International Organisations Research Journal, 2021, vol. 16, no 3, pp. 7–33
Original article
doi:10.17323/1996-7845-2021-03-01

U.S. & China Approaches to Global Internet Governance: "New Bipolarity" in Terms of "The Network Society"[1, 2]

D. Degterev, M. Ramich, D. Piskunov

Denis Degterev – Dr. of Sc. (Political Science), PhD in Economics, Head, Department of Theory and History of International Relations, RUDN University; Professor, World Economy Department, MGIMO University; Professor, Department of European Studies; St. Petersburg State University; 6 Miklukho-Maklaya Ulitsa, Moscow, 117198, Russian Federation; degterev-da@rudn.ru

Mirzet Ramich – PhD candidate, Department of Theory and History of International Relations, RUDN University; 6 Miklukho-Maklaya Ulitsa, Moscow, 117198, Russian Federation; ramich_ms@mail.ru

Danil Piskunov – Student of the Department of Theory and History of International Relations, RUDN University; 6 Miklukho-Maklaya Ulitsa, Moscow, 117198, Russian Federation; piskunov_da@mail.ru

Abstract

From the perspective of power transition theory, the international relations system is gradually entering a phase of power transition, in which the United States, as a global hegemon, seeks to maintain the existing world order, while China seeks to establish alternative international mechanisms to reorganize the system of international relations and strengthen its own structural power. Cyberspace and the technological sphere are becoming the fields for non-violent competition between states, which makes the study of the global governance of cyberspace critical to the understanding of the outlines of the new bipolarity.

The analysis in this article is focused on U.S. and Chinese approaches to global governance of cyberspace through the prism of Manuel Castells' theory of network society. The authors assess the directions of U.S. and Chinese policy across four types of power in cyberspace: networking power, network power, networked power, and network-making power.

The authors conclude that the United States plays a crucial role across the four types of power at the expense of a decentralized model of Internet governance, which is based on the idea of "multi-stakeholderism." Non-governmental organizations (NGOs) and other entities play a decisive role in such a model. Nonetheless, China has already developed the necessary tools to reform the present system of global governance of cyberspace, based on a centralized model with a leading role for the United Nations (UN) as an international governance organization and with the state as the basic actor. The main beneficiaries of the centralized model are developing countries, which are unable to influence the global governance of cyberspace under the dominance of private companies based in the developed countries.

Keywords: U.S., China, global governance, cyberspace, "network society", "new bipolarity"

For citation: Degterev D., Ramich M., Piskunov D. (2021). U.S. China Approaches to Global Internet Governance: "New Bipolarity" in Terms of "The Network Society". *International Organisations Research Journal*, vol. 16, no 3, pp. 7–33 (in English). doi:10.17323/1996-7845-2021-03-01

[1] The reported study was funded by RFBR within research project No 20-514-93003 "Russia and China in the Global Political Space: Harmonization of National Interests in Global Governance."

[2] The article was submitted 10.04.2021.

Introduction

With the formation of a new bipolarity between China and the United States, issues of global governance gain new impetus. Nuclear deterrence has gradually reduced the relevance of hard power confrontation, and in this context new global political spaces are becoming increasingly important as arenas of geopolitical confrontation. Cyberspace is one such political dimension. It takes on special significance in view of the accelerated digitalization process against the background of COVID-19. The U.S. and China, as primary poles of power, promote their own approaches to global cyberspace governance to manage information flows and develop intergovernmental technological ecosystems. Global Internet governance is an important area of global governance. Cyberspace governance achieves its purpose by means of the production of global public goods to address failures in governments and other networks. The driving force of cyberspace refers to the principal promoter of the global governance of cyberspace or the main provider of public goods in cyberspace [Yan, 2019].

In the framework of power transition theory, the world is undergoing a power transition where China, as a revisionist emerging power, is challenging the U.S. as the dominant state [Chan, 2019; Degterev, Ramich, Cvyk, 2021]. In this article, the U.S.-China competition for the role of *rule maker* of global cyberspace governance is examined. This analysis of the U.S.-China rivalry draws on power transition theory according to which states compete to be the main provider of international public goods [Kugler, Organski, 1980; Organski, 1958]. Currently, the U.S. forms the core of the liberal world order and is the main provider of international public goods. However, growing dissatisfaction with the international system among developing states and China's potential reluctance to maintain the liberal world order in the event of a successful power transition create uncertainty about the future of the international system [Nye, 2020].

The two most relevant approaches to global Internet governance are, first, multistakeholderism, that is, a decentralized model of governance led by non-governmental organizations (NGOs) [Carr, 2015; Hofmann, 2016; Kleinwächter, 2007; Mueller, 2020; Strickling, Hill, 2017; Vasilkovsky, Ignatov, 2020] and second, a centralized model of governance with the leading role played by a state [Arsène, 2016; Bi, 2020; Cai, 2021; Galloway, Baogang, 2014; Hong, Harwit, 2020; Zeng, Stevens, Chen, 2017]. The former model is supported by the U.S. and other developed states, while the latter is encouraged by China and developing states. Various studies have extensively reviewed the principles and foundations of these two approaches. However, insufficient attention has been paid to the practical and theoretical aspects of the two countries' rivalry for leadership in global cyberspace governance.

The U.S. occupies a key role in cyberspace governance for several reasons. First, it was in the U.S. that the first protocols for the functioning of the Internet were established. Second, an Internet governance system is already in place in the U.S. – the Internet Corporation for Assigned Names and Numbers (ICAAN), a non-profit organization, was registered in California in 1998 [Demidov, 2017]. When ICAAN was established, it signed a memorandum of understanding with the U.S. Department of Commerce, which enshrined several functions within the jurisdiction of ICAAN; ICAAN remained accountable to the government of the U.S. [Vasilkovsky, Ignatov, 2020, p. 16] until 2016, when the management of top-level domain (TLD) and IP addresses came under its jurisdiction [ICAAN, 2016]. The primary objectives of the U.S. model are the function of management of critical infrastructure in hands of private companies and the development of an inclusive process of Internet governance with the participation of ICAAN and other NGOs.

A crucial contribution, which defined the basis of global Internet governance, was made during the World Summit on the Information Society (WSIS), held in two phases in 2003 and 2005. The term "global internet governance" was defined during the WSIS to mean that both

governmental and non-governmental actors, including public organizations and the scientific and technical community, can participate in the process of global governance. The key result of the summit was the creation of the Internet Governance Forum (IGF), which became a coordinating and advisory body [Van Eeten, Mueller, 2013, p. 724]. As a result of the WSIS, the principles and characteristics of a model that considers the perspectives of all interested parties – multistakeholderism – were shaped [Carr, 2015]. With the renewal of the IGF's mandate in 2015 the multistakeholder model with the participation of all interested parties was preserved for another 10 years [Yakushev, 2016].

China offers an alternative approach to global cyberspace governance. This approach is based on the principle of state sovereignty in the context of internal Internet governance. It limits the technological influence and role of non-state actors in cyberspace governance. From this point of view, the basis of global governance is the United Nations (UN) system and the decision-making process involves states on equal terms, while NGOs play advisory roles [Zinoveva, 2015, p. 116; Wang, 2020]. The principle of sovereignty in cyberspace, that is, control over the internal segment of the Internet, takes the central place in this approach. The foundation of China's approach is the idea of a community of common destiny for mankind in the network society based on "four principles" and "five suggestions" offered by Xi Jinping during the 2nd International Conference on Global Governance in 2015 [Li, Tang, 2020, p. 27].

