DOI: 10.22363/2313-0660-2022-22-2-238-255

Research article / Научная статья

The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes

Mirzet S. Ramich ✉, **Danil A. Piskunov**

Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation
✉ramich-ms@rudn.ru

Abstract. With the development of information and communication technologies (ICTs), the Internet has become increasingly important in terms of national security, economic development, and global leadership. Apparently, conflicts and contentious issues in cyberspace requires creating rules and development of regulation. The authors examine the process of making up rules in cyberspace from the perspective of M. Castells' network society theory and B. Buzan' securitization theory. According to M. Castells, key challenges have gradually altered in the network society and power relations and social management are based on the control of communication and information which embraces a network society. Furthermore, the authors investigate the development of the Internet in the context of securitization theory. It is stressed that cyberspace has become a full-fledged political space with the central position of digital sovereignty and information security. The article for the first time proposes a comprehensive periodization of international relations' transformation in cyberspace. Afterwards, the authors consider the appearance of tensions between actors in cyber space, which include political and economic threats. It encourages state actors to establish a preliminary regulation and to agree on norms regulating state behavior in cyberspace. These mechanisms have become a venue for promoting different concepts of cyber law and establishing legal regimes. In conclusion the authors analyze the hierarchy of actors in global Internet governance to assess the actors' influence on the establishment of legal regimes in cyberspace. The main assessment criteria are as follows: ability to influence global production chains of high-tech goods, ability to conduct offensive and defensive cyber operations, and influence on the formation of international legal regimes. The authors divide actors into two major groups — rule-markers capable of influencing the global information space and constructing legal regimes, and rule-takers that are an object of great powers competition in cyberspace.

Key words: network society, cyberspace, securitization, US, China, Russia

For citation: Ramich, M. S., & Piskunov, D. A. (2022). The securitization of cyberspace: From rulemaking to establishing legal regimes. *Vestnik RUDN. International Relations*, 22(2), 238—255. https://doi.org/10.22363/2313-0660-2022-22-2-238-255

Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов

М.С. Рамич ✉, **Д.А. Пискунов**

Российский университет дружбы народов, Москва, Российская Федерация
✉ramich-ms@rudn.ru

Аннотация. С развитием информационно-коммуникационных технологий (ИКТ) сеть Интернет стала приобретать большее значение с точки зрения национальной безопасности, экономического развития и мирового лидерства. Конфликты и спорные вопросы, возникающие в информационном пространстве, требуют согласования норм и выработки инструментов правового регулирования. Авторы статьи рассматривают процесс конструирования норм в информационном пространстве с точки зрения теории «сетевого общества» М. Кастельса и теории секьюритизации. По мнению М. Кастельса, в «сетевом обществе» произошла смена ключевых вызовов и угроз, а управление им стало осуществляться за счет инструментов контроля над информацией и формирования фреймов. Вместе с тем авторы, анализируя развитие сети Интернет с точки зрения концепции секьюритизации, приходят к выводу, что информационное пространство стало полноценным политическим пространством с центральным положением «цифрового суверенитета» и информационной безопасности. В статье впервые предлагается комплексная периодизация процесса трансформации международных отношений в информационном пространстве. Возникновение в информационном пространстве точек напряженности, которые несут экономические и политические риски, побуждает государственных акторов к формированию предварительного регулирования и согласованию норм поведения в информационном пространстве. Такой процесс конструирования предварительного регулирования был начат под эгидой ООН в рамках двух механизмов, созданных США и Россией. Эти механизмы стали площадкой для продвижения концепций регулирования и создания правовых режимов. В заключении авторы анализируют иерархию акторов в глобальном управлении информационным пространством с целью оценить влияние акторов на создание правовых режимов. Основными критериями оценки выступают способность влиять на глобальные цепочки производства высокотехнологичных товаров, проводить наступательные и оборонительные кибероперации и влиять на формирование международно-правовых режимов. Среди таких акторов авторы выделяют две группы: rule maker, способных воздействовать на глобальное информационное пространство и конструировать правовые режимы, и rule taker, которые выступают объектом конкуренции держав в информационном пространстве.

Ключевые слова: сетевое общество, информационное пространство, секьюритизация, США, КНР, Россия

Для цитирования: *Рамич М. С., Пискунов Д. А.* Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 238—255. https://doi.org/10.22363/2313-0660-2022-22-2-238-255

Introduction

The development of ICTs has increased the digitalization of societies and economies in the late 20th century and early 21st centuries. From the national security perspective, cybersecurity takes priority. It includes infrastructure facilities' security, domestic Internet governance, and foreign influence reduction. The critical importance of cybersecurity stems firstly from the lack of comprehensive legal regulation of relations between states in this sphere, secondly from the presence of non-state actors on the Internet affecting states' security, thirdly from the role of cybersecurity in the social management processes of society.

Moreover, there are emerging conflicts and tensions that force states to develop rules of engagement in cyberspace. Such conflicts illustrate the importance of Internet governance and ensuring the critical infrastructure's security. Additionally, 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.[1] It becomes a prerequisite for developing norms of states' responsible behavior in cyberspace.

There are two approaches to global Internet governance — the Western concept (the US and EU) and the emerging countries' concept (China + Russia) (Krutskikh, 2019; Zinovieva, 2019a). Both concepts deal with such issues as cybersecurity, the development of the Internet, global Internet governance, internal Internet

[1] Lewis J. A. Technological Competition and China // Center for Strategic and International Studies. November 30, 2018. URL: https://www.csis.org/analysis/technological-competition-and-china (accessed: 26.02.2022). See also: (Degterev, Ramich & Piskunov, 2021; Zhao, 2021, p. 3).

management and others (Degterev, Ramich & Piskunov, 2021, p. 9). Their competition is driven not only by national security advantages, but also by the increasing confrontation between the US and China on the world stage (Danilin, 2020b; Degterev, Ramich & Tsvyk, 2021, p. 220).

The technological sphere is the core of US — China rivalry because both sides promote their tech ecosystems, ranging from Internet governance approaches to technology services and innovations (Danilin, 2020a; Xingdong & Du, 2019, p. 47). US — China tech rivalry makes sense because social media and other services play a greater role in the dissemination of values, patterns, and norms in the society. It forms the basis of social management and constructs the perception of the state (Castells, 2013). In terms of global technological influence, the US and China compete for the global spread of its social media (TikTok, WeChat, Facebook,[2] Google and others) (Danilin, 2020b).

The development of the Internet has led to the formation of "network society" in which power is exercised through the control of communications (Castells, 2011). In the context of M. Castells' network society theory it becomes relevant to consider power in the emerging global network society, in which power of actors will be constructed at the expense of established norms and rules of behavior in cyberspace.

Regulation in the nuclear sphere is a relevant example of developing norms of states' responsible behavior (Nye, 2011, p. 18). J. Nye provides a comparative analysis of developing norms and rules in the nuclear field and cyberspace (Nye, 2011, p. 22). According to J. Nye, the experience of developing norms in the nuclear sphere is applicable to the cyberspace because the Internet and cybersecurity come to the fore for states with a highly digitalized economy and the use of ICT in military and civilian infrastructure (Nye, 2016, p. 46).

