Internet Governance: System Imbalances and Ways to Resolve Them[1, 2]

S. Vasilkovsky, A. Ignatov

Sergei Vasilkovsky – Researcher, Centre for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration; 11 Prechistenskaya naberezhnaya, Moscow, 119034, Russian Federation; E-mail: vasilkovskiy-sa@ranepa.ru

Alexander Ignatov – Researcher, Centre for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration, 11 Prechistenskaya naberezhnaya, Moscow, 119034, Russian Federation; PhD Student, MGIMO University, 76 Prospect Vernadskogo, Moscow, 119454, Russian Federation; E-mail: ignatov-aa@ranepa.ru

Abstract

The spread of digital technologies has led to the global digitalization of all types of public activities. The digital economy emerging during this process has become a leading factor in world economic growth and one of the criteria of national development. The digital economy is based on the Internet, which ensures the functioning of new business models, forms of social interaction and public diplomacy. The Internet's governance system differs from other modern international systems of public and political relations in that the leading role in it is played by non-governmental organizations, in particular, the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society (ISOC). The activities of states are significantly limited by the basic properties of the system, which complicates the implementation of the state's digital sovereignty. The aim of this article is to determine ways to resolve this discrepancy.

Analyzing the current state of Internet governance, the authors outline the key characteristics that lead to potential conflict. These include decentralization, an insufficient evaluative level of accountability and lack of legitimacy. The authors analyze ICANN and ISOC toolkits and identify the key instruments that actually make organizations central to the Internet's governance system. In conclusion, the authors provide recommendations for action by the international community to mitigate the identified imbalances.

Key words: digital technologies; digital economy; digital sovereignty; Internet; Internet governance; cyber power; ICANN; ISOC

For citation: Vasilkovsky S., Ignatov A. (2020) Internet Governance: System Imbalances and Ways to Resolve Them. *International Organisations Research Journal*, vol. 15, no 4, pp. 7–29. (in English). DOI: 10.17323/1996-7845-2020-04-01.

Introduction

In recent decades, the quick spread of the digital economy and the Internet as its main component [Bukht, Heeks, 2018, pp. 148–51] has led to transformation of all aspects of social interactions. Developments in the sphere of Internet-based economic activities raised the profile of the Internet as a means of production in various economic spheres [see Kaila, Tarp, 2019;

[1] The editorial board received the article in August 2020.

[2] The article was written on the basis of the RANEPA state assignment research programme.

Korchagin, Deniskina, Fateeva, 2019; Pozdnyakova et al., 2019; Shiroma et al., 2019; Zhang, Chen, 2019]. Growth in the traffic capacity of digital infrastructure[3] opened prospects for proliferation of digital trade: in 2017, the total amount of digitally delivered goods and services grew to $29 trillion [UNCTAD, 2019, p. 15]. As a result, the digital economy, also known as the Internet economy, makes up 22% of the global economy, and this figure tends to grow [Bukht, Heeks, 2018, p. 158].

At the same time, the Internet is acknowledged to be a source of new security threats. The European Union's (EU) NIS Directive on the security of network and information systems across the Union is premised on the notion that the security of information networks, including the Internet, plays the fundamental role in transboundary movement of goods, services and people and thus is the pillar of sustained functioning of the internal market [EU, 2016, Para. 3].

The Internet is a competition ground for various parties and groups of interests. At the same time, states' decision-making capacities concerning the management of the Internet are quite limited despite the fact that they remain the main subjects of global policy by their nature [Haugen, 2020; Liaropoulos, 2013; Nye, 2014]. The Internet's governance system is characterized by a relatively low level of accountability for the main non-state actors and thus the system itself could be defined as non-legitimate [Haugen, 2020; Keohane, 2011]. Selected papers argue for the more active participation of states in Internet governance, for instance, in human rights-related matters [Zalnieriute, Milan, 2019].

Taking into account the conflictogenity of the Internet's governance system, it is not surprising that states argue for more delegated power in Internet-related matters. The goal of gaining more weight in Internet governance is embedded in Russia's doctrine of information security [President of Russia, 2016].

This article seeks ways to resolve the disproportions that are entrenched in the Internet's governance system. We start with an analysis of the basic characteristics of the system which predetermine the conflict between the limitations of state sovereignty and the low level of accountability for non-governmental parties. Next, we consider the main features of the main non-governmental parties in Internet governance – the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society (ISOC). We conclude with recommendations intended to iron out the constraints of the Internet's governance system.

Basic Characteristics and the Role of States in Internet Governance

Internet governance is a complex process because 'the Internet is, by definition, a complex system that is not governed by some separate organization' [van Horenbeeck, 2018, p. 6]. A brief overview of the emergence and development of the Internet allows for the identification of the contradictions that characterize this system.

In the late 1960s the U.S. created the Advanced Research Project Agency Network (ARPANET) system, a prototype of the modern Internet. Despite the fact that systems like ARPANET were under development in several other countries, it was the American project that became the forerunner [Paloque-Berges, Schafer, 2019, p. 4].

The first ARPANET sponsor was the Defense Advanced Research Projects Agency. The system was created to provide access to remote computers throughout the United States. Within

[3] The Organisation for Economic Co-operation and Development (OECD) proposed one of the most prominent definitions of this notion: 'Digital infrastructures, including efficient, reliable and widely accessible broadband communication networks and services, data, software, and hardware, are the foundations on which the digital economy is based' [OECD, 2017, p. 28]. In the past decade the carrying capacity of transnational data networks has grown by 45 times [Nye, 2017], and the total number of devices based on the 'Internet of things' technology is expected to surpass 20 billion [Naughton, 2016].

the framework of ARPANET technologies were developed which subsequently determined the features of the modern Internet – in particular, data routing technology and the first version of the Internet protocol. In 1986, the former members of the ARPANET project created the Internet Engineering Task Force (IETF), the first open professional organization with a focus on networking. The ARPANET project was scrapped in 1990 due to the revision of the budgetary policy of the U.S. Department of Defense.

Since the 1990s, the number of Internet users has grown at a rapid pace, surpassing one billion in 2006 according to International Telecommunication Union (ITU) statistics. The determining factors for the spread of the Internet included falling prices for personal computers and the development of global infrastructure.