In this article, we investigate the question of global cyberspace governance in the context of the theory of network society. In the network society, the main function of a government is to maintain control over the telecommunications industry and information flows. The methodological basis for this analysis is M. Castells' network society theory. The U.S. and Chinese approaches to global Internet governance are discussed and compared in relation to practical activity in the context of their strategic rivalry. The article concludes with a summary table that compares characteristics of the two approaches and an explanation of the new bipolarity concept in the context of global Internet governance.

Global Internet Governance Through the Prism of Network Society Theory

The methodological foundation of this analysis is the theory of network society described by M. Castells in *Communication Power* [2009]. The establishment and administration of power and power relations within a country has changed with the appearance of communication technologies. The basis of power, excluding violence and fear, is the control over minds and perceptions in a society. Such control is implemented through the construction of the image of the state, the meaning of power, and power relations in the consciousness of society. The key idea of the theory is that power is based on the control of communication and information, which embraces a "network society" [Castells, 2007].

The development of technologies promotes the development of global and state network societies. In the framework of network society theory, all nodes establishing a network are interconnected. In its turn, communication is managed by networks that include programmed values and protocols of communication.

Castells described four forms of power that explain the management of power in the global network society. The first is *networking power*, which refers to the power of the actors and organizations included in the networks that constitute the core of the global network. This form of power operates by exclusion/inclusion [Castells, 2011]. For instance, by developing social networks, information technology (IT) corporations maintain their power in the global network society. It allows them to use gate-keeping strategies to exclude users who do not accept values and protocols of communications programmed in that society.

The second form of power is *network power* constructed through the development of standards and protocols of communication. According to Castells, network power is constituted through the popularity of standards and rules of communication and the elimination of alternatives. This form of power operates by establishing global communication standards that are accepted by the majority of actors or nodes in a society [2011]. An example of this is the technological leadership of the western countries in the development of e-commerce services and technological standards. The main point of this leadership is the establishment of a western approach to global cyberspace governance. In fact, large IT companies form a single technological ecosystem offering many IT services with a view to limiting a user's ability to choose another technological ecosystem.

The third form of power is *networked power*. According to Castells, networked power, especially in a dominant network, is relational. A dominant actor exercising the most power seizes an opportunity to impose its will. This power is constructed through dominant mechanisms [2011]. It is worth mentioning that the U.S. uses this form of power to attach its rules and principles to the development of the Internet. International organizations such as ICAAN, the IGF, the WSIS, and the Internet Engineering Task Force (IETF), follow key principles of the U.S. approach.

The fourth form of power is *network-making power*. This power is based on the operation of two mechanisms: programming the goals of the network and managing mass communication. Programming provides an opportunity to define the goals, values, and ideas of a network. It is an essential part of the network because values and goals are products of a network's culture and are used in the process of communication. Network programming is about developing an identity and an ideology [Castells, 2011]. This type of power was applied in 2008 during Barack Obama's election campaign, the basis of which was communication through the Internet.

According to the theory, control over communication in the network society is an inherent attribute of state power, through which the image of the state itself is constructed. Power in the network develops at the individual, national and global level. The reason for technological decoupling between states is the dominance of several approaches in the framework of global governance, similar to the division of users choosing network ecosystems within a national market for technological solutions.

The U.S. Approach to Global Internet Governance: A Multistakeholder, Decentralized Model

As the country in which the Internet was born, the U.S. plays a crucial role in global Internet governance. The first time the U.S. expressed its views on global Internet governance was in the Statement of Policy on the Management of Internet Names and Addresses issued by the Department of Commerce in 1998. The Statement asserted that governance functions should be under the jurisdiction of private companies because the Internet is a decentralized system with respect to human rights and without supervision by any state [NTIA, 1998]. Thus, global cyberspace governance initially was seen as a decentralized system based on private companies and non-profit organizations.

The international strategy for cyberspace released by the Obama administration in 2011 followed the principle of freedom of the Internet, promoting a multistakeholder model of Internet governance within a non-state framework. According to the U.S. approach, the flows of information on the Internet cannot be limited and controlled by other states. The issue of critical resource management should have a multistakeholder decision-making process involving private organizations to ensure the stability and security of critical Internet infrastructure [The White House, 2011].

Cyberspace governance is based on a decentralized architecture consisting of non-governmental organizations and companies such as the IGF, ICAAN and the IETF [Strickling, Hill, 2017, p. 299]. ICAAN and the IETF are responsible for the technical aspects of governance. For example, the IETF is responsible for developing and updating basic technical standards for the Internet. All interested parties can participate in the organization. In the IGF, states are on an equal footing with other actors, leading to an erosion of the line between rule-makers and rule-takers in cyberspace [Hofmann, Katzenbach, Gollatz, 2017, p. 1410]. In the context of the theory of network society, these organizations constitute the third form of power – networked power. The activities of the IGF, the IETF, ICAAN are based primarily on the principle of multistakeholder participation, which contributes to the recognition of the U.S. approach.

A separate aspect of U.S. power in the network society is the administration of critical Internet resources. Governmental organizations, private companies, NGO, universities, and Internet providers are all actors that exercise the administration of critical Internet resources, including domain name system (DNS) root servers. The operators of 10 root servers are the U.S. Army, the U.S. Department of Defense (Network Information Center of Defense Information Systems Agency), NASA (Ames Research Center), the University of Southern California, the University of Maryland and NGO and Internet providers such as VeriSign, Cogent Communications, ICAAN, and the Internet Systems Consortium [IANA, 2021]. With such access to the administration of critical resources, the U.S. gains the power to develop and define rules of inclusion and other standards of the Internet.

In its 2018 National Cyber Strategy, under "Principle IV. Promoting American Influence" the U.S. condemns attempts to control the domestic Internet in violation of the principle of freedom on the Internet [Department of Defense, 2018]. This makes it possible for foreign telecommunications companies to penetrate domestic networks and extend foreign influence into a country's society. In its cyber strategy, the U.S. promotes the multistakeholder model of Internet governance and resists the development of a state-oriented model of cyberspace governance which seeks to maintain control over the Internet [Department of Defense, 2018].

During a U.S. House of Representatives hearing in 2012, representatives put forward a resolution concerning an alternative, state-oriented model of global Internet governance. The resolution stated that the model led by the International Telecommunication Union (ITU) would increase state control of global governance and the multistakeholder model promoted by the U.S. would lose force [U.S. Congress, 2012]. As a consequence of transferring administration rights to the ITU, one state would have one vote to express its will on issues of global Internet governance [DeNardis, 2014, p. 33].

The group of IT corporations known as GAFAM (Google, Apple, Facebook, Amazon, and Microsoft) plays a crucial role in the network power of the U.S. and the maintenance of its international leadership status in cyberspace. GAFAM leads the world in search services, social networking, e-commerce services, and operating system production [Moore, 2016, p. 15]. These companies have established an ecosystem of services that is used by states and societies. Google controls more than 60% of the world's search engine market [GlobalStats, 2021] while Facebook has 70% of the world's social media market, second only to social networks in a number of countries [GlobalStats, 2021a]. In turn, Apple, Google, Microsoft control more than 70% of the global operating system market [GlobalStats, 2021b].

