, pp. 25–31 (in Russian)

Clemente D. (2013) Cyber Security and Global Interdependence: What Is Critical? Available at: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf (accessed: February 21, 2020)

Dashyan M.S. (2007) Law of Information Highways: Legal Regulation of the Internet In: Pravo informatsionnykh magistraley: voprosy pravovogo regulirovaniya v sfere Internet. Garant.ru. (in Russian)

Dementiev S.A. (2017) Transdisciplinary analysis of information space of modern society. *Vestnik Krasnodarskogo universiteta MVD Rossii,* no 4, pp. 145–149 (in Russian)

Dobrinskaya D.Ye. (2018) Cyberspace: a territory of modern life. *Vestnik Moskovskogo universiteta*, no 1, pp. 52–70 (in Russian)

Fedotov M.A. (2016) Constitutional responses to challenges of cyberspace. *Lex Russica*, no 3, pp. 164-182 (in Russian)

Galushko D.V. (2013) State sovereignty in international law. *Vestnik Voronezhskogo universiteta*, no 1, pp. 366–374 (in Russian)

Girich V.L., Chuprina V.N. (2007) Global information space and access to the world's resources. Available at: URL: http://marc21.rsl.ru/upload/mba2007/mba2007_05.pdf. (in Russian)

Hitsevich N. (2015) Intellectual property rights infringement on the Internet: an analysis of the private international implications. Available at: http://openaccess.city.ac.uk/17914/ (accessed: November 1, 2020)

Ivanov V. (2009) The state and sovereignty. A discussion of sovereignty. Available at: URL: http://www.russ.ru/Mirovaya-povestka/Gosudarstvo-i-suverenitet (accessed: May 10, 2020) (in Russian)

Izbulatov K.K. (2007) Methodological tools for political and legal inquiry into the notion of economic sovereignty. *Filosofiya prava*, no 3, pp. 139–141 (in Russian)

Johnson D., Post D. (1996) Law And Borders: The Rise of Law in Cyberspace. Available at: https://cyber.harvard.edu/is02/readings/johnson-post.html (accessed: May 10, 2020)

Kopylov V.A. (2002) *Information Law*. Moscow: Delo, 512 p. (in Russian)

Khavanova I.A. (2013) Fiscal (taxation) sovereignty and its limits in integrationist alliances. *Zhurnal rossiyskogo prava*, no 11, pp. 41–51 (in Russian)

Khutornoi S.N. (2003) Cyberspace and the Formation of Network Society. Candidate of Philosophical Sciences Thesis. Voronezh, 166 p. (in Russian)

Kirilenko V.P., Alexeyev G.V. (2016) State sovereignty in the present-day geopolitical situation. *Upravlencheskoe konsul'tirovanie*, no 3, pp. 14–23 (in Russian)

Kobrin S. (1997) Electronic cash and the end of national markets. *Global Issues*, vol. 2, pp. 65–77.

Kucheryavyi M.M. (2015) The Russian state's policies of information sovereignty in the modern globalized environment. *Upravlencheskoe konsul'tirovanie*, no 2, pp. 8–15 (in Russian)

Kuehl D. (2009) From Cyberspace to Cyberpower: Defining the Problem» in Cyberpower and National Security 48. Available at: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210 (accessed: February 15, 2021)

Malakhov V.C. (2007) *The State in an Age of Globalization.* Moscow: Knizhny dom, 252 p. (in Russian)

Manuel C. (2003) *The Internet Galaxy: Reflections on the Internet, Business and Society.* Oxford: University Press, 292 p.

Marchenko M.N. (2011) *The State and Law in an Age of Globalization.* Moscow: Prospect, 656 p. (in Russian)

Matusitz J. (2014) Intercultural perspectives on cyberspace: An updated examination. *Journal of Human Behaviour in the Social Environment,* vol. 24, pp. 713–724.

Moiseyev A.A. (2007) Relationship Between Sovereignty and Supranationality in the Modern International Context of Globalization. Doctor of Juridical Sciences Summary. Moscow, 45 p.

Polikarpov V.S., Polikarpova Ye.V. (2014) The newest information and communications technologies and Russia's information sovereignty. *Informatsionnoe protivodeystvie ugrozam terrorizma,* no 23, pp. 279–284 (in Russian)

Prosvirnin Yu. G. (2000) *Information Law*. Voronezh: University, p.64 (in Russian)

Reut O.Ch. (2007) Adjectives of sovereignty. Sovereignty as an adjective. *Polis*, no 3, pp. 115–124 (in Russian)

Samarin A.A. (2016) Extraterritorial Effects of Law. Candidate of Juridical Sciences Summary. Nizhny Novgorod, 31 p. (in Russian)

Schaap A. (2009) Cyber Warfare Operations: Development and Use under International Law. *Air Force Law Review*, vol. 64, pp.121–173.

Shakhmametiev A.A. (2013) Taxation sovereignty and taxation jurisdiction of the state. *Sovremennoe pravo*, no 3, pp. 76–81 (in Russian)

Sharifov M.S. (2009) Sovereign power in cyberspace and in network space. *Sovremennoe pravo*, no 6, pp. 40–44 (in Russian)

Schmitt M. (2013) *Tallinn Manual of the International Law Applicable to Cyber Warfare.* Cambridge: University Press, 215 p.

Spade C. (2012) Information as Power: China's Cyber Power and America's National Security. Available at: https://itlaw.wikia.org/wiki/Information_as_Power:_China%27s_Cyber_Power_and_America%27s_National_Security (accessed: January 12, 2021)

Streltsov A. (2017) Sovereignty and jurisdiction of the state in an age of information and communication technologies in the context of international security. *Mezhdunarodnaya zhizn*, no 2, pp. 88–106 (in Russian)

Talapina E.V. (2018) State sovereignty and information space: new objectives of law. *Gosudarstvo i pravo*, no 5, pp. 60–67 (in Russian)

Tulikov A.V. (2016) International legal thought in an age of the development of information technologies. *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*, no 3, pp. 235–243 (in Russian)

Vaganov P.A. (2006) Legal defense of cyberspace in the United States. *Izvestiya vysshikh uchebnykh zavedeniy. Pravovedenie, n*o 4, pp. 73–89 (n Russian)

Vagin O.A., Goriainov K.K. et al (2018) *Theoretical Framework of Crime Detection and Investigation.* Garant.ru. (in Russian)

Voinikanis Ye.A. (2013) Intellectual Property Law in a Digital Age: A Paradigm of Balance and Flexibility. Garant.ru. (in Russian)

Volov A.G. (2011) Philosophical analysis of the idea of "cyberspace". *Filosofskie problemy informatsionnykh tekhnologiy i kiberprostranstva, n*o 2, pp. 49–54 (in Russian)

Yefremov A.A. (2017) Formation of the concept of information sovereignty of the state. *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*, no 1, pp. 201–215 (in Russian)