The article is based on the methodological toolkit that includes the "network society" theory and securitization theory (Section I), which help to comprehensively examine the securitization of cyberspace and offer the author's periodization of this process depending on the nature of threats and states' interaction (Section II). Section III provides examples of tensions between states in cyberspace and illustrates the lack of regulation. Afterwards, the authors provide an overview of developing preliminary regulation and describe the main drafts of international legal regimes (Section IV). The authors conclude by offering their perspective on the hierarchy of global governance in cyberspace (Section V). The conclusion summarizes the main points on each aspect and provides projections for the future of global governance in cyberspace.

I. Methodology

The complex character of challenges in cyberspace determines the choice of methodological toolkit and multidisciplinary approach. The methodological basis of the present article is securitization theory and the "network society" theory.

In the 21st century cyberspace has become a full-fledged political dimension which gains importance in all spheres of international relations ranging from socio-economic interaction to international security issues. The authors consider the transformation of threats and interactions between states in cyberspace through the prism of securitization theory described by the Copenhagen School (Buzan, 1983; Buzan & Wæver, 2003; Buzan & Hansen, 2009; Hansen & Nissenbaum, 2009). This theory provides a methodological basis for examining security issues in cyberspace as

[2] On March 21, 2022, the Tverskoy District Court of Moscow satisfied the claim of the Prosecutor General's Office of the Russian Federation and recognized the activities of the social networks Instagram and Facebook, owned by Meta, as extremist, banning their work in Russia.

challenges in cyber domain exist globally and affect IR system without reference to national borders (Hjalmarsson, 2013, p. 4). In this paper, the authors compare the transformation of the security issues and international regulation in the cyberspace. To trace the securitization processes in the cyberspace authors contrast the nature of threats, the main actors and international legal regimes since the creation of the Internet (Table 1). Technological developments and the increase in ICT users have set a precedent for threats to move from the physical domain to the digital domain, where the system of interaction between actors appears anarchic and is not controlled by generally accepted regulatory regimes

The nature of so-called "choke points," or points of tension between actors has also changed due to the specifics of the cyberspace. While critical infrastructure (root services, etc.) was initially seen as the most vulnerable places in the digital domain, then the points of tension have become 'virtual' along with the evolution of interactions and threats.

There has also been an unprecedented transformation in the social sphere. User behavior has changed, and states, in turn, have adapted their policies to the new realities. Society has begun to communicate through the global Internet. More than 4.8 billion people currently use the Internet, and the majority (90%) access the Internet from mobile devices.[3] At the same time, the nature of power in society has experienced significant changes. Traditional power based on violence and fear has been transformed into "network power" through framing ideas and controlling communication (Castells, 2011; 2013). The "network society" theory considers the power as a primary aspect of national security. It happens since external actors can exert influence over society and undermine established ideas and values, and consequently gain mechanisms of social management.

According to M. Castells, the basis of the network society is power relations, and furthermore a state establishes institutions and norms in the network society to promote its interests and values (Castells, 2011). The construction of the network society is aimed at the establishing power relations, which are exercised through media and technology companies, and political institutions. These actors occupy a position of power because it exercises global governance and oversight.

As a new political dimension, cyberspace plays an important role not only within the framework of influence and governance issues in the network society, but also in the context of contemporary international economic and political relations. Such relations formed between state and non-state actors require rules of conduct and norms, but at the moment there is no comprehensive regulation of relations in this sphere. A relevant example of developing norms of responsible behavior is the example of establishing legal regulation in nuclear domain, as described by J. Nye (Nye, 2011).

II. Securitization of the Cyberspace

The securitization in the cyberspace can be divided into several phases, depending on the major actors, the nature of threats, and the international legal context environment. The Internet, as the main information communications domain of the 21st century, was originally designed for highly specialized tasks. The main focus in the early stages was made on the scientific and communication aspect, so there were no new security threats shaped during these phases. Similarly, until the early 2000s, the development of the digital space did not reach global proportions.

A clear parallel can be drawn with the development of nuclear technology. Before World War II, their development was generally limited to the scientific and energy fields. Nevertheless, the World War II and the

[3] Digital Around the World // DataReportal. URL: https://datareportal.com/global-digital-overview (accessed: 08.01.2022).

invention of controlled thermonuclear reactions caused the expansion of nuclear technologies into the military sphere. Thus, nuclear weapons and the threat of all-out nuclear war became major international security issues during the Cold War and remain so today.

Turning to cyberspace and international information security, the development of international rules and regulations has lagged behind the development of ICTs, causing numerous new challenges and threats in the digital domain. In cyberspace, technological development plays a crucial role and has also had a significant impact on the development of interstate interactions within the maritime and air domains (Rattray, 2009).

In the early 2000s, cyberspace was incorporated into national and international security at the political level. Like other new challenges and threats, increasing international attention to cybersecurity has been linked to the acceleration of globalization. Following the 9/11 attacks in 2001, many states have reflected on the challenges and opportunities that could come from the global network, given that the digital domain was not directly managed by governmental institutions (Stevens, 2012, p. 16).

It was in 2001 that the first international document regulating cybersecurity was adopted — the Council of Europe Convention on Cybercrime (The Budapest Convention on Cybercrime or the Budapest Convention).[4] In 2003, the UN adopted the Declaration of Principles for the Information Society,[5] and in 2005 the Tunis Commitment[6] and the Tunis Agenda for the Information Society[7] were adopted. The signing of these documents was a prerequisite for the establishment of the Internet Governance Forum in 2006.[8]

This phase marked an important milestone in the process of recognizing international issues related to international security in the cyberspace, since new challenges and threats were defined, and new formats of interaction were established. However, within the process of norm legalization there was a lack of full coverage of all issues related to the Internet regulation, which was due to the perception of the global network solely as a means of communication. This had changed by the early 2010s, when the Internet and the cyberspace became a key element in the scientific, technological and economic development of most countries in the world.

In the 2010s, the amount of users of IT increased, and it meant the need for states to regulate a new political space. During this time, the 4th generation (4G)[9] communication protocols, which became the driver of mobile Internet development and significantly increased the availability of network resources, became widely used. Threats in cyberspace have been both ‘real’ and ‘virtual’ — such as threats to physical network elements or critical

[4] Budapest Convention on Cybercrime // Council of Europe. November 23, 2001. URL: https://rm.coe.int/1680081561 (accessed: 08.01.2022).

[5] Declaration of Principles “Building the Information Society: A Global Challenge in the New Millennium” // International Telecommunication Union. December 12, 2003. URL: https://digitallibrary.un.org/record/533621/files/S03-WSIS-DOC-0004%21%21PDF-E.pdf (accessed: 08.01.2022).

[6] Tunis Commitment (WSIS-05/TUNIS/DOC/7-E) // International Telecommunication Union. November 18, 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/7.html (accessed: 08.01.2022).