Telecommunication companies conduct research and develop technical protocols for communication and operation of the social services on the Internet. In that way, technological corporations form a global network of influence on both the security of states and global society as a whole [Slaughter, 2009, p. 98]. A significant example of private companies' power is the case connected with the intelligence programme PRISM. The U.S. carried out PRISM with the participation of Google, Apple, Skype, Facebook and other big tech companies [Hill, 2014,

p. 87]. In the view of network society theory, IT corporations' monopolistic position is the basis for the first form of U.S. power – networking power.

The decentralized model and open cyberspace are preferred by the U.S. because they promote the expansion of U.S. influence in the context of technological dependence and information influence on cyberspace. The mass media, tech companies, and private companies managing information flows on the Internet are permanent tools for maintaining power in the network society.

The Budapest Convention on Cybercrime is among the strategic documents that serve as the basis of the U.S. model. The Convention not only works to harmonize the signatories' legislation but also establishes the right to collect and use data across borders without notifying relevant states. The Convention was ratified mainly by the countries with high gross national incomes, whereas developing states or countries of the Global South have largely refrained from ratification. With limitless access to data, developed states are obtaining data processed by AI algorithms that reveal weaknesses in developing states' technology companies. In this way, technology company leaders, receiving flows of processed information, can influence the competitiveness of national companies in particular and the development of the state as a whole.

Other international documents corresponding to the U.S. model of global governance include the WSIS Declaration of Principles [UN, 2003] and the Tunis Agenda for the Information Society [UN, 2005]. Both documents laid the foundation for the current system of global governance. Market forces are driving the development of the Internet. The Internet is recognized as an open space, and global governance is exercised with the participation of all interested parties.

The Global Multistakeholder Summit on the Future of Internet Governance, held in Brazil in 2014, adopted a document that included basic principles for multistakeholder governance and a road map for Internet governance [NETmundial, 2014]. Unlike the WSIS declaration, the final document of the Brazil summit dealt with national and regional Internet governance issues.

Thus, the U.S. implements its approach through multistakeholder organizations. It is responsible for adopting protocols and developing the Internet architecture. Finally, multistakeholder organizations are fora in which non-state actors participate on an equal footing with government representatives. The main functions of Internet governance are controlled by U.S.-registered non-profit organizations. The U.S. preserves the state system of global Internet governance and its influence within the system using the mechanisms listed above.

China's Approach to Global Cyberspace Governance: A Multilateral, Centralized Model

An examination of the Chinese approach to this issue must begin with the principles of domestic or national network regulation. While the development of the Internet and the information and communications technology (ICT) sphere has resulted in an increase in the role and influence of non-governmental actors on world politics and the national security of individual states, the issues of information and cybersecurity have become a priority for China. In China's 2010 White Paper the governance of the Internet is considered an important element of national security, and the infrastructure facilities, Internet sites, and the Internet in general located within the territory of China are under Chinese jurisdiction [PRC, 2010]. China's approach to cyberspace governance is based on maintaining legitimacy and economic growth [Jiang, 2010, p. 72].

The technological basis is an important element for the implementation of domestic policy in the information space. In 2016, China adopted the National Informatization Development

Strategy, which outlines several stages in the development of China as a "strong cyber power." According to this strategy, China intends to improve the competitiveness of Chinese technology companies in the global market and the development of an advanced mobile communications network, functioning on Chinese software and network applications, by 2025 [Ponka, Ramich, Yu, 2020, p. 385].

The domestic network is based on an ecosystem of applications from Chinese telecommunications companies. China's domestic companies (Alibaba, Tencent, Baidu, Huawei and China Mobile) are the pillars of public power, as they provide the search engine (Baidu), the social networks (Tencent), e-commerce (Alibaba), manufacturing of telecommunication equipment (Huawei), and mobile communications (China Mobile). These companies form the core of China's national network and have regulatory functions. As such, the Chinese government gets access to the management of the national segment of the Internet and, in terms of theory, regulates the communication networks. Thus, the state gains control over the technical functions of managing the Internet and provides social management in society based on the regulation of the content of information flows.

One aspect of sovereignty in cyberspace is the independence of the state from the products and services of foreign companies and the development of national telecommunications companies and infrastructure, including the development and use of national software, building a system of fiber optic cables, and data localization [Couture, Toupin, 2020, p. 56]. Moreover, the management of the Internet is aligned with social management and public administration traditions. With the development of ICTs, the social management system has been transformed from police surveillance and harsh repressive policies to the systemic ideological shaping of society to maintain the Party's credibility. Such policy results in controlling the Internet through blocking, censorship, and filtering on the one hand, and by disseminating ideological information on the other [Yang, 2014, p. 111]. Thus, China uses a state-oriented model of domestic Internet governance to maintain stability and produce ideas and images for transmission to society through communication networks.

The principles of administration of the domestic Internet are transmitted to the international level in China's strategies for global cyberspace governance. The theoretical basis of China's global governance is the "theory of a harmonious world" proposed by Hu Jintao and the concept of a "community with a shared future for mankind" proposed by Xi Jinping. The theory of a harmonious world considers the development of a society of states based on cooperation to ensure common development and security. According to this theory, the priority in resolving international disputes is given to the UN [Grachikov, 2020, p. 140]. At the same time, attention to the formation of a community with a shared future in cyberspace intensified during the pandemic, when people around the world began to spend most of their time online [Cai, 2021].

China's general framework for the policy in cyberspace is the Strategy for International Cooperation in Cyberspace [Ministry of Foreign Affairs of China, 2017]. The document notes the main principles of China's policy in cyberspace according to which it is necessary to ensure peace and security and to prevent an arms race and conflicts in cyberspace. A principle of sovereignty that includes the right to choose the model of network governance and the model of public policy on the Internet has a significant role in the Strategy. Additionally, the Strategy highlights shared governance of cyberspace as a principle in which the UN represents a key management tool. The conclusion highlights the principle of inclusive access, aimed at bridging the digital divide between developed and developing states. In the context of the network society theory, the network power of the Chinese government, realized through the activities of national telecommunication companies, is the main means of maintaining social stability and economic growth.

China's approach to global governance of cyberspace is characterized by the tasks set out in the Strategy, among which are the recognition of state sovereignty in information space, non-interference in the internal affairs of the state, and the establishment of a code of rules and principles of behaviour for states in cyberspace. Regarding the U.S., Chinese experts believe that developed countries led by the U.S. are pursuing a policy of network hegemony, establishing conditions in which developing countries are not involved in the global governance of the Internet [Li, Li, 2018, p. 15]. Under these conditions, developed countries and their technology corporations can control cyberspace within the framework of the multistakeholder model.

China defines global cyberspace governance as a multilateral, transparent system of Internet governance that operates within the UN system. In such a system, states play a defining role and non-state actors and stakeholders are given an advisory role. The distribution and co-management of critical information infrastructure, such as Internet root servers, is an important aspect of Internet governance [Li, Li, 2018, p. 18].

China's model of global Internet governance involves extending and applying international rules to the administration of cyberspace. A key role in such a model is given to states that have sovereignty over the internal segment of the Internet. The decision-making process takes place within the framework of the ITU and the UN system, in which developing and developed states can participate equally.

China's presence in the ITU is remarkable in terms of the broad participation of government, business, and the academic community [Negro, 2020, p. 109]. The Chinese government is represented by the Ministry of Industry and Information. More than 40 Chinese telecommunications companies represent the position of private organizations. The academic community is represented by more than 20 technical universities [ITU, 2021].