In the 2000s, the growing importance of the Internet made it urgent for the global community to find consensus on the basic characteristics of the global information network management system. The basic principles were enshrined in a declaration adopted during the World Summit on the Information Society in 2003–05. The declaration focused on 'cooperation and partnerships between all stakeholders' [UN, 2003, Para. 20], including governments, private companies, civil society, the United Nations (UN) and other international organizations. It also stated that 'Internet governance encompasses both technical and public policy issues' [UN, 2003, Para. 49]. The declaration assigned responsibilities to all parties involved in developing the technical and economic aspects of the Internet and clarified the role of states: 'Political authority over Internet-related public policy issues is the sovereign right of states. States have rights and responsibilities regarding Internet-related public policy issues at the international level' [UN, 2003, Para. 49 (a)].

The variety of actors participating in the regulation of the Internet determines the complexity of interactions between them and the impossibility of identifying a single centre in this system. Joseph S. Nye characterizes the Internet's governance system as a complex regime, encompassing the interaction of the actors involved at the physical and informational levels. Internet governance is also a component of a more sophisticated cyberspace governance regime [Nye, 2014]. States 'nesting among other subjects of <Internet> governance' [Scholte, 2017, p. 166] operate mainly at the physical level, while private companies and international organizations mainly operate at the information level. It is from this level that the main threats emanate because the actions of attackers in the information space can cause disproportionately high damage at the physical level, 'where resources are limited and have a high price' [Nye, 2014, p. 5].

Cyberspace governance, as a new reality, presupposes the presence of fundamentally different instruments. With the integration of digital technologies into social and political realities, the role of cyber power is increasing and is no longer limited to states. The asymmetry generated by this phenomenon is leading to a redistribution of power in the international arena [Nye, 2010].

The monopoly of states on the possession and exercise of traditional power does not at all predetermine their leadership in cyberspace. The relatively low cost of entering the market, user anonymity, and asymmetry in vulnerabilities mean that new actors have more opportunities to use hard and soft power in cyberspace than in other areas of international politics. The main problem here is the disproportionate power of states due to their traditional role in international affairs and their limited ability to control cyberspace.

The high cost of state activity at the information level determines the dominance of non-state actors in it. Among other components, the addressing system and technical standards are important elements of the Internet's management system. They are uniformly applied throughout the entire space of the global network and without them the existence of the Internet is impossible. The first element is under the authority of ICANN, and the second is within the responsibility of organizations administered by ISOC (see Fig. 1).

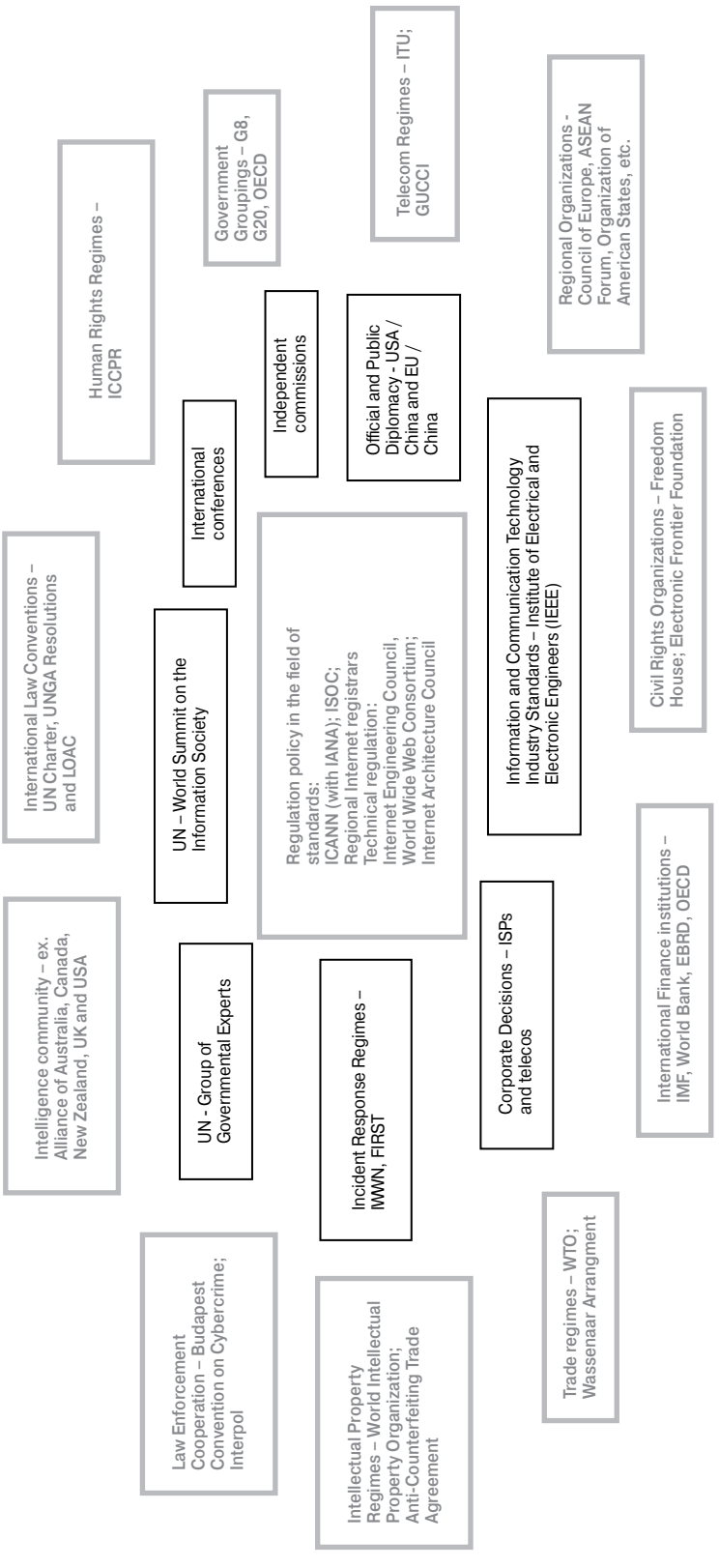

Fig. 1. The Complex System of Cyberspace Management

Source: [Nye, 2014, p. 8].