[7] Tunis Agenda for the Information society (WSIS-05/TUNIS/DOC/6(Rev.1)-E) // International Telecommunication Union. November 18, 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (accessed: 08.01.2022).

[8] Governance via the Internet // Division of Government Institutions and Digital Government, United Nations Department of Economic and Social Affairs [Управление через Интернет // Отдел государственных учреждений и цифрового правительства Департамента ООН по экономическим и социальным вопросам]. (In Russian). URL: https://publicadministration.un.org/ru/internetgovernance (accessed: 08.01.2022).

[9] In 2009, Stockholm and Oslo launched their first commercial 4G networks. Later on, other countries also began to adopt the new communication protocols. But in some countries the adoption process has not been completed yet.

infrastructure and threats that come directly from the cyberspace, including a wide range of international threats ranging from copyright infringement to illegal political activity (Deibert & Rohozinski, 2010, pp. 29—30).

There has been a significant increase in the number of recorded interstate cyber incidents. Between 2003 and 2009, there were only 66 such incidents, but in 2017 alone, the number exceeded 71, and in 2018 and 2019 it was 114 and 116, respectively.[10] Moreover, ICTs played a major role in the Arab Spring[11] and have generally been used to organize "color revolutions" (Manoylo, 2014). For states with insufficient level of technology and lack of experience in dealing with new types of threats, the risks emanating from the cyberspace have become one of the serious challenges to national sovereignty and stability. Meanwhile, technologically developed states were able to use new tools to achieve their foreign policy goals.

In 2015, the Report of Group of Government Experts (GGE) UN on Developments in the Field of Information and Telecommunications in the Context of International Security was approved, which consolidated the results of the work of three groups of experts in 2010, 2013, and 2015. It generalized the concepts of threats in the cyberspace and proposed norms and rules of behavior for states.[12] In 2013, the NATO Cooperative Cyber Defence Centre of Excellence published the Tallinn Manual on International Law Applicable to Cyber Warfare. In 2017, the second edition was released and the third version is currently in progress. One of the distinctive features of the document was that it considered the possibility of a physical military response to cyberattacks.[13] The second version classified cyber-attacks that could be considered a violation of a country's sovereignty (resulting in loss of life or physical damage).[14] Along with the adoption of such documents, it launched the process of establishing international normative legal regimes to govern the behavior of states in the cyberspace.

With the securitization of the cyberspace, countries have begun bean to build up their offensive and defensive capabilities, which led to a "security dilemma" in cyberspace. In such an environment, powerful states can simultaneously impose rules that are convenient for them and violate them themselves, pursuing a policy of double standards, meanwhile weaker states can do nothing to oppose them (Buchanan, 2017, pp. 192—193). Thus, technologically advanced states gained more influence in cyberspace, as they bean started to implement their projects in the new political space before others.

Under these conditions, the attribution of hostile actions in the cyberspace has become a particularly urgent issue. The majority of cyberattacks and cybercrimes are committed by hacker groups whose affiliation to a particular state is almost impossible to determine. Even with the emergence of specialized institutions to preempt incidents in the cyberspace, the issue of attribution remains highly complicated (Zinovieva, 2019a, p. 58). Several countries

[10] Significant Cyber Incidents // Center of Strategic International Studies. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed: 01.02.2022).

[11] Eriksson M., Franke U., Granåsen M., Lindahl D. Social Media and ICT during the Arab Spring // FOI Report. 2013. P. 46. URL: https://www.foi.se/rest-api/report/FOI-R--3702--SE (accessed: 08.01.2022).

[12] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174 // General Assembly of the United Nations. July 22, 2015. URL: https://namib.online/wp-content/uploads/2020/04/Report-of-the-UN-Group-of-Governmental-Experts-on-Developments-in-the-Field-of-Information-of-22-July-2015.pdf (accessed: 08.01.2022).

[13] Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. by M. N. Schmitt. Cambridge; New York : Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139169288

[14] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge : Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524

have undertaken efforts to share intelligence and computer information about malicious activity in the cyberspace on their territories. Thus, within the European Union, the issue of attribution is regulated in the framework of the 2001 Budapest Convention, which was also joined by the United States, Canada, Japan, Australia, etc.[15] On the other hand, Russia and the Shanghai Cooperation Organization (SCO) countries also use the practice of exchanging intelligence while coordinating their respective agencies.[16] The Russian-Chinese Agreement on International Information Security also includes a clause for the exchange of information about malicious activity in the cyberspace.[17] In this way, experience is gained with the establishment of authorship of attacks in the cyberspace.

On the private level, leading IT companies involved in the development of antivirus systems, use the method of the so-called "hacker handwriting" code analysis to attribute cyberattacks.[18] For example, attack attribution at Kaspersky Lab is a process of comparing new incident results with accumulated experience. International information Security Company established the Kaspersky Threat Attribution Engine database, which analyzes malware and correlates it with previously saved information in order to successfully attribute attacks.[19]

During the next phase of cyberspace development, greater emphasis has been placed on establishing digital ecosystems which are designed to cluster users around a group of related applications. Big Data required higher speed communication protocols, causing an accelerated transition to 5G networks. Microsoft 365 is an example of a digital ecosystem applied at both the public and private level. Consider the fact that user data is stored and processed on the servers of the digital service provider, potentially leaving vulnerabilities for the security of sensitive information and personal data. As of 2021, the following companies provide the majority of cloud servers: Amazon (US) — 33%, Microsoft (US) — 21%, Google (US) — 10%, Alibaba (China) — 6%, IBM (US) — 4%, Salesforce (US) — 3%, Tencent (China) — 3% and Oracle (US) — 2%.[20] Such statistics clearly illustrate that most of the cloud technology market is occupied by the U.S. companies, while Chinese companies are the only competitors. Therefore, we cannot consider it a serious competition in the global cloud market. Countries pursuing the principles of digital sovereignty restrict the cross-border transfer of personal data and information by law. But given the specifics of the cyberspace, digital sovereignty in the political sense will lead to the technological isolation of the

[15] The Budapest Convention and its Protocols // Council of Europe. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed: 01.02.2022).

[16] Documents // Shanghai Cooperation Organization [Документы // Шанхайская организация сотрудничества]. (In Russian). URL: http://rus.sectsco.org/politics/ (accessed: 01.02.2022).

[17] Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of International Information Security // Official Internet portal of legal information [Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // Официальный интернет-портал правовой информации]. May 8, 2015. (In Russian). URL: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1 (accessed: 01.02.2022).

[18] Omand D. Attribution of a Cyber Attack Is a Political Decision, It Is Not a Judicial Process // Nuclear Control [Оманд Д. Атрибуция кибератаки является политическим решением, это не судебный процесс // Ядерный Контроль]. 2017. No. 4 (486). (In Russian). URL: http://www.pircenter.org/articles/2099-atribuciya-kiberataki-yavlyaetsya-politicheskim-resheniem-eto-ne-sudebnyj-process (accessed: 01.02.2022).