To achieve its goals, China develops cooperation within bilateral and multilateral fora, promotes the involvement of less developed states in the formation of global cyberspace governance, and builds coalitions of states.

In 2011, members of the Shanghai Cooperation Organization (SCO) ratified the Agreement on Cooperation in Ensuring International Information Security, defining such principles as non-interference in other states' information resources and the internationalization of global Internet governance [MFA Russia, 2009]. The Agreement marked a major step forward in the development of a common position of states, as the document established a regulatory framework of concepts defining key terminology for cyberspace, the identification of threats and risks, and consolidated the information sphere as a state jurisdiction area.

Moreover, the position of China on the establishment of a common legal regulation is similar to that of the Russian Federation. An agreement on cooperation in the field of international information security was signed between the governments of these two states [Government of the Russian Federation, 2015]. Russia has proposed two conventions to regulate the information space, observing the principles of sovereignty and the model of state management of the national segment of the Internet. The first is on Ensuring International Information Security [MFA Russia, 2011] and the second concerns the institutionalization of the safe operation and development of the Internet on the basis of equal participation of the international community in global Internet governance [Minkomsvyaz Russia, 2017] – both have been proposed in the UN.

The basic principles of the proposed conventions were taken into consideration in the SCO's submission of the International Code of Conduct for Information Security to the UN [Suvorov, 2020]. The adoption of unified codes of conduct within the UN would transform cyberspace from a "grey zone" of international politics into a comfortable legal field, which would avoid the consequences of geopolitical confrontation between the largest technological actors [Chen, 2020, pp. 95–7]. China and Russia prioritize collective regulatory mechanisms such as

the UN system and the ITU in global cyberspace governance. The UN is the central platform for the development of the International Information Security (IIS), the ITU is an alternative institution of cyberspace governance offering more sovereign control over the national segment of the Internet [Larionova, Shelepov, 2021].

Established by Beijing in 2014, the World Internet Conference in Wuzhen provided a forum for the exchange of views among states and participants looking for a revision of the current global governance paradigm. In 2015, Chinese leader Xi Jinping noted that the Internet should be regulated in accordance with the same principles as other areas of international interaction, thereby insisting on the key principles of China's policy on the issue. On the agenda for the 2019 and 2020 summits was the initiative to "build a community of shared future in cyberspace" [WIC, 2020]. This initiative focused on both economic and technological cooperation, including the dissemination of 5G technologies, and joint Internet governance, with the UN playing a leading role [WIC, 2020]. It aimed to unite developing countries to oppose the model of global cyberspace management based on U.S. principles [Hong, Harwit, 2020, p. 3].

China implements the objectives established in this approach through international governmental organizations as well as consultative and advisory platforms. Such fora coordinate a unified position on global cyberspace governance and the development of the Internet. As a result of the work of the above-mentioned multilateral mechanisms, a joint draft UN convention, SCO and BRICS (made up of Brazil, Russia, India, China and South Africa) declarations on IIS were adopted, as well as bilateral agreements on the establishment of codes of conduct in cyberspace.

Thus, the model of global cyberspace governance promoted by China is based on the principles of sovereignty, equal participation of all states in the decision-making process, and the leading role of the UN in the administration of critical infrastructure and cyberspace. Such a model of governance complies with China's state-level policies.

The accelerating pace of digitalization makes it necessary for China to simultaneously address several challenges: to shape an image of a responsible state in the international arena, to promote its technology companies in the global market, to improve cyberspace management at the national level, and to create a favourable environment for development at the international level [Zhu, Liu, 2021].

The Practical Aspects of U.S.-Chinese Rivalry in Cyberspace

Cyberspace has become one of the key fields of strategic rivalry between the U.S. and China. Telecommunication corporations play an important role in the struggle for leadership in cyberspace, as they are also drivers of economic development and core actors in cyberspace [Danilin, 2020, p. 109]. Thus, the U.S. and China both pursue policies that limit the influence of telecommunications companies due to threats posed to national security. Within the framework of the theory of the network society, the state seeks the consolidation of control over the flow of information and communication protocols between network nodes.

ICAAN plays a key role in global cyberspace governance. U.S. and Chinese representatives are actively involved in the activities of this NGO. Among the 75 companies accredited as generic top-level domain (gTLD) registrars[3], 46 are U.S. companies [ICAAN, n. d., a]. The government advisory committee includes three representatives from the National Telecommunications and Information Administration and two experts from the U.S. Department of Commerce. The Root Server System Advisory Committee, which also participates in shaping NGO

[3] gTLD is one of the categories of top-level domains (TLDs) maintained by the Internet Assigned Numbers Authority (IANA) for use in the Domain Name System of the Internet.

policy, includes representatives of the root server operating companies [ICAAN, n. d., c]. On the other hand, eight Chinese companies are accredited by ICAAN [ICAAN, n. d., a]. There are four representatives from the Ministry of Industry and Information Technology of China and two researchers from the Chinese Academy of Information and Communication Technology on the Government Advisory Committee [ICAAN, n. d., c.]

As part of its information security system, China applies information flow filtering and bans foreign companies. The key element of such a system is a firewall, the purpose of which is to provide protection from external threats [Ponka, Ramich, Yu, 2020]. The ban covers such companies as Facebook (including Instagram, WhatsApp, Messenger), Google (including all Google services), Twitter, Snapchat, Dropbox, and others. Other corporations are forced to comply with a rigid system of application rules. For example, Apple had to exclude a number of applications from the AppStore due to their impact on the national security of China, including HKMap Live, Quartz, and Clubhouse. The first two apps were used by protesters in 2019 in Hong Kong. In addition to limiting foreign influence within its information space, China has restricted the use of Windows software in government computer systems, where the alternative is Ubuntu Kylin, based on the Linux OS. China is developing Harmony OS as an alternative software for mobile devices. Thus, China limits the influence of social networks, news agencies, and foreign IT companies on its society and bans the use of applications, software, and equipment that collect and process user data and can influence social attitudes in society.

In return, during the trade war, the U.S. banned applications, social networks, e-commerce services, and the use of equipment of Chinese companies that had links to the People's Liberation Army (PLA) due to the threat to U.S. national security. The policy of sanctions and blocking against Chinese companies began in 2018 in the first phase of the trade war, when the U.S. Department of Commerce adopted a ban on the export of component parts and software needed for ZTE's telecommunications equipment [BIS, 2018]. In addition, the U.S. Department of Defense has published a list of companies that directly or indirectly interact with the PLA [Department of Defense, 2021]. The list includes Huawei, China Telecom, China Mobile and Xiaomi. This was the reason for sanctions against Huawei on the export of components and the use of services of the Google ecosystem in devices manufactured under the company's brand. Huawei was banned from deploying its hardware in the U.S., mainly for 5G infrastructure and video surveillance. On the same basis, the U.S. Federal Communications Commission rejected China Mobile's application to provide mobile telecommunications service in the U.S. [FCC, 2019]. In January 2021, Xiaomi was added to the blacklist of Chinese companies cooperating with the PLA. This, in turn, led to a ban on the export of technology of American companies and investments. In March 2021, Xiaomi was able to successfully appeal the blacklisting of the company and thus succeeded in getting the investment restrictions lifted [Xiaomi, 2021]. The appeal was the first such precedent in the U.S.-China trade war.