The actions of states at all levels of Internet governance are dictated by the logic of sovereignty protection. But, in the context of Internet and cyberspace governance, we might use not the traditional approach to sovereignty, but the *digital* one. There are two ways to define the essence of digital sovereignty, which is critical for understanding the current role of states in Internet governance.

The first approach follows the traditional realist and neorealist understanding of the state's role and the properties of state sovereignty in the context of the development of digital technologies. Researchers using this approach maintain the notion of the primacy of the state and national law in the digital (cyber) space, which leads to a similarity between the concepts of classical and digital sovereignty [see Franzese, 2009; Irion, 2012; Polatin-Reuben, Wright, 2014; Qi, Shao, Zheng, 2018; Schmitt, 2013; Ukolov, Cherkasov, 2019; Wu, 1997; Zeng, Stevens, Chen, 2017]. The state's power over the elements of digital infrastructure located in national territories creates the basis for the expansion of sovereignty to cyberspace. Some authors [see Kukkola, Ristolainen, 2018] indicate that such a conclusion is not merely academic. They find its direct expression in the politics of some states – Russia, in particular [Ibid., p. 1]. Similar statements are found in the works of Chinese researchers [Qi, Shao, Zheng, 2018; Zeng, Stevens, Chen, 2017].

The second approach follows a more liberal tradition [see Bratton, 2015; Couture, Toupin, 2019; Globerman, 1978; Grant, 1983; Istomin, 2020; Mueller, 2017]. Accordingly, the state is seen as one of the carriers of digital sovereignty, along with private companies [Grant, 1983; Istomin, 2020] and individuals [Couture, Toupin, 2019]. A 'blurring' of state sovereignty when attempting to project it into cyberspace is based on several factors, the main one being the creation of new technological solutions by private companies without the participation of states [Grant, 1983] as well as the limited presence of the state in new systems of digital development management [Bratton, 2015]. The inertia of the state in cyberspace means that, in some issues, its role has been limited to standard setting. For example, as in the case of managing the address space of the Internet – the 'legitimacy of the activities' of private companies is recognized 'in the national law of states, in entities..., in international law...' [Istomin, 2020].

Both approaches agree that on the physical level states have many more opportunities to realize their own digital sovereignty than on the information level. The state can control elements of digital infrastructure within its jurisdiction, which makes it possible on the physical level to consider digital sovereignty as identical to the classical, Westphalian notion of sovereignty [Nye, 2014, p. 8]. Conflicts at this level have a horizontal nature, which means states compete with actors of the same nature when exercising their cyber power.

At the information level, the situation is different. In controlling the digital infrastructure up to a certain limit, the state can apply the provisions of its own national law to regulate a separate segment of the Internet, but not the entire system. The conflict in this case has not only horizontal, but also vertical expression – states compete both among themselves and with actors of a fundamentally different nature, for example, with non-governmental organizations such as ICANN and ISOC, which 'take into account opinions, but not the "voices" of states' [Nye, 2014, p. 6]. At the same time, attempts to develop a general consensus on certain issues of Internet governance through international organizations such as ad hoc working groups of the United Nations and the ITU have not led to the development of a universal, practical solution. More results have been achieved at the level of regional and interregional agreements, an example of which is the 2001 Budapest Convention on Cybercrime. However, regarding that convention, the following statement is true: 'The most significant cybercrime agreement to date was agreed upon before Facebook and Twitter, and roughly matches the dawn of digital giant Google. It is unlikely that this agreement will be able to cover the rapid transformation of Internet technologies that we see today' [van Horenbeeck, 2018, p. 6].

Based on the above discussion, we come to the conclusion that some of the very important mechanisms that ensure the functioning of the Internet at the present stage were formed without the participation of states. This is partly due to the insufficient assessment level of accountability of such mechanisms, and, as a consequence, the insufficient level of legitimacy of the Internet governance system as a whole.

In general, the concept of accountability for global governance institutions, to which the mechanisms of Internet governance can certainly be attributed, is based on three components: transparency of the decision-making process; provision of a rationale for decisions and actions; and the ability of actors to impose sanctions in response to decisions and actions taken by the institution [Hilbrich, Schwab, 2018, p. 10].

Accountability is seen as one of the most important components of the legitimacy of global governance institutions [Keohane, 2011, p. 102]. Even if the other criteria of an institution's legitimacy[4] are fully met, the discrepancy between individual components and the expectations of stakeholders inevitably leads to a decrease of the institution's legitimacy. Incomplete evaluative legitimacy of the institution, however, does not negate the possibility of reaching a temporary consensus regarding its actions. Such an outcome may satisfy most of the participants for a certain period of time, but a system of this kind cannot maintain itself in a long run. This inevitably leads to the revision of the status quo.

Thus, we note three characteristics of the modern system of Internet governance. First, this system is complex and multi-levelled. Internet governance itself implies decision-making at two levels – physical (digital infrastructure) and informational (various system-related international regimes, technical standards and addresses). States make decisions primarily at the physical level, establishing rules for the functioning of digital infrastructure on their territory, thereby partially realizing their digital sovereignty. The activities of states at the information level are currently limited by the existing status quo in which non-state actors play a significant role in decision-making.

Second, the current configuration of the Internet's management system does not allow for the emergence of a single centre that makes decisions both at the physical and informational levels. Attempts to attribute the decision-making functions on specific issues of Internet governance to existing international institutions have not had significant success. The current model of Internet governance allows for the existence of many actors with the 'decisive vote,' among which a significant number are represented by non-governmental organizations.

Finally, a logical derivative of the first two characteristics is low accountability of the key institutions and, consequently, the incomplete legitimacy of the Internet's governance system. This will be discussed in more detail in the analysis of the activities and structure of key non-governmental organizations involved in Internet governance – ICANN and ISOC.