[19] Kaspersky Threat Attribution Engine // Kaspersky. URL: https://media.kaspersky.com/ru/business-security/enterprise/Kaspersky_Threat_Attribution_Engine_Product_Datasheet-ru.pdf (дата обращения: 01.02.2022).

[20] As Quarterly Cloud Spending Jumps to Over $50B, Microsoft Looms Larger in Amazon's Rear Mirror // Synergy Research Group. February 3, 2022. URL: https://www.srgresearch.com/articles/as-quarterly-cloud-spending-jumps-to-over-50b-microsoft-looms-larger-in-amazons-rear-mirror (accessed: 26.02.2022).

Table 1

Chronology of the Cyberspace Securitization Process, 1970—2020s

Attribute / Period	**1970s to 2000s Internet for Science**	**2000s The development of the digital domain**	**2010s Securitization of the cyberspace**	**2020 — present Transition to the meta-universes**
Broadband cellular networks	2G	3G	4G	5G
Actors	Individual governmental and private entities	States, non-governmental actors, international organizations	States, non-governmental actors, international organizations	States, non-governmental actors, international organizations
Threats Scale	Local	Local	Global	Global
Threats Nature	Industrial espionage, physical impact on critical infrastructure	Backbone of the shadow economy, a threat to physical infrastructure	Emergence of a new type of security challenges and threats, interstate cyber-attacks	The predominance of threats emanating from the cyberspace (virtual), over physical threats (real)
Regimes	—	Establishment of fundamental international legal regimes, International cooperation on cybersecurity	Competition between different approaches to the international legal regulation of the cyberspace	Development of global digital ecosystems, increasing digital divide, the struggle for leadership in the technological sphere

Source: compiled by the authors.

country. Thus, one can either secure sovereignty within political boundaries in cyberspace or achieve global interoperability of the Internet, which would mean interdependence (Mueller, 2020, p. 798).

By the early 2020s, the cyberspace had become a full-fledged political space that is central to the processes of international socio-economic and technological development. As the fourth phase began, the problem of digital sovereignty, which cannot fully correspond to the political boundaries of the state, became particularly evident. Simultaneously, countries have divided into several coalitions, which promote different forms of regulation of interstate relations in the cyberspace. The U.S. and developed countries favor a multistakeholder model of digital domain management, while Russia, China and developing countries advocate a multilateral approach (Degterev, Ramich & Piskunov, 2021). However, in addition to government initiatives, the popularization of blockchain technology enables discussions about the establishment of autonomous decentralized systems beyond government control.[21]

III. Potential Points of Tensions

Due to the emerging threats and challenges the cyberspace has become one of major spheres of national security (Hansen & Nissenbaum, 2009). Cyber-attacks on infrastructure facilities, foreign influence in the internal segment of the Internet, etc. belong to such threats.

The authors examine points of tensions in the cyberspace and analyze possible areas of overlapping interests between states and possible ways to develop rules of responsible behavior in the new political dimension. Similar to the nuclear domain, states actors have begun to agree on tacit rules and norms on the use of nuclear weapons in order to minimize the risks of nuclear proliferation,

[21] Weyl G., Ohlhaver P., Buterin V. Decentralized Society: Finding Web3's Soul // Social Science Research Network. May 11, 2022. URL: https://ssrn.com/abstract=4105763 (accessed: 26.05.2022).

escalation of conflict, etc. (Nye, 2011). The experience of conflicts and crisis involving possible use of nuclear weapon provided the basis for developing primary tacit norms. Emerging conflicts in the cyberspace involving malware could lead to a “Caribbean crisis 2.0” which would become a common challenge for leading states (Zinovieva & Alborova, 2021). This challenge will give a boost to the development of regulation in the cyber domain, as it will require joint actions and comprehensive commitment to comply it.

Given the specific nature of the cyberspace, “security” can be divided into two dimensions: physical risks to critical infrastructure, protocols and equipment and risks arising in the cyber domain without physical damage (Deibert & Rohozinski, 2010). This section examines conflicts and points of tensions between states in a number of areas affecting the cyber security: critical infrastructure, foreign influence and social services, technological security and supply chains resilience, internal Internet management.

In terms of risks to physical infrastructure under state jurisdiction, the case of the attack on the Colonial Pipeline and JBS Foods facilities should be mentioned, which resulted in the suspension of gas supplies to the US East Coast for five days and forced JBS Foods to suspend operations at its plants.[22]

As a result of the infrastructure disruption, the Biden’s administration issued the memorandum on “Improving Cybersecurity for Critical Infrastructure Control Systems.”[23] Similar attacks were carried out against Russian energy systems in 2019. Its authorship is ascribed to the United States.[24] Both states see the protection of critical infrastructure as a primary objective of the national security. In 2013, the U.S. identified 16 critical infrastructure sectors and admitted that cyber-attacks on it have a debilitating effect on security, national economic security, national public health or safety, etc.[25] Russia has passed the law on critical information infrastructure security in 2017.[26]

China has similarly passed several regulations on the cybersecurity which indicate its approaches of internal Internet management on the global scale. Firstly, it is worth noting the Cybersecurity Law of China.[27] The law has determined the notion of sovereignty in the cyberspace (网络空间主权) and specified requirements for network operators to store select data within China. Additionally, the law has set out the system of China critical infrastructure protection. In 2021 The State Council of PRC has published a number of

[22] JBS and Colonial Pipeline Hacks Highlight How Large Food and Energy Companies Have Become Prime Targets // South China Morning Post. June 4, 2021. URL: https://www.scmp.com/tech/tech-trends/article/3135990/jbs-and-colonial-pipeline-hacks-highlight-how-large-food-and (accessed: 08.01.2021).

[23] Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure // The White House. July 28, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ (accessed: 08.01.2021).

[24] U.S. Escalates Online Attacks on Russia’s Power Grid // The New York Times. June 15, 2019. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?action=click&module=Top%20 Stories&pgtype=Homepage (accessed: 08.01.2021).

[25] Critical Infrastructure Sectors // Cybersecurity and Infrastructure Security Agency. October 21, 2020. URL: https://www.cisa.gov/critical-infrastructure-sectors (accessed: 08.01.2021).

[26] Federal Law No. 187 “Security of Critical Information Infrastructure of the Russian Federation” // Official Internet Portal of Legal Information [Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации]. July 26, 2017. (In Russian). URL: http://publication.pravo.gov.ru/Document/View/0001201707260023?index=0&rangeSize=1 (accessed: 08.01.2021).

[27] Zhonghua renmin gongheguo wangluoanquanfa quanwen (2017 nianshishi) // Wu yang xian ren min zheng fu [Cybersecurity Law of the People’s Republic of China (implemented in 2017) // Maeyang County People’s Government]. (In Chinese). URL: http://www.wuyang.gov.cn/fazhizaixian/falvfagui/20200419/38978.html (accessed: 08.01.20221).

documents specifying its domestic cybersecurity policy: the Critical Information Infrastructure Security Protection Regulations,[28] Data Security Law[29] and Law on the Protection of Personal Information.[30]

In addition, the tensions between the US and China over the development of 5G networks should be noted. Based on these regulations, it can be concluded that China has taken measures to localize data, establish a critical infrastructure protection system and limit import of foreign technologies to ensure national security.