In addition to the above-mentioned restrictions on the activities of Chinese technology giants, the U.S. has banned the operation of Chinese e-commerce services, applications and social networks. In the first phase, the social networks WeChat (Tencent) and Tiktok (ByteDance) were banned by the decree of U.S. president Donald Trump [Executive Office of the President, 2020]. The capitalization of the companies fell by $100 million [Dmitriev, 2020, p. 72]. Similar measures were applied to the non-bank payment systems Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay and WPS Office [Executive Office of the President, 2021]. In both cases, sanctions against applications were justified on the grounds that telecommunications companies could collect and process vast amounts of user information (big data) as well as impose censorship on political content posted by users. Chinese experts have described the ongoing rivalry in the technology space as a "digital cold war," the

outcome of which will determine which approach will dominate global Internet governance in the coming decades [Xu, 2021].

Another relevant issue in the U.S.-China rivalry is the competition between technological companies for the distribution of 5G technologies. The leaders in the deployment of 5G equipment are Huawei, ZTE, Ericsson and Nokia. For example, Huawei technology is used and tested in 68 countries, while another Chinese company, ZTE, provides its 5G equipment to 28 countries. On the other hand, European companies Ericsson and Nokia cooperate with 42 and 46 countries, respectively. Although U.S. companies are not directly involved in the global race to deploy 5G networks, the U.S. supports European partners through sanctions pressure on Chinese companies, acting as a united front of developed countries.

In August 2020, competition between companies intensified after Mike Pompeo announced the implementation of the Clean Network Initiative, the key goal of which is to limit the activities of Chinese companies in five areas – provision of ICT services, installation and use of Chinese software applications, storage and processing of cloud data, and building a fiber-optic cable system [Department of State, 2020]. Countries that join this initiative are reducing the presence of Chinese telecommunications companies in their markets and rejecting Chinese 5G technologies. According to the U.S. Department of State, about 53 states have joined the programme, including North Atlantic Treaty Organization (NATO) and European Union (EU) states and members of the Five Eyes alliance [Department of State, 2020]. The digital cold war between the U.S. and China began with the adoption of this programme [Xu, 2021, p. 19].

The adoption of the programme has had an impact on the activities of Chinese companies in the world. In 2019, Huawei was developing 5G networks in Greece and had planned to launch commercial use of the networks in 2020 [Michalopoulos, 2019]. But in September 2020, after Pompeo's visit, Greece joined the programme and opted for Ericsson [Department of State, 2020]. A similar situation can be observed in many of the states that have joined the U.S. programme. In addition, the EU has developed a 5G security toolbox, which defines standards and security criteria for 5G networks [EC, 2020]. This will give Ericsson and Nokia an advantage in the European 5G market. The programme identifies companies that offer services and equipment that do not threaten the security of the state; it also outlines the criteria and security measures to prevent the entry of high-risk suppliers into the market.

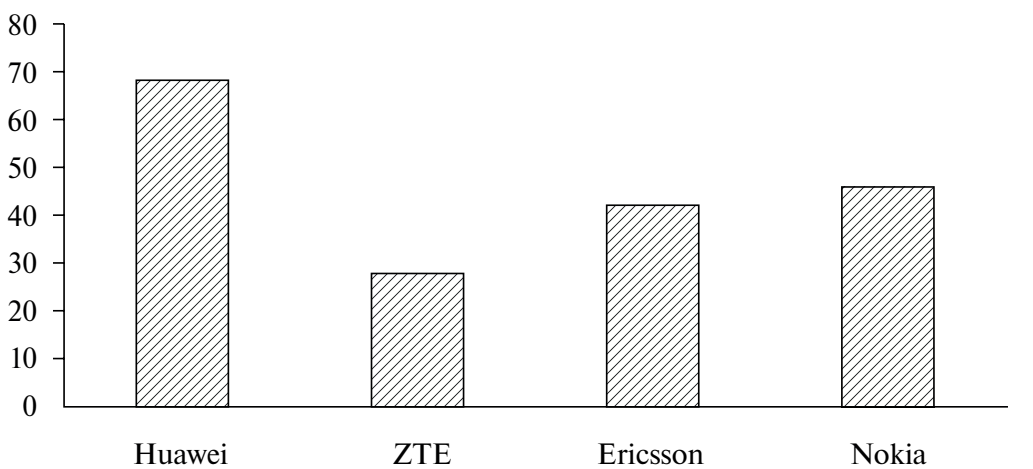

Fig. 1. Number of Countries That Have Signed 5G Agreements

Source: [Ericsson, 2021; Huawei, 2021; Nokia, 2021; ZTE, 2021].

Thus, the problem of cyberspace management in the framework of power in the network society comes to the fore in the new bipolar rivalry between the U.S. and China. The adoption of either model will ensure the absolute leadership and influence of respective power in the world. The U.S., as a hegemon both within the traditional system of international relations and within cyberspace, maintains and develops the existing model of power "on the Internet" and "through the Internet" and this is supported by developed countries. China unites developing countries, interested in the legitimization and equalization of the rights of all countries in global governance [Zhao, 2021, pp. 50–1]. Despite this, it is worth acknowledging that Chinese experts propose to reform the international system of cyberspace management "according to the Chinese model" [Zhao, 2021, p. 59].

The Outlines of the Global Cyberspace Governance System: Competing Approaches

Table 1 provides a visual comparison of the differences between the approaches of the U.S. and China to the global governance of cyberspace. China has already formed a complete set of alternative tools to implement its approach to global governance in cyberspace, while the U.S. seeks to use the already established fora to maintain a leading position in this political space.

The existing model for global governance of cyberspace operates on principles that were developed at the end of the 20th century. The administration and development of the Internet and the ICT sphere is ensured through market mechanisms, that is, through interaction between non-state actors such as ICAAN, VeriSign, Cogent Communications, and others. Moreover, the principles of a free and open Internet established by the foundation of ICAAN allow U.S. technology corporations and media to spread their influence, thereby providing a unique advantageous environment for the U.S. in the global governance of cyberspace. The main beneficiaries of the decentralized model are developed countries, where the world's largest IT corporations are located, which allows them to use the "power in the network" to promote their interests.

China, on the other hand, proposes an alternative approach in which the role of market forces is much smaller. The domestic network administration processes are carried out by the state in accordance with its internal laws. Global Internet governance issues should primarily be resolved within the UN system, in the ITU. This would prevent technology companies from influencing global governance issues and ensure equal participation by all states. At this stage, China is establishing alternative platforms to promote its position among developing countries, including the World Internet Conference in Wuzhen.

The inevitability of the transformation of the system of global cyberspace management is evidenced by the ratio of Internet users: residents of developed countries account for about one third of the total number of Internet users, while developing countries account for two thirds [Li, 2020]. At the same time, about half of the population of developing countries does not have access to the Internet, which means that simultaneously with digitalization, the share of these countries will increase and there will be increasing support for Chinese ideas to transform the international system of cyberspace governance.

The COVID-19 pandemic accelerated the process of digitalization and revealed the vulnerabilities of the existing system of global cyberspace governance. States were unprepared for the new normalcy of people spending more time online than offline. This has given rise to the phenomenon of "digital authoritarianism" and once again proved the danger of a digital divide between developed and developing countries [Cai, Wang, 2021, pp. 5–8]. The crisis has opened

new opportunities for the U.S. and China to implement their global projects in the digital space, which has led to a new round of competition in the context of a new bipolarity.