[4] Robert Keohane identifies six criteria of legitimacy: 1) compliance with minimum moral standards (compliance with generally accepted criteria, for example, in matters of ensuring human rights); 2) inclusiveness (the possibility of participation of a wide range of stakeholders in the decision-making); 3) epistemological equality (the availability of information about the activities of the institution to those who are influenced by the decisions made); 4) accountability (the ability of stakeholders to influence decisions); 5) democratic principles of governance (the presence of mechanisms of public control, protection of minority rights, ensuring a general consensus in decision-making at the international level); 6) the creation of comparative advantages (activities on an international basis should bring more benefits than alternative schemes of interaction, for example, on a bilateral basis) [2011, pp. 101–4]. Compliance with some criteria and non-compliance with others, as, for example, occurs in the case of the activities of the UN Security Council in creating comparative advantages [Ibid., p. 105], expresses a lack of confidence in the institution and decisions made on its platform.

ICANN and ISOC in Internet Governance: Key Features and Imbalances

ICANN and ISOC play a special role in the governance of the Internet and cyberspace. Their task is to develop standards for activities in cyberspace. The IETF and the Internet Architecture Board (IAB), which hold key positions in the development and harmonization of technical aspects of the functioning of the Internet, belong to the system of organizations whose activities are directly supported by ISOC. It is reasonable to argue that ISOC has authority not only in policy but also in applied technology issues (see Fig. 1).

Below, we consider the main characteristics of these organizations and identify the tools with which they participate in Internet governance, as well as the problems that arise in this regard.

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN is 'a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. Through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet' [ICANN, 2020a].

Technically, ICANN helps to maintain the functions of the Internet Assigned Numbers Authority (IANA), which provides key services for the Internet's basic address book, the domain name system (DNS). ICANN's key sphere of activity is the regulation of the domain name market and the unification of the Internet address system. In addition, the organization performs other functions: Internet-related services, intellectual property protection, and protection of the interests of commercial and non-commercial organizations and Internet users.

ICANN relies on two main tools in its operations: market mechanisms and a deliberative structure. There are two reasons for this. First, the goal is to demonopolize the Internet services market; second, the socio-political agenda is formed from the bottom up. Thus, ICANN's policy is based on a multi-stakeholder consensus-seeking approach.

ICANN member organizations and users form requests at the lower level. They are then reviewed in various advisory committees and working groups. Finally, the recommendations are submitted to the board for voting. As adopted in the bylaws, ICANN organizes international conventions and conferences, thus providing a discussion forum for supporters to discuss policy issues related to the Internet's development. Anyone can join most of ICANN's working groups, ensuring broad representation. The issue is then brought up for public discussion or submitted for revision by the committees. The process is repeated until ICANN stakeholders reach consensus or the board accepts all amendments and proposals.

In a similar way, the corporation builds its relations with organizations representing states and establishes outreach interaction with other international firms, unions and groups. Such interaction primarily relies on market mechanisms and international law, as well as on the civil law of the United States and other states.

The main issue, however, is ICANN's location in California. The organization has a long history of partnership with the U.S. government and of being accountable to the state. The movement toward independence began on 25 November 1998, when ICANN and the U.S. Department of Commerce entered a memorandum of understanding [NTIA, 1998]. The department relied on ICANN to manage some of the technical functions of the DNS, such as numbering Internet addresses, coordinating port assignments and helping to maintain the sta-

bility of the Internet's unique identifiers. The memorandum of understanding required regular reporting to the U.S. Department of Commerce. However, on 10 March 2016 ICANN submitted a proposal to transfer the IANA's governance functions from the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce to the global community.

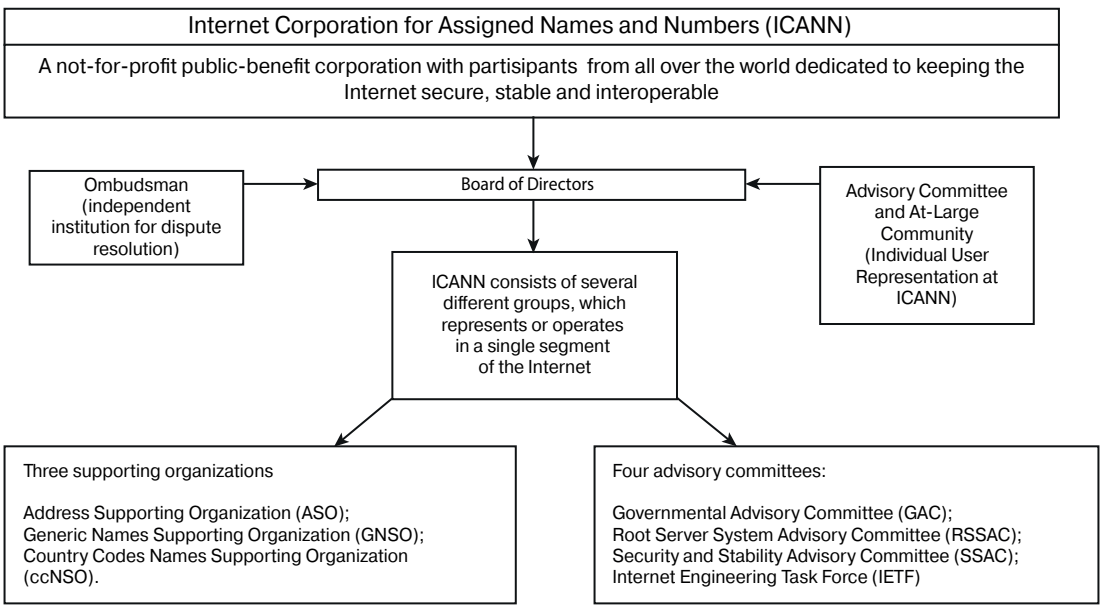

Fig. 2. ICANN's Organizational Structure

Source: Compiled by the authors.

This agreement completed a joint public-private partnership. The overall legal part of these changes was significantly less than the political: the United States retained a reduced, but still real, degree of control. However, the introduction of an additional independent actor to the world arena reduced international tension. The transition from state control to public sector control has solved three problems. The first is related to the issue of the organization's legitimacy. The withdrawal from the influence of the U.S. government improved the organization's reputation in the international arena and reduced tension within the international community [Becker, 2019]. Second, the transition reduced the influence of states on international organizations and unions, in particular in the EU. Third, the main functions of a specific industry were given to the expert community with a bottom-up decision-making system that made it possible to democratize the corporation's activities.