Moreover, in terms of the "network society" theory, states should exercise control over internal segment of the Internet and content in social services. It allows limiting foreign influence and ensuring domestic stability. China limits information flows with the Great Firewall and blocks foreign applications, including Google, Facebook, etc. (Ponka, Ramich & Wu, 2020). Consequently, according to the White Paper on the Internet, China implements the principle of sovereignty and preserves the right of the internal Internet governance.[31] The other example of securitization of foreign influence is the banning of the social apps such as TikTok and WeChat. During D. Trump administration, the US has tried to block these applications charging it of processing of personal data by AI technologies, blocking content, and the impact on social stability (Williams, 2020).

Furthermore, the domestic governance of the Internet plays a greater role in the context of internal conflicts. States block the Internet and limit the spread of information in order to reduce foreign influence in the social services and restrict the dissemination of information. During the 2020 mass protests in Belarus, the government shut down Internet access. As a consequence of that developments, Belarus has issued a requirement for mobile providers to set up internet access through the National Traffic Exchange Centre.[32] It has ensured the control over the access to the Internet provided by private companies. The government of Kazakhstan has chosen the same way to ensure its domestic stability and blocked the Internet throughout the country. During the 2022 Kazakh unrest protesters used secure social media to coordinate riots. The authorities made a decision to shut down the Internet to stop the dissemination of information.[33] The Internet shutdown is increasingly popular as a mechanism to strengthen domestic stability. In total, there

[28] Guanjianxinxi jichusheshi anquanbaohu tiaoli // Zhonghua renmin gongheguo guowuyuanling [Critical Information Infrastructure Security Protection Regulations // Decree of the State Council of the People's Republic of China]. September 1, 2021. (In Chinese). URL: https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/ (accessed: 08.01.2021).

[29] Data Security Law of the People's Republic of China // The National People's Congress of the People's Republic of China. June 10, 2021. URL: http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (accessed: 08.01.2021).

[30] Zhonghua renmin gongheguo geren xinxi baohufa // Quanguo renmin daibiao dahui [Law of the People's Republic of China on the Protection of Personal Information // The National People's Congress of the People's Republic of China]. August 20, 2021. (In Chinese). URL: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed: 08.01.2021).

[31] Full Text: White Paper on the Internet in China // China Daily. June 08, 2010. URL: https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm (accessed: 08.01.2021)

[32] Belarus's National Traffic Exchange Centre Attributed Problems of Internet Access in the Country to an External Attack [Белорусский «Национальный центр обмена трафиком» объяснил проблемы доступа к Интернету в стране внешней атакой] // D-Russia. August 12, 2020. (In Russian). URL: https://d-russia.ru/belorusskij-nacionalnyj-centr-obmena-trafikom-objasnil-problemy-dostupa-k-internetu-v-strane-vneshnej-atakoj.html (accessed: 08.01.2021).

[33] Kazakhstan's Largest City Almaty, Back Online after Clashes, Blackout // Hindustan Times. January 10, 2022. URL: https://www.hindustantimes.com/world-news/kazakhstans-largest-city-almaty-back-online-after-clashes-blackout-101641788351208.html (accessed: 08.03.2022).

were 182 internet shutdowns in 34 countries where protests took place in 2021.[34]

Another aspect of cybersecurity is the resilience of production chains and supplies of components and semiconductors. In terms of the economic and technological security the key challenge for states is to secure production chains and the supply of semiconductors. The semiconductor crisis, which erupted during the COVID-19 pandemic, forced states to control production chains and invest in the industry.

During the trade war with the United States China has begun to ensure its semiconductor security and to work on its own production and development of semiconductors. In 2020, China's State Council proposed that tech companies move the processes of R&D, design, manufacturing, testing and packaging of semiconductors to China.[35] This program aims to accumulate production within its territory and obtain the advanced R&D facilities in the field of semiconductors.

After J. Biden came to power, the US started to work on securing supplies chains of semiconductors. The White House issued the report on the US semiconductor industry which was commissioned by J. Biden.[36] Nevertheless, the value chain represents the involvement of a number of economies in the production process. Amid the confrontation with China, the US therefore intends to bring production processes such as manufacturing, packaging and testing back. Most of them are carried out in China or other Asian economies due to lower economic costs. A key vulnerability here is the dependence on the PRC manufacturing sector and the potential instability of the manufacturing chain, which could lead to a shortage of semiconductors in the supply chain. In order to explore vulnerabilities in this industry, the US held a summit with representatives of private companies, including TSMC, Samsung, Qualcomm and Apple, and offered funding for chip manufacturing facilities in the US.[37] It helped the US to examine the bottlenecks in the semiconductor industry.

The development of the Internet has brought new vulnerabilities such as security of root servers and reliability of the information. So-called "choke points" are critical nodes in the cyber space which are highly important for the functioning of computer systems, critical infrastructure and data exchange on the Internet.[38] These "choke points" include the ecosystems created by the technology corporations better known as the "Big Five" (Google, Amazon, Facebook, Microsoft, Apple (GAFAM)).[39] Both governmental entities and private companies use services and applications of GAFAM companies in the whole world. That is why the stability of the major part of the Internet depends on GAFAM companies. They are responsible for data centers functioning,

[34] Keep it On // Access now. URL: https://www.accessnow.org/keepiton/ (accessed: 08.01.2021).

[35] Xinshiqi cujin jicheng dianlu chanyehe ruanjianchanye gaozhiliangfazhande ruogan ganzheng zhengce // Zhonghua renmin gongheguo zhongyangrenmin zhengfu [China's State Council Policies to Promote the High-Quality Development of the Integrated Circuit (IC) and Software Industries in the New Era // Government of the People's Republic of China]. July 27, 2020. (In Chinese). URL: http://www.gov.cn/zhengce/content/2020-08/04/content_5532370.htm (accessed: 08.01.2021).

[36] Building Resilient Supply Chains, Revitalizing American Manufactures, and Fostering Broad-Based Growth. 100-Day Reviews under Executive Order 14017 // The White House. June 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf (accessed: 08.01.2022).

[37] Readout of Biden Administration Convening to Discuss and Address Semiconductor Supply Chain // The White House. September 23, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/23/readout-of-biden-administration-convening-to-discuss-and-address-semiconductor-supply-chain/ (accessed: 08.01.2022).

[38] Farrell H., Newman A. Choke Points // Harvard Business Review. January-February 2020. URL: https://hbr.org/2020/01/choke-points (accessed: 01.02.2022).

[39] Sen C. The 'Big Five' Could Destroy the Tech Ecosystem // Bloomberg. November 15, 2017. URL: https://web.archive.org/web/20201109030953/https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem (accessed: 08.01.2022).

worldwide data processing, and continuous operation of its services. A similar ecosystem of networked applications has been created by China. Alibaba, Tencent, and Huawei have developed the same tech ecosystem in China which includes various digital applications and services. Such issues as stability of digital payments system, data processing and storing, the spread of information, etc., are dependent on the resilience of tech ecosystems.