Table 1. Comparison of Global Cyberspace Governance Models

	U.S.	**China**
Internet governance mode	Multistakeholder model of cyberspace governance with broad participation of non-governmental, private, and public organizations (multistakeholder)	Multilateral model of cyberspace governance with the leading role of states within the UN system (multilateral)
Information environment governance model	Open Internet space based on a decentralized structure	State-oriented model with an emphasis on sovereignty
Key authorities in cyberspace governance	ICAAN, IETF	UN/ITU
International Internet governance platform	Internet Governance Forum (IGF)	World Internet Conference in Wuzhen
Position papers	**National level:** U.S. National Cybersecurity Strategy 2011 U.S. National Cybersecurity Strategy 2018 **International level:** Budapest Convention on Combating Cybercrime The Declaration of Principles "Building an Information Society: A Global Challenge in the New Millennium" Tunisian Programme for the Information Society The final document of the World Multilateral Summit in Brazil 2014	**National level:** China White Paper International Strategy for Cooperation in Cyberspace Informatization and Development Strategy **International level:** Agreement on Cooperation in the Field of Ensuring International Information Security of the SCO Convention on International Information Security 2011 Convention on the Safe Functioning and Development of the Internet 2017
The role of telecommunications companies	Telecommunications companies as a key actor in the development and cyberspace governance	Telecommunications companies can be actors of state policy in cyberspace

Source: Compiled by the authors.

Conclusion

This article explored the problem of competition between the U.S. and Chinese approaches to global governance through the prism of Castells' theory of the network society. According to the theory, the power of the state undergoes changes in a technological context and receives new tools for its implementation. As a result, we can draw the following conclusions.

In the space of network power, where the competition is for the establishment of a global network society in which the actors implement the strategy of geotaping – switching on and off from the global network – the position of leader is occupied by the U.S. due to the current

near-monopoly status of GAFAM corporations in the technology markets. China is building an alternative network operating on its application ecosystem, which has no global distribution but reduces the dependence of the national network on the international context.

Similarly, the U.S. leads in networking power, where the competition between the two powers is for determining communication protocols, principles for managing critical Internet resources, and implementing the domain address distribution function, as most of these functions are currently shared between organizations based in the U.S. and developed countries. China seeks to reshape the existing order and seeks a state-driven, UN-led critical infrastructure management function.

Control over networked power is carried out through the establishment of institutions of global governance of cyberspace. Existing institutions of global Internet governance (ICAAN, the IGF, the WSIS, and the IETF) operate according to the principles of the U.S. global governance model. On the other hand, China promotes its institutions and bodies of global Internet governance, while establishing an alternative choice and a basis for the coexistence of the two systems.

The U.S. and China seek the ability to define the principles of communication in the global network and to set goals and directions for global interaction for leadership in network-making power. Each state establishes its own network based on the principles of global cyberspace governance that give them the most room for development in the future. All countries of the world have to make choices in the context of the formation of a new bipolarity and thus are participants in such networks.

References

Arsène S. (2016) Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic World Order? *China Perspectives*, vol. 106, no 2, pp. 25–35. Available at: https://doi.org/10.4000/chinaperspectives.6973.

Bi S. (2020) Yingdui "Niquanqiuhua" Zhongguo Quanqiu Wangluokongjian Zhili Linian De Chuanbo [Responding to "Counter-Globalization": The Spread of China's Global Cyberspace Governance Philosophy]. China Publishing, pp. 50–3 (in Chinese).

Bureau of Industry and Security (BIS) (2018) ZTE Order Terminating Denial Order. Available at: https://www.bis.doc.gov/index.php/documents/pdfs/2246-zte-order-terminating-denial-order (accessed 6 April 2021).

Cai C. (2021) Promoting the Building of a Community of Destiny in Cyberspace *China Social Science Journal*, vol. 1, no 8, pp. 10–2 (in Chinese).

Cai C., Wang T. (2021) Global Cyber Governance in the Context of COVID-19: Opportunities and Challenges. *International Forum*, vol. 23, no 1, pp. 3–17 (in Chinese).

Carr M. (2015) Power Plays in Global Internet Governance. *Millennium*, vol. 43, iss. 2, pp. 640–59. Available at: https://doi.org/10.1177%2F0305829814562655.

Castells M. (2007) Communication, Power and Counter-Power in the Network Society. *International Journal of Communication*, vol. 1, pp. 238–66. Available at: https://ijoc.org/index.php/ijoc/article/view/46/35 (accessed 18 August 2021).

Castells M. (2009) *Communication Power*. Oxford University Press.

Castells M. (2011) Network Theory: A Network Theory of Power. *International Journal of Communication*, vol. 5, pp. 773–87. Available at: https://ijoc.org/index.php/ijoc/article/view/1136/553 (accessed 18 August 2021).

Chan S. (2019) More Than One Trap: Problematic Interpretations and Overlooked Lessons From Thucydides. *Journal of Chinese Political Science*, vol. 24, no 1, pp. 11–24. Available at: http://dx.doi.org/10.1007/s11366-018-9583-2.

Chen W. (2020) Cyberspace and Its Security in a Geopolitical Context. *Academia*, vol. 261, no 2, pp. 87–97 (in Chinese).

Couture S., Toupin S. (2020) Chto oznachaet ponjatie "suverenitet" v cifrovom mire? [What Does the Notion of "Sovereignty" Mean When Referring to the Digital?] *International Organisations Research Journal,* vol. 15, no 4, pp. 48–69. Available at: https://doi.org/10.17323/1996-7845-2020-04-03 (in Russian).

Danilin I.V. (2020) Vlijanie cifrovyh tehnologij na liderstvo v global'nyh processah: ot platform k rynkam? [The Impact of Digital Technologies on Leadership in Global Processes: From Platforms to Markets?] *MGIMO Review of International Relations*, vol. 13, no 1, pp. 100–16. Available at: https://doi.org/10.24833/2071-8160-2020-1-70-100-116 (in Russian).

Degterev D.A., Ramich M.S., Cvyk V.A (2021) U.S.-China: "Power Transition" and the Outlines of "Conflict Bipolarity." *Vestnik RUDN: International Relations*, vol. 21, no 2, pp. 210–31. Available at: https://doi.org/10.22363/2313-0660-2021-21-2-210-231 (in Russian and English).

Demidov O. (2017) *Global'noye upravleniye Internetom i bezopasnost' v sfere ispol'zovaniya IKT: Klyuchevyye vyzovy dlya mirovogo soobshchestva* [*Global Internet Governance and ICT Security: Key Challenges for the Global Community*]. Moscow: Al'pina Publisher (in Russian).

Denardis L. (2014) *The Global War for Internet Governance*. Yale University Press. Available at: https://www.jstor.org/stable/j.ctt5vkz4n.

Dmitriev S. (2020) Amerikano-kitajskoe tehnologicheskoe sopernichestvo: ot "vysokomerija" k bojkotu [U.S.-China Technological Rivalry: From "Arrogance" to Boycott]. *World Economy and International Relations*, vol. 64, no 12, pp. 70–7. Available at: https://doi.org/10.20542/0131-2227-2020-64-12-70-77 (in Russian).

Ericsson (2021) Available at: https://www.ericsson.com/en (accessed 6 April 2021).

European Commission (EC) (2020) Secure 5 Networks: Questions and Answers on the EU Toolbox. 29 July. Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127 (accessed 6 April 2021).

Executive Office of the President (2020) Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain. Executive Order 13942, 6 August. Available at: https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency (accessed 6 April 2021).