However, ICANN's independence has increased the profile of the Governmental Advisory Committee (GAC). Any ICANN decision concerning member countries must be made in consultation with the GAC [ICANN, 2020a]. The GAC currently has 178 members and 38 observers, the latter including such organizations as the Council of Europe, the International Telecommunication Union, the International Criminal Court, the World Health Organization, WHOIS, the World Trade Organization, the UN Educational, Scientific and Cultural Organization, and others. According to ICANN's charter, decisions of the committee are advisory and 'relate to the activities of an organization affecting the interests of governments, in particular

on the interaction of ICANN rules with various national laws and international agreements, or affecting public policy issues' [ICANN, 2020b].

The GAC has considerable political influence over ICANN. As a result, decisions that are not welcomed by the U.S. and European governments and their most influential business lobbies may not be made in the organization, as the board must find consensus with the committee. On the one hand, each country has only one vote in the committee, which often does not allow for a consolidated decision. On the other hand, regional associations such as the EU have more weight in the committee.

In addition, the domain name system is increasingly influenced by government law enforcement agencies. Some of this influence is channelled through the GAC, but the latter goes through other bodies such as the Generic Names Supporting Organization (GNSO) [Bygrave, 2015].

Internet Society (ISOC)

ISOC was established in 1992 by a group of enthusiasts who had formerly worked for the IETF. ISOC's task was defined as 'to provide an institutional home for and financial support for the Internet Standards process' [Cerf, 1995]. Growth of the Internet ecosystem, the urgent need for regional bodies to maintain the commonality in processing and formulation of the Internet standards, and new technological solutions required financing that exceeded the limits of government-sponsored programmes.

ISOC provides financing for the IETF, the IAB, the Internet Research Task Force (IRTF), the Internet Engineering Steering Group (IESG), the Online Trust Alliance (OTA) and the Public Interest Registry (PIR) (Fig. 3). The ISOC collects membership fees from individual members of the Society and donations from sponsoring companies.

ISOC is administered by a 13-member board of trustees elected by ISOC's regional bodies, member companies and the IETF. In addition to general management, the board governs the work of the IAB. Since the establishment of ISOC, no Russian citizen or representative of Russian information technology (IT) companies has been elected to the board. The largest number of nominations has been given to citizens of the United States [Internet Society, n. d., a].

ISOC provides several privileges to sponsoring companies based on the size of the contribution [Internet Society, n. d., b]. For instance, platinum-tier companies may sponsor specific programmes of the Society and are able to nominate members to the board. Russian companies do not contribute to ISOC. Most of the top sponsors of the Society are U.S.-based IT holdings (see Table 1).

Table 1. The Top Sponsors of the ISOC With a Contribution of More than $100,000

Country of Origin	Name	General Characteristic
U.S.	Comcast	Cable TV/Internet provider
U.S.	Juniper Networks	Communication devices manufacturer
U.S.	NBCUniversal	Cable TV/Internet provider
U.S.	Oracle Corporation	Software company
U.S.	Private Internet Access	VPN provider
The Netherlands	RIPE NCC	Regional Internet addressing administrator

Source: [Internet Society, n. d., c].

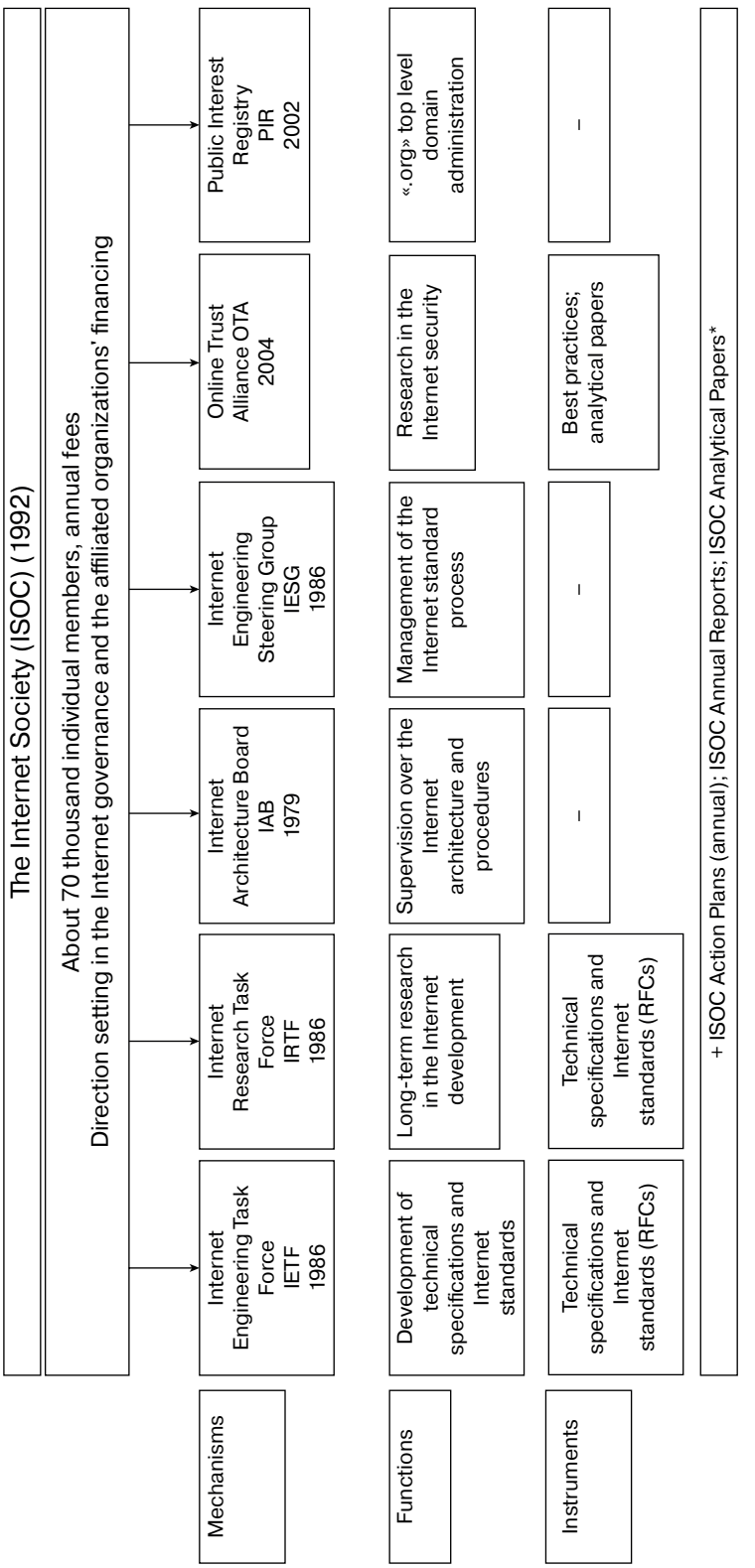

Fig. 3. Organizations Affiliated With the ISOC: Their Functions and Instruments

Source: Compiled by the authors.