These examples of tensions in the cyberspace can be a decisive factor for agreeing on rules between states. Similar to the nuclear sphere, state and non-state actors can ensure security in the cyberspace by constructing a code of conduct. Otherwise, cyber-attacks on critical infrastructure and instability of supply chains impose economic costs on state and non-state actors. Social and sovereign management of the domestic segment of the Internet are becoming an integral part of national security policy. Thus, states can reduce frictions in these areas involving non-state actors and developing at first stage tacit norms and rules.

IV. Developing a Pre-regulation in the Cyberspace

The control over contemporary leverages of power such as global regimes and institutes, standards and technologies is determined by the competition between states.[40] International rules of responsible behavior in the cyberspace are also subject of competition between powers (the Russian Federation and the United States). The rules in the cyberspace are becoming a new leverage of power which will benefit one of approaches. Like institutions of Bretton Woods's system, created after World War II, new mechanisms and institutions that are responsible for the pre-regulation (soft law) in the cyberspace are becoming a critical element in terms of a state's power and influence in the international relations.

The leading powers in creating pre-regulation in the cyberspace are the US and Russia. Both states promote their own concepts of international rules on responsible behavior in the cyberspace. This competition takes place on the platform of the United Nations. Russia and the US have suggested opposing resolutions in the UN General Assembly sessions until 2021 (Levinson, 2021, p. 2). For its part, the Russian Federation, realising the importance and significance of the information space in terms of security and economic development initiated a process of elaboration and discussion of norms of behaviour within the UN. In 1998, the first resolution on "Developments in the field of information and telecommunications in the context of international security" (A/RES/53/70) was drafted.[41] The pre-regulatory process was institutionalized in 2004 with the establishment of the Group of Government Experts (GGE) UN.[42] The GGE primary goal is to promote the developing norms in the cyberspace. As a result, the GGE has adopted several reports in 2010, 2013, 2015, but The Group hasn't reached a consensus in 2017.[43] It has become one of the reasons to

[40] Lewis J. A. Technological Competition and China // Center for Strategic and International Studies. November 30, 2018. URL: https://www.csis.org/analysis/technological-competition-and-china (accessed: 26.02.2022).

[41] Resolution A/RES/53/70 "Developments in the Field of Information and Telecommunications in the Context of International Security" // General Assembly of the United Nations. January 4, 1999. URL: https://digitallibrary.un.org/record/265311/files/A_RES_53_70-EN.pdf (accessed: 01.02.2022).

[42] Resolution A/RES/58/32 "Developments in the Field of Information and Telecommunications in the Context of International Security" // General Assembly of the United Nations. December 18, 2003. URL: https://digitallibrary.un.org/record/507790 (accessed: 01.02.2022).

[43] The Answer of the Special Representative of the President of the Russian Federation on International Cooperation in the Field of Information Security, A.V. Krutskikh to a Question by the TASS News Agency on the State of International Dialogue in This Sphere // Ministry of Foreign Affairs of the Russian Federation [Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских

organize a new mechanism which should make the process of developing norms more inclusive. In 2018, Russia has made a proposal to organize a new format for defining norms and to set up the Open-Ended Working Group (OEWG).[44]

The "collective West" (USA France, UK, Canada, Germany, etc.) has opposed the resolution to create the OEWG. On the contrary, in 2018, the US has proposed its own resolution on the security in the cyberspace called "Advancing responsible State behavior in cyberspace in the context of international security." The resolution was targeted to define a new mandate for action by the GGE.[45] In addition, in 2021, Russia and the US were the main co-sponsors of the UN General Assembly resolution (A/RES/76/19),[46] which recognized the activities of both formats and signalled the convergence of the two powers.[47] Thus, the UN GGE and OEWG are mechanisms for developing legal regimes and promoting different concepts of regulations in the cyberspace.

Both Russia and the US define pre-regulations principles in strategies and concepts, which are the basis for harmonization of norms within the UN framework. According to the International Cyber Strategy, the US stands for accepting a standardized procedure for cyber oversight and ensuring Internet access (Davis & Lewis, 2019, p. 163). Global Internet governance should be conducted with broad participation of non-state actors, including telecommunications and technology corporations, non-profit organizations and scientific communities. States have a responsibility to protect critical infrastructure.[48] Russia and China promote the right to sovereign management of information space and restrict access to data stored on their territory. The International Information Security concept, signed by the SCO member states, defines the possibility of establishing sovereign norms and mechanisms to manage their information space and the freedom to pursue their sovereign interests in the information sphere (Zinovieva, 2019b). According to the concepts, states maintain the right to limit the access to the Internet due to threats to stability, national security, etc. (Krutskikh, 2019). State actors play a key role in global Internet governance, while non-state actors play an advisory one. An important aspect of Russia's and China's approach is to respect the role of all states in constructing norms and rules of behavior in the information space.

на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере // Министерство иностранных дел Российской Федерации]. June 29, 2017. (In Russian). URL: https://web.archive.org/web/20170705020039/http://www.mid.ru/ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288 (accessed: 27.02.2022).

[44] "Online incidents could unleash a full-scale offline war" // Kommersant [«Инциденты онлайн могут привести к развязыванию полномасштабной войны офлайн» // Коммерсантъ]. June 6, 2019. (In Russian). URL: https://www.kommersant.ru/doc/3992579 (accessed: 27.02.2022).

[45] Resolution A/RES/73/266 "Advancing Responsible State Behavior in Cyberspace in the Context of International Security" // General Assembly of the United Nations. January 2, 2019. URL: https://digitallibrary.un.org/record/1658328/files/A_RES_73_266-EN.pdf (accessed: 01.02.2022).

[46] Resolution A/RES/76/19 "Developments in the Field of Information and Telecommunications in the Context of International Security, and Advancing Responsible State Behaviour in the Use of Information and Communications Technologies" // General Assembly of the United Nations. December 8, 2021. URL: https://digitallibrary.un.org/record/3951137 (accessed: 27.02.2022).

[47] Zinovieva E., Zinchenko A. Russia and the United States Establish Cooperation in the Field of Information Security // Russian International Affairs Council [Зиновьева Е., Зинченко А. Россия и США налаживают сотрудничество в сфере информационной безопасности // Российский совет по международным делам]. November 9, 2021. (In Russian). URL: https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-nalazhivayut-sotrudnichestvo-v-sfere-informatsionnoy-bezopasnosti/ (accessed: 27.02.2022).

[48] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World // The White House. May 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed: 01.02.2022).

The above analysis demonstrates that Russia — US approaches are opposite in terms of global and domestic Internet governance, principles of development of the Internet, etc. Nevertheless, common interests in the field of cybersecurity force Russia and the U.S. to have a dialogue on the issue of developing a legal regulation.

Thus, authors conclude that pre-regulation in the cyberspace takes place through the Russian and U.S. legal mechanisms established within the framework of the United Nations. These mechanisms also serve as a key tool to promote their vision and establish legal regimes.