Executive Office of the President (2021) Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies. Executive Order 13971, 5 January. Available at: https://www.federalregister.gov/documents/2021/01/08/2021-00305/addressing-the-threat-posed-by-applications-and-other-software-developed-or-controlled-by-chinese (accessed 6 April 2021).

Federal Communications Commission (FCC) (2019) FCC Denies China Mobile Telecom Services Application. News Release, 9 May. Available at: https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application (accessed 6 April 2021).

Galloway T., Baogang H. (2014) China and Technical Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance Within ICANN, WSIS and the IGF. *China: An International Journal*, vol. 12, no 3, pp. 72–93. Available at: https://muse.jhu.edu/article/563560 (accessed 19 August 2021).

GlobalStats (2021a) Browser Market Share Worldwide. Available at: https://gs.statcounter.com/ (accessed 6 April 2021).

GlobalStats (2021b) Social Media Stats Worldwide. Available at: https://gs.statcounter.com/social-media-stats (accessed 6 April 2021).

GlobalStats (2021c) Operating System Market Share Worldwide. Available at: https://gs.statcounter.com/os-market-share#monthly-202002-202102-bar (accessed 6 April 2021).

Grachikov E.N. (2020) China in Global Governance: Ideology, Theory, and Instrumentation. *Russia in Global Affairs*, no 4, pp. 132–53. Available at: http://dx.doi.org/10.31278/1810-6374-2020-18-4-132–153.

Government of the Russian Federation (2015) Soglasheniye mezhdu Pravitel'stvom Rossiyskoy Federatsii i Pravitel'stvom Kitayskoy Narodnoy Respubliki o sotrudnichestve v oblasti informatsionnoy bezopasnosti [Agreement Between the Russian Government and the Government of the People's Republic of China on Co-

operation in the Field of International Information Security]. Available at: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (accessed 6 April 2021) (in Russian).

Hill R. (2014) Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means? *The Evolution of Global Internet Governance* (R. Radu, J.M. Chenou, R. Weber (eds)). Berlin: Springer. Available at: https://doi.org/10.1007/978-3-642-45299-4_5.

Hofmann J. (2016) Multi-Stakeholderism in Internet Governance: Putting a Fiction Into Practice. *Journal of Cyber Policy*, vol. 1, iss. 1, pp. 29–49. Available at: https://doi.org/10.1080/23738871.2016.1158303.

Hofmann J., Katzenbach C., Gollatz K. (2017) Between Coordination and Regulation: Finding the Governance in Internet Governance. *New Media & Society*, vol. 19, iss. 9, pp. 1406–23. Available at: http://dx.doi.org/10.1177/1461444816639975.

Hong Y., Harwit E. (2020) China's Globalizing Internet: History, Power, and Governance. *Chinese Journal of Communication*, vol. 13, iss. 1, pp. 1–7. Available at: https://doi.org/10.1080/17544750.2020.1722903.

Huawei (n. d.) Available at: https://www.huawei.com (accessed 6 April 2021).

Internet Assigned Numbers Authority (IANA) (n. d.) List of Root Servers. Available at: https://www.iana.org/domains/root/servers (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (2016) NTIA IANA Functions' Stewardship Transition. Available at: https://www.icann.org/stewardship (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., a) List of Accredited Registrars. Available at: https://www.icann.org/en/accredited-registrars?filter-letter=a&sort-direction=desc&sort-param=name&page=1 (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., b) GAC Membership. Available at: https://gac.icann.org/about/members# (accessed 6 April 2021).

Internet Corporation for Assigned Names and Numbers (ICAAN) (n. d., c.) Root Server System Advisory Committee. Available at: https://www.icann.org/groups/rssac (accessed 6 April 2021).

International Telecommunication Union (ITU) (n. d.) China. Available at: https://www.itu.int/online/mm/scripts/gensel9?_ctryid=1000100502 (accessed 6 April 2021).

Jakushev M. (2016) Itogi vsemirnoy vstrechi na vysshem urovne po voprosam informatsionnogo obshchestva [Results of the World High-Level Meeting on the Information Society]. *Pul's Kibermira*, vol. 19, no 1. Available at: http://www.pircenter.org/articles/2009-itogi-vsemirnoj-vstrechi-na-vysshem-urovne-po-voprosam-informacionnogo-obschestva (accessed 6 April 2021) (in Russian).

Jiang M. (2010) Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*, vol. 30, no 2, pp. 71–89. Available at: http://dx.doi.org/10.1353/sais.2010.0006.

Kleinwächter W. (ed) (2007) *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment*. Berlin: Marketing für Deutschland.

Larionova M., Shelepov A. (2021) Formirujushhiesja mehanizmy regulirovanija cifrovoj jekonomiki. Riski i vozmozhnosti dlja mnogostoronnej sistemy globalnogo upravlenija [Emerging Regulation for the Digital Economy: Challenges and Opportunities for Multilateral Global Governance]. *International Organisations Research Journal*, vol. 16, no 1, pp. 29–63. Available at: https://doi.org/10.17323/1996-7845-2021-01-02 (in Russian and English).

Li C., Li H. (2018) Global Governance of the Internet Based on Sovereignty in Cyberspace. *E-Government*, vol. 185, no 5, pp. 9–17 (in Chinese).

Li H. (2020) "Digital Silk Road" and the Reconstruction of Global Cyberspace Governance. *International Forum*, vol. 21, no 6, pp. 42–4 (In Chinese).

Li Z., Tang R. (2020) Multi-Stakeholder Model: Path to Build Global Internet Governance System. *Media Observer*, vol. 444, no 12, pp. 21–8 (in Chinese).

Michalopoulos S. (2019) Huawei Official: 5G Is a "Historic" Opportunity for Greece and Cyprus. Euroactiv, 30 July. Available at: https://www.euractiv.com/section/5g/news/huawei-official-5g-is-a-historic-opportunity-for-greece-and-cyprus/ (accessed 6 April 2021).

Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Minkomsvyaz Russia) (2017) Kontseptsiya konventsii OON (ili kontseptsiya bezopasnogo funktsionirovaniya i razvitiya seti Internet) [The Concept of Safe Functioning and Development of the Internet]. Available at: https://digital.gov.ru/uploaded/files/prilozheniekontseptsiikonventsiioon.docx (accessed 6 April 2021) (in Russian).

Ministry of Foreign Affairs of People's Republic of China (PRC) (2017) International Strategy of Cooperation on Cyberspace. Available at: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (accessed 6 April 2021).

Ministry of Foreign Affairs of the Russian Federation (MFA Russia) (2009) Mnogostoronniye dogovory [Multilateral Agreements]. Available at: https://www.mid.ru/ru/foreign_policy/international_contracts/multilateral_contract/-/storage-viewer/multilateral/page-1/50243 (accessed 6 April 2021) (in Russian).

Ministry of Foreign Affairs of the Russian Federation (MFA Russia) (2011) Konventsiya ob obespechenii mezhdunarodnoy informatsionnoy bezopasnosti (kontseptsiya) [Convention on International Information Security]. 22 September. Available at: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (accessed 6 April 2021) (in Russian).

Moore M. (2016) Tech Giants and Civic Power. Centre for the Study of Media, Communication & Power, King's College London. Retrieved February, vol. 5, pp. 88. Available at: https://www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf (accessed 19 August 2021).