ISOC regularly publishes papers on the Internet's development. The instruments created and possessed by ISOC lack formality and there are no established mechanisms for further monitoring and control of the process of implementation of its decisions. ISOC publishes Requests for Comments (RFCs) that serve as the basis for the Internet standard process, Action Plans, Global Internet Reports, analytical papers and best practices on network security (the main responsibility of the ODA).

As the main sponsor of the IETF and the IRTF, ISOC has proprietary rights to the RFCs and the Internet standards. The notion of the Internet standard implies 'a specification that is stable and well-understood, technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet' [Bradner, 1996, p. 2]. The specification here is 'any description of a protocol, service, procedure, convention, or format' [Ibid., p. 8].

Every active standard of the Internet focuses on a specific issue related to the sustainable operation of the global Internet network. A standard may be described by more than one RFC, based on the complexity of the issue. The relevant RFCs present the description of an issue, propose solutions to the problem and definitions.

Proposals on technical specifications processing are presented by the IETF and the IRTF. The decision on whether a specification is to serve as the Internet standard is the responsibility of the IESG and the IAB. If the conditions mentioned in the definition of the Internet standard are met it will be approved as the universal standard.

The Internet standards are not legally binding. However, their importance for the Internet's functionality raises their status to the level of 'soft law.' The Internet standards approved by ISOC are universally accepted across the Internet. Taking into account the importance of the Internet for manufacturing, communications and governmental affairs, ISOC's Internet standards are thus unique and indispensable.

We witness an important discrepancy between ICANN/ISOC functions and their structure. The Corporation and the Society make decisions on issues that are critically important for the Internet's functioning, but their accountability can be questioned. The soft spot here is the lack of formalized feedback mechanisms to communicate with all Internet users (governments, companies, individuals, etc.) (see Table 2)

Table 2. ICANN/ISOC Accountability Components

	ICANN	**ISOC**
Transparency	Form 990 financial statement (U.S. standard)	Form 990 financial statement (U.S. standard); Annual activity reports
Decision feasibility	Five-year strategic plan	Annual activity reports
Feedback mechanisms	Governmental Advisory Committee (GAC) *The GAC makes non-regulatory decisions* The ICANN committees constantly interact with counterparts and end users	*Permanent representation of states is not provided* Premium corporate membership mechanism Regional and international *ad hoc* conferences [Internet Society, n. d., d].

Source: Compiled by the authors.

Conclusion: The Future of the Internet and General Proposals

This analysis shows that decentralization, lack of accountability and unfulfilled legitimacy are the key features of the contemporary Internet governance system due to the passiveness and inability of states to formulate common ground on issues of Internet governance. The Internet as an idea and the conglomerate of various technical specifications has been developed by professional communities, mainly in the U.S. and later with participation from other countries. The system does not imply participation of states in decision-making by default because at the very beginning of the Internet and during its avalanche-like global proliferation in the 1990s its potential as a productive factor was not taken seriously.

The modern decentralized, unaccountable and non-legitimate system of Internet governance is a conflict-generating one by nature. This feature is defined by limitations on states' participation in decision-making and their understanding of digital sovereignty in traditional sovereignty terms. States are eager to specify the rules of the game in cyberspace to maximize their security level. This is an open road for nationalization of selected segments of the Internet in future.

The Internet's nationalization process is intensifying. Countries such as Russia [Kukkola, Ristolainen, 2018] aim at the full realization of their digital sovereignty. This implies further strengthening control over incoming, outgoing and stored data, addressing, and the technical development of the Internet. Attempts to establish a unified standard of Internet policy are considered a violation of digital sovereignty, which thus constrains the formulation of an international consensus [see Wouters, Verhelst, 2020].

Non-governmental organizations such as ICANN and ISOC play a significant part in Internet governance. These bodies secure some degree of consensus on Internet addressing and the standards in use but the situation is far from stable. These NGOs do not provide for the full participation of states in decision-making. ISOC is also characterized by its tendency to be influenced by large corporate units, mostly American ones. ICANN is criticized for being a U.S. tax resident and thus subject to the influence of the U.S. government, plus the inability of other states to exercise any form of control on decisions made concerning Internet addressing.

All in all, our proposals aimed at overcoming the system's disproportions are as follows.

First, the decentralized nature of the Internet is not likely to change in the near future if we consider existing mechanisms and practices. The examples of the unsatisfying results of UN and ITU-led processes prove the political nature of this feature. This factor prevents the formalization of a universally accepted consensus of any kind and thus the current state of affairs may be regarded as the 'best of the worst.'

Second, the accountability issue could be partly settled right now, by contrast with the decentralization problem. Despite the fact that ICANN and ISOC possess some accountability mechanisms, they do not match the current demand, especially in ISOC's case. By contrast with ICANN, ISOC's structure does not include any means to provide necessary feedback for state stakeholders. ICANN has established the GAC to fulfil this task; however, the GAC does not allow state members and other accountability addressees to influence the decision-making process. Thus, the first step toward greater accountability of the Internet governance system could be the establishment of a body with the same functionality as the GAC within ISOC.

However, even if ISOC were to establish a GAC-like mechanism, it would not be enough in terms of accountability. The next step would be to strengthen the authority of the ICANN GAC and the hypothetical ISOC equivalent by giving them voting rights when the board members are to be elected and when choosing strategic priorities. These measures would provide states with almost the same status as the other stakeholders, namely the media corporations, and thus would give a hand to the full realization of the UN declaration [UN 2003].