V. Global Governance Hierarchy in the Cyberspace

Given the lack of regulation in the information space and the conflict of several draft regulations in this field, one can speak of competition for the right to set norms in the new political space.

Globally, the power of a state has traditionally been measured by the possession of some resources, technology, or quantitative indicators of power (Degterev, 2020; Degterev, Nikulin & Ramich, 2021). However, there is no such set of criteria for assessing the power of the state in cyberspace. The main criteria of influence that ensure leadership in the digital domain are the ability to control the global production chains of technological products critical to the functioning of the network; the ability to conduct offensive and defensive cyber operations and influence the formation of international legal regimes in this sphere depend.

Control over the supply chains of high-tech products enables states to influence the availability of technology. Thus, the limitation on semiconductor production is one of the most serious constraints for China in the technological sphere. Currently, advanced processors are produced by several companies: TSMC (Taiwan) — 54% of the global market, Samsung (Republic of Korea) — 17% of the world market, Global Foundries (USA) — 7% of the world market, SMIC (PRC) — 5% of the global market.[49] At the same time, TSMC, Samsung and the largest computer chip manufacturer Intel are directly dependent on the supply of photolithographic equipment company ASML (Netherlands), which controls 62% of the global market and has no competitors, except for Japanese companies Canon and Nikon.[50] Actually, the control of these companies plays a defining role in the development of global technological processes and US, China, EU, Japan and the Republic of Korea have the greatest influence on this sphere.

The cybersecurity capabilities of countries are difficult to assess due to the protection of information on the actual capabilities of cyber forces and ongoing cyber operations. Nevertheless, the International Telecommunication Union (ITU) issues The Global Cybersecurity Index, among the most powerful actors in the cyberspace are the United States (1st), South Korea (4th), Russian Federation (5th), Japan (7th), India (10th), Türkiye (11th) and China (33rd).[51]

Two states — the Russian Federation and the United States — currently have the highest influence on the establishment of international regimes in the cyberspace. As mentioned earlier, these two countries have united most of the world around them and are promoting two projects of international regulation. Currently, there are no significant alternatives to these two projects.

[49] 2 Charts Show How Much the World Depends on Taiwan for Semiconductors // CNBC. March 15, 2021. URL: https://www.cnbc.com/2021/03/16/2-charts-show-how-much-the-world-depends-on-taiwan-for-semiconductors.html (accessed: 26.02.2022).

[50] How ASML Became Chipmaking's Biggest Monopoly // The Economist. February 29, 2020. URL: https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly (accessed: 26.02.2022).

[51] Global Cybersecurity Index 2020 // International Telecommunication Union. 2020. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/ (accessed: 26.02.2022).

Based on the above criteria, the authors present the hierarchy of global governance in the cyberspace as follows: Tier I is full control over all three spheres, which provides leadership in global governance of information space; Tier II is control over most spheres (two of the three), which allows the greatest influence on the system of global governance in cyberspace; Tier III is control over one key sphere, which allows influence on international relations in cyberspace; Tier IV is indirect influence, which only allows participation (Fig. 1). This model was built using the methodological insights of Tim Maurer, who proposed a classification of actors to identify the place of proxies in the cyberthreat taxonomy (Maurer, 2018, p. 16).

As of the early 2020s, the U.S. remains the only state that can simultaneously control global production chains of high-tech goods, has impressive cyber capabilities, and has an influence on the establishment of international legal regimes. The U.S. is seeking to maintain its leadership in the cyberspace by establishing a coalition of developed nations interested in preserving the existing international order. At the same time, Russia, China and European Union have a significant influence on the system of global governance, because they wield an impressive influence in the cyberspace and determine the major trends. Meanwhile, major suppliers of high-tech goods, as well as countries that actively use cyber operations to solve foreign policy problems, often act jointly with Tier I and II actors, unable to influence the system of global governance alone. Countries with a low level of technological development and non-state actors have an indirect influence on the cyberspace and are rather an object of competition for major actors and do not have a significant impact on the system of global governance of the cyberspace.

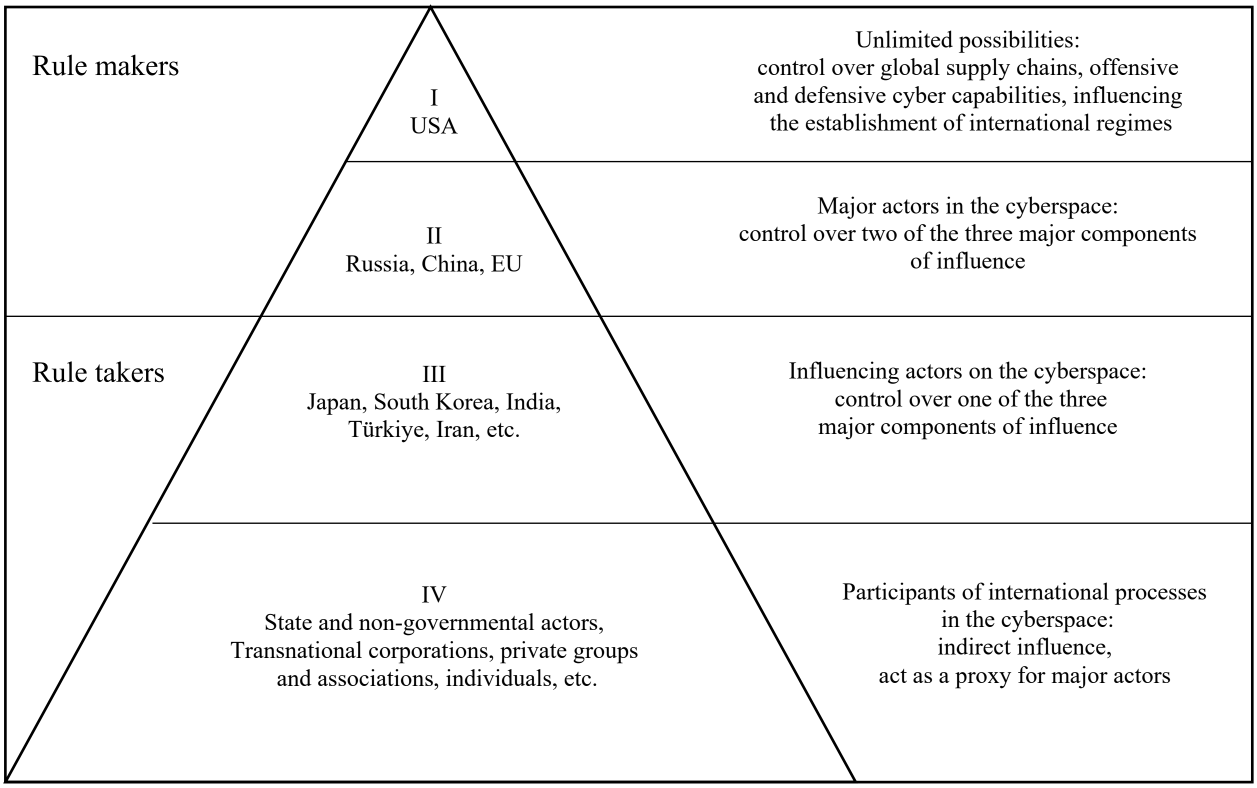
Rule makers
I
USA
Unlimited possibilities:
control over global supply chains, offensive and defensive cyber capabilities, influencing the establishment of international regimes
II
Russia, China, EU
Major actors in the cyberspace:
control over two of the three major components of influence
Rule takers
III
Japan, South Korea, India, Türkiye, Iran, etc.
Influencing actors on the cyberspace:
control over one of the three major components of influence
IV
State and non-governmental actors, Transnational corporations, private groups and associations, individuals, etc.
Participants of international processes in the cyberspace:
indirect influence,
act as a proxy for major actors

Fig. 1. Hierarchy of the Global Governance System in the Cyberspace
Note: rule makers — actors, influencing the development of international norms;
rule takers — actors, who accept established norms and follow them.
Source: compiled by the authors.