Mueller M.L. (2020) Against Sovereignty in Cyberspace. *International Studies Review*, vol. 22, iss. 4, pp. 779–801. Available at: https://doi.org/10.1093/isr/viz044.

Negro G. (2020) A History of Chinese Global Internet Governance and Its Relations With ITU and ICANN. *Chinese Journal of Communication*, vol. 13, iss. 1, pp. 104–21. Available at: https://doi.org/10.1080/17544750.2019.1650789.

NETmundial (2014) Multistakeholder Statement. The Global Multistakeholder Meeting on the Future of Internet Governance. Available at: https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (accessed 6 April 2021).

National Telecommunications and Information Administration (NTIA) (1998) Statement of Policy on the Management of Internet Names and Addresses. 5 June. Available at: https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (accessed 6 April 2021).

Nokia (n. d.) Available at: https://www.nokia.com (accessed 6 April 2021).

Nye J.S. (2020) Power and Interdependence With China. *The Washington Quarterly*, vol. 43, iss. 1, pp. 7–21. Available at: https://doi.org/10.1080/0163660X.2020.1734303.

Organski A.F.K. (1958) *World Politics*. New York: A. Knopf.

Organski A.F.K., Kugler J. (1980) *The War Ledger*. Chicago: The University of Chicago Press.

People's Republic of China (PRC) (2010) White Paper on the Internet in China. Available at: https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm (accessed 6 April 2021).

Ponka T., Ramich M., Yu U. (2020) Informatsionnaya politika i informatsionnaya bezopasnost' KNR:razvitiye, podkhody i realizatsiya [Information Policy and Information Security of PRC: Development, Approaches and Implementation]. *Vestnik RUDN: International Relations*, vol. 20, no 2, pp. 382–94. Available at: https://doi.org/10.22363/2313-0660-2020-20-2-382-394 (in Russian).

Shen H. (2016) China and Global Internet Governance: Toward an Alternative Analytical Framework. *Chinese Journal of Communication*, vol. 9, iss. 3, pp. 304–24. Available at: https://doi.org/10.1080/17544750.2016.1206028.

Slaughter A.M. (2009) America's Edge: Power in the Networked Century. *Foreign Affairs*, vol. 88, no 1, pp. 94–113. Available at https://www.jstor.org/stable/20699436 (accessed 6 April 2021).

Strickling L.E., Hill J.F. (2017) Multi-Stakeholder Internet Governance: Successes and Opportunities. *Journal of Cyber Policy*, vol. 2, iss. 3, pp. 296–317. Available at: https://doi.org/10.1080/23738871.2017.1404619.

Suvorov A. (2020) Sovremennye realii kiberprostranstva: Rossija kak vedushhij igrok v obespechenii mezhdunarodnoj informacionnoj bezopasnosti [The Present Realities of Cyberspace: Russia as a Leading Player in

International Information Security]. PIR-Centre, 2 November. Available at: http://www.pircenter.org/blog/view/id/433 (accessed 6 April 2021) (in Russian).

The White House (2011) International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 6 April 2021).

United Nations (UN) (2003) Deklaratsiya printsipov. Postroyeniye informatsionnogo obshchestva – global'naya zadacha v novom tysyacheletii: Vsemirnaya vstrecha na vysshem urovne po voprosam informatsionnogo obshchestva. Zheneva, 2003 g.–Tunis, 2005 g. [Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium. World Summit on the Information Society. Geneva, 2003–Tunis, 2005]. Available at: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (accessed 6 April 2021) (in Russian).

United Nations (UN) (2005) Tunisskaya programma dlya informatsionnogo obshchestva: Vsemirnaya vstrecha na vysshem urovne po voprosam informatsionnogo obshchestva. Zheneva, 2003 g.–Tunis, 2005 g [Tunis Agenda for the Information Society. World Summit on the Information Society. Geneva, 2003–Tunis, 2005]. Available at: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (accessed 6 April 2021) (in Russian).

United States Congress (2012) International Proposals to Regulate the Internet. Committee on Energy and Commerce, 31 May. Available at: https://archive.org/details/gov.gpo.fdsys.CHRG-112hhrg79558/page/n11/mode/2up (accessed 6 April 2021).

United States Department of Defense (2018) Summary: Department of Defense Cyber Strategy. Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed 6 April 2021).

United States Department of Defense (2021) List of Additional Companies, in Accordance With Section 1237 of FY99 NDAA. News Release, 14 January. Available at: https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/ (accessed 6 April 2021).

United States Department of State (n. d.) The Clean Network. Available at: https://2017-2021.state.gov/the-clean-network/index.html (accessed 6 April 2021).

van Eeten M.J.G., Mueller M. (2013) Where Is the Governance in Internet Governance? *New Media & Society*, vol. 15, iss. 5, pp. 720–36. Available at: https://doi.org/10.1177%2F1461444812462850.

Vasilkovsky S., Ignatov A. (2020) Upravlenie Internetom: sistemnye disproporcii i puti ih razreshenija [Internet Governance: System Imbalances and Ways to Resolve Them]. *International Organisations Research Journal*, vol. 15, no 4, pp. 7–29. Available at: https://doi.org/10.17323/1996-7845-2020-04-01 (in Russian and English).

Wang Z. (2020) The New Dynamics of Global Cyberspace Rule-Making Under the UN Dual-Track System. *China Information Security*, vol. 20, no 1, pp. 40–3 (in Chinese).

World Internet Conference (WIC) (2020) Initiative on Jointly Building a Community With a Shared Future in Cyberspace. News, 18 November. Available at: http://www.wuzhenwic.org/2020-11/18/c_564467.htm (accessed 6 April 2021).

Xiaomi (2021) Statement. 14 March. Available at: https://blog.mi.com/en/2021/03/14/statement/ (accessed 6 April 2021).

Xu P. (2021) 2020 Global Internet Governance Towards Digital Cold War or Digital Commons. *Information Security and Communications Privacy*, vol. 21, no 3, pp. 16–23 (in Chinese).

Yan L. (2019) Global Cyberspace Governance: State Actors and the China-US Cyber Relationship. *Contemporary International Relations*, vol. 29, no 2, pp. 105–24. Available at: http://www.cicir.ac.cn/UpFiles/file/20200227/637184169973143065186752 2.pdf (accessed 19 August 2021).

Yang G. (2014) The Return of Ideology and the Future of Chinese Internet Policy. *Critical Studies in Media Communication*, vol. 31, iss. 2, pp. 109–13. Available at: https://doi.org/10.1080/15295036.2014.913803.

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, iss. 3, pp. 432–64. Available at: https://doi.org/10.1111/polp. 12202.

Zhao R. (2021) Global Network Governance Reform: Path Choices for Rising Powers. *Academia*, vol. 272, no 1, pp. 50–9 (in Chinese).

Zhu D., Liu Y-W. (2021) The Legal Governance System of Cyberspace in the Community of Shared Future of Mankind and China's Plans. *Journal of Yangtze Normal University*, vol. 37, no 1, pp. 30–9 (in Chinese).

Zinovieva E. (2015) Globalnoe upravlenie Internetom: rossijskij podhod i mezhdunarodnaja praktika [Global Internet Governance: Russian Approach and International Practice]. *MGIMO Review of International Relations*, vol. 43, no 4, pp. 111–8. Available at: https://doi.org/10.24833/2071-8160-2015-4-43-111-118 (in Russian).

ZTE (n. d.) Available at: https://www.zte.com.cn/ (accessed 6 April 2021).