References

Becker M. (2019) When Public Principals Give Up Control Over Private Agents: The New Independence of ICANN in Internet Governance. *Regulation & Governance*, vol. 13, no 4, pp. 561–76. Available at: https://doi.org/10.1111/rego.12250.

Bradner S. (1996) Best Current Practice: Internet Standards Process: Revision 3. Available at: https://tools.ietf.org/html/rfc2026 (accessed 3 November 2020).

Bradshaw S., DeNardis L., Hampson F.O., Jardine E., Raymond M. (2016) The Emergence of Contention in Global Internet Governance. *Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance*. Global Commission on Internet Governance Research Volume Two. Center for International Governance Innovation/Chatham House. Available at: https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf (accessed 2 November 2020).

Bratton B.H. (2015) *The Stack: On Software and Sovereignty*. The MIT Press.

Bukht R., Heeks R. (2018) Opredeleniye, kontseptsiya i izmereniye tsifrovoy ekonomiki [Defining, Conceptualising and Measuring the Digital Economy]. *Vestnik mezhdunarodnykh organizatsiy* [International Organisations Research Journal], vol. 13, no 2, pp.143–72. Available at: https://doi.org/10.17323/1996-7845-2018-02-07 (in Russian).

Bygrave L. (2015) *Internet Governance by Contract*. Oxford University Press.

Cerf V. (1995) IETF and the Internet Society. Internet Society, 18 July. Available at: https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/ (accessed 8 July 2020).

European Union (EU) (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. *Official Journal of the European Union*, L 194/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1 (accessed 3 November 2020).

Franzese P. W. (2009) Sovereignty in Cyberspace: Can It Exist? *Airforce Law Review*, vol. 64, pp. 1–42. Available at: https://www.afjag.af.mil/Portals/77/documents/AFD-091026-024.pdf (accessed 3 November 2020).

Froomkin M.A. (2011) Almost Free: An Analysis of ICANN's 'Affirmation of Commitments.' *Journal on Telecommunications & High Technology Law*, vol. 9, pp. 187–234. Available at: http://www.jthtl.org/content/articles/V9I1/JTHTLv9i1.pdf (accessed 6 July 2020).

Haugen H.M. (2020) The Crucial and Contested Global Public Good: Principles and Goals in Internet Governance. *Internet Policy Review*, vol. 9, no 1, pp. 1–22. Available at: https://doi.org/10.14763/2020.1.1447.

Hilbrich S., Schwab J. (2018) Towards a More Accountable G20? Accountability Mechanisms of the G20 and the New Challenges Posed to Them by the 2030 Agenda. *International Organisations Research Journal*, vol. 13, no 4, pp. 7–38. Available at: https://doi.org/10.17323/1996-7845-2018-04-01.

International Telecommunication Union (ITU). (2012) Final Acts of the World Conference on International Communications (Dubai, 2012). Available at: https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf (accessed 6 July 2020).

Internet Corporation for Assigned Names and Number (ICANN). (2020a) Annex A-2: GNSO Guidance Process. Bylaws for Internet Corporation for Assigned Names and Numbers, as Amended 28 November 2019. Available at: https://www.icann.org/resources/pages/governance/bylaws-en/#annexA2 (accessed 6 July 2020).

Internet Corporation for Assigned Names and Number (ICANN). (2020b) ICANN Strategic Plan for Fiscal Years 2021–2025. Available at: https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf (accessed 6 July 2020).

Internet Society (ISOC). (n. d., a) Board of Trustees. Available at: https://www.internetsociety.org/board-of-trustees/ (accessed 3 November 2020).

Internet Society (ISOC). (n. d., c) Our Organization Members. Available at: https://www.internetsociety.org/about-internet-society/organization-members/list/ (accessed 3 November 2020).

Internet Society (ISOC). (n. d., d) Attend an Event. Available at: https://www.internetsociety.org/events/ (accessed 3 November 2020).

Internet Society (ISOC). (n. d., b) Organization Membership Levels. Available at: https://www.internetsociety.org/about-internet-society/organization-members/membership-levels/ (accessed 3 November 2020).

Istomin N.A. (2020) Priznaniye gosudarstvami pravomernosti deyatel'nosti ICANN po upravleniyu adresnym prostranstvom Interneta [State Recognition of ICANN's Internet Address Space Management Activities]. *Mezhdunarodnyy pravovoy kur'yer* [International Legal Courier]. Available at: http://inter-legal.ru/priznanie-gosudarstvami-pravomernosti-deyatelnosti-icann-po-upravleniyu-adresnym-prostranstvom-interneta (accessed 8 June 2020) (in Russian).

Jensen J.L. (2020) *The Medieval Internet: Power, Politics and Participation in the Digital Age*. Emerald Publishing Limited.

Kaila H., Tarp F. (2019) Can the Internet Improve Agricultural Production? Evidence From Viet Nam. *Agricultural Economics*, vol. 50, no 6, pp. 675–91. Available at: https://doi.org/10.1111/agec.12517.

Keohane R. (2011) Global Governance and Legitimacy. *Review of International Political Economy*, vol. 18, no 1, pp. 99–109. Available at: https://doi.org/10.1080/09692290.2011.545222.

Korchagin A., Deniskina A., Fateeva I. (2019) Lean and Energy Efficient Production Based on Internet of Things (IOT) in Aviation Industry. *E3S Web of Conferences*, vol. 110. Available at: https://doi.org/10.1051/e3sconf/201911002124.

Kukkola R., Ristolainen M. (2018) Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders.' Paper presented at the 17th European Conference on Cyber Warfare and Security ECCWS, Oslo. Available at: https://www.researchgate.net/publication/326292919_Projected_territoriality_A_case_study_of_the_infrastructure_of_Russian_%27digital_borders%27 (accessed 3 November 2020).

Liaropoulos A. (2013) Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *Journal of Information Warfare*, vol. 12, no 2, pp. 19–26. Available at: https://www.jstor.org/stable/26486852.

Liaropoulos A. (2016) Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics. *Journal of Information Warfare*, vol. 15, no 4, pp. 14–26.

Mueller M. (2017) *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge: Polity.

National Telecommunications and Information Administration (NTIA) (1998) Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers. 25 November. Available at: https://www.ntia.doc.gov/other-publication/1998/memorandum-understanding-between-us-department-commerce-and-internet-corporat (accessed 6 July 2020).

Naughton J. (2016) The Evolution of the Internet: From Military Experiment to General Purpose Technology. *Journal of Cyber Policy*, vol. 1, no 1, pp. 5–28. Available at: https://doi.org/10.1080/23738871.2016.1157619.

Nye J.S. (2010) Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School. Available at: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf (accessed 6 July 2020).

Nye J.S. (2014) The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series No 1, Centre for International Governance Innovation. Available at: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities (accessed 3 November 2020).

Nye J.S. (2017) Deterrence and Dissuasion in Cyberspace. *International Security*, vol. 41, no 3, pp. 44–7. Available at: https://doi.org/10.1162/ISEC_a_00266.

Organisation for Economic Co-operation and Development (OECD) (2017) Digital Economy Outlook 2017. Available at: https://dx.doi.org/10.1787/9789264276284-en.

Organisation for Economic Co-operation and Development (OECD) (2019) Vectors of Digital Transformation. Available at: OECD Digital Economy Papers No 273. https://www.sipotra.it/wp-content/uploads/2019/03/VECTORS-OF-DIGITAL-TRANSFORMATION.pdf (accessed 4 June 2020).

Paloque-Berges C., Schafer V. (2019) ARPANET (1969–2019). *Internet Histories*, vol. 3, no 1, pp. 1–14. Available at: https://doi.org/10.1080/24701475.2018.1560921.

Polatin-Reuben D., Wright J. (2014) An Internet With BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. Paper presented at the FOCI'14 Conference, San Diego, 18 August. Available at: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf (accessed 3 November 2020).

Pozdnyakova U., Mukhomorova I., Golikov V., Sazonov S., Pleshakov G. (2019) Internet of Things as a New Factor of Production in the Conditions of Digital Economy. *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT* (E. Popkova (ed.)). Springer.

President of Russia (2016) *Ukaz Prezidenta Rossiyskoy Federatsii ot 05.12.2016 № 646 Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii* [Decree of the President of the Russian Federation dated 05.12.2016 No 646 On Approval of the Doctrine of Information Security of the Russian Federation]. Available at: http://kremlin.ru/acts/bank/41460 (accessed 3 November 2020) (in Russian).

Qi A., Shao G., Zheng W. (2018) Assessing China's Cybersecurity Law. *Computer Law & Security Review*, vol. 34, no 6, pp. 1342–54. Available at: https://doi.org/10.1016/j.clsr.2018.08.007.

Ruggie J.G. (1982) International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order. *International Organization*, vol. 36, no 2, pp. 379–415. Available at: https://doi.org/10.1017/S0020818300018993.

Schmitt M.N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Shiroma Y., Afuso H., Suwa R., Kinjo A., Tonooka Y., Kaga T., Nagayama I., Tamaki S., Maharjan G. (2019) Development of Higher Yield and High-Quality Mango Production System Based on Internet of Things. *Electronics and Communications in Japan*, vol. 102, no 6, pp. 33–41. Available at: https://doi.org/10.1002/ecj.12170.

Sholte J.A. (2017) Polycentrism and Democracy in Internet Governance. *The Net and the Nation State* (U. Kohl (ed.)). Cambridge University Press. Available at: https://doi.org/10.1017/9781316534168.012.

Ukolov V., Cherkasov V. (2019) Development of Digital Economy Regulatory Environment in Supply Chains Operations. *International Journal of Supply Chain Management*, vol. 8, no 6. Available at: https://ojs.excelingtech.co.uk/index.php/IJSCM/article/view/4107/2069 (accessed 3 November 2020).

United Nations (UN). (2003) *Deklaratsiya printsipov Vsemirnoy vstrechi na vysshem urovne po voprosam informatsionnogo obshchestva Zheneva, 2003 g. Tunis, 2005. Postroyeniye informatsionnogo obshchestva – global'naya zadacha v novom tysyacheletii* [Declaration of Principles of the World Summit on the Information Society, Geneva, 2003 – Tunisia, 2005 Building the Information Society: A Global Challenge in the New Millennium]. Available at: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf (accessed 13 July 2020) (in Russian).

United Nations Conference on Trade and Development (UNCTAD). (2019) Value Creation and Capture: Implications for Developing Countries. Digital Economy Report 2019. Available at: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 3 July 2020).

van Horenbeeck M. (2018) The Future of Internet Governance and Cyber-Security. *Computer Fraud & Security*, no 5, pp. 6–8. Available at: https://doi.org/10.1016/S1361-3723(18)30042-3.

Wouters J., Verhelst A. (2020) Global'noye upravleniye v sfere kiberbezopasnosti: vzglyad s pozitsii mezhdunarodnogo prava i prava YES [Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives]. *Vestnik mezhdunarodnykh organizatsiy* [International Organisations Research Journal], vol. 15, no 2, pp. 141–72. Available at: https://doi.org/10.17323/1996-7845-2020-02-07 (in Russian).

Wu T.S. (1997) Cyberspace Sovereignty? The Internet and the International System. *Harvard Journal of Law & Technology*, vol. 10, no 3. Available at: http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech647.pdf (accessed 3 November 2020).

Zalnieriute M., Milan S. (2019) Internet Architecture and Human Rights: Beyond the Human Rights Gap. *Policy & Internet*, vol. 11, no 1, pp. 6–15. Available at: https://doi.org/10.1002/poi3.200.

Zeng J., Stevens T., Chen Y. (2017) China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty.' *Politics & Policy*, vol. 45, no 3, pp. 432–64. Available at: https://doi.org/10.1111/polp.12202.

Zhang L., Chen S. (2019) Tsifrovaya ekonomika Kitaya: vozmozhnosti i riski [China's Digital Economy: Opportunities and Risks]. *Vestnik mezhdunarodnykh organizatsiy* [International Organisations Research Journal], vol. 14, no 2, pp. 275–303. Available at: https://doi.org/10.17323/1996-7845-2019-02-11 (in Russian).