Conclusion

Through the continuous evolution of threats in the cyberspace, the digital domain has become a full-fledged area for both inter-state cooperation and competition. The special nature of digital domain, which is simultaneously in physical and virtual space, has led to the invention of fundamentally new approaches to regulate it and counter new threats.

Within the four phases of securitization discussed in the article, the actors, the scale and nature of threats, and the international legal regimes in the cyberspace have changed. Despite this, there is still a lack of regulation that allows more powerful states to exert greater influence on international processes by establishing rules and regulations that maintain their leadership. This raises a fundamental conflict of interest between the existing hegemon — the U.S. and the countries that seek to reshape the system of global governance in the cyberspace — the Russian Federation and the People's Republic of China.

For the time being, we can observe a pre-regulatory process in the information space, within which several drafts of comprehensive international legal regimes can be distinguished, which compete with each other. At the same time, the countries supporting these drafts adopt the regulations specified in them within the framework of some international formats. These are separate agreements between NATO and the EU in the case of the United States and European countries, and separate documents within the SCO and BRICS in the case of the Russia and China.

Global governance of the cyberspace itself is hierarchical and the influence on the establishment of new norms and rules can be exerted by a limited number of states — the United States, Russia, China and the EU countries. Other countries often do not act as independent actors and are included in one of the existing coalitions.

Considering these factors, it can be assumed that an alternative option to state models of regulation of the cyberspace will be proposed. Perhaps this will be a decentralized model based on blockchain technology, which will allow non-governmental actors to have a greater influence on the system of global governance in the cyberspace.

Received / Поступила в редакцию: 27.02.2022
Revised / Доработана после рецензирования: 01.04.2022
Accepted / Принята к публикации: 18.04.2022

References

Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, Trust And Fear Between Nations*. New York, NY: Oxford University Press.

Buzan, B. (1983). *People, states, and fear: The national security problem in international relations.* Brighton: Wheatsheaf Books.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge: Cambridge University Press.

Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511491252

Castells, M. (2011). Network theory. A network theory of power. *International journal of communication*, 5(15), 773—787.

Castells, M. (2013). *Communication power*. Oxford: Oxford University Press.

Danilin, I. V. (2020a). The U.S. — China technology war: Risks and opportunities for P.R.C. and global tech sector. *Comparative Politics Russia*, 11(4), 160—176. (In Russian). https://doi.org/10.24411/2221-3279-2020-10056

Danilin, I. V. (2020b). Conceptualizing American strategy in the technology war against China: Economy, geopolitics, techno-nationalism. *Journal of International Analytics*, 11(4), 21—38. (In Russian). https://doi.org/10.46272/2587-8476-2020-11-4-21-38

Davis, J. A., & Lewis, C. (2019). Beyond the United Nations group of governmental experts: Norms of responsible nation-state behavior in cyberspace. *The Cyber Defense Review*, 161—168.

Degterev, D. A. (2020). *Assessment of the current international arrangement of forces and the formation of a multipolar world.* Moscow: Ru-Science publ. (In Russian).

Degterev, D. A., Nikulin, M. A., & Ramich, M. S. (Eds.). (2021). *Balance of powers in key regions: Conceptualization and applied analysis*. Moscow: RUDN publ. (In Russian).

Degterev, D. A., Ramich, M. S., & Piskunov, D. A. (2021). U.S. — China approaches to global Internet governance: "New bipolarity" in terms of "the network society". *International Organisations Research Journal*, 16(3), 7—33. https://doi.org/10.17323/1996-7845-2021-03-01

Degterev, D. A., Ramich, M. S., & Tsvyk, A. V. (2021). U.S. — China: "Power transition" and the outlines of "conflict bipolarity". *Vestnik RUDN. International Relations*, 21(2), 210—231. https://doi.org/10.22363/2313-0660-2021-21-2-210-231

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1), 15—32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, 53(4), 1155—1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hjalmarsson, O. (2013). The securitization of cyberspace. How the Web was won. *Lund University Libraries*, 1—28. Retrieved from http://lup.lub.lu.se/student-papers/record/3357990

Krutskikh, A. V. (Ed.). (2019). *International information security: Theory and Practice* (Volume 1). Moscow: Aspekt Press publ. (In Russian).

Levinson, N. S. (2021). Idea entrepreneurs: The United Nations open-ended working group & cybersecurity. *Telecommunications Policy*, 45(6), 1—11. https://doi.org/10.1016/j.telpol.2021.102142

Manoylo, A. V. (2014). Information factor color revolutions and modern technology of dismantling of political regimes. *MGIMO Review of International Relations*, (6), 61—67. (In Russian). https://doi.org/10.24833/2071-8160-2014-6-39-61-67

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316422724

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review,* 22(4), 779—801. https://doi.org/10.1093/isr/viz044

Nye, J. S. (2016). Deterrence and dissuasion in cyberspace. *International Security,* 41(3), 44—71. https://doi.org/10.1162/ISEC_a_00266

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly*. 5(4), 18—38.

Ponka, T. I., Ramich, M. S., & Wu, Y. (2020). Information policy and information security of PRC: Development, approaches and implementation. *Vestnik RUDN. International Relations,* 20(2), 382—394. (In Russian). https://doi.org/10.22363/2313-0660-2020-20-2-382-394

Rattray, G. J. (2009). An environmental approach to understanding cyberpower. In F. D. Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 253—274). Washington, DC: National Defense University Press, Potomac Books.

Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy,* 33(1), 148—170. https://doi.org/10.1080/13523260.2012.659597

Williams, R. D. (2020). Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security. *Working Paper for the Penn Project on the Future of U.S. — China Relations*, 1—44. Retrieved from https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201030_huawei_tiktok_williams.pdf

Xingdong, F., & Du, L. (2019). Zhongmei keji jingzhengde weilai qushiyanjiu — quanqiu keji chuangxin qudongxiade chanye youshi zhuanyi、chongtu yuzai pingheng. *Renminluntan xueshuqianyan* [Study on the future trends of Sino-U.S. technological competition — industrial advantage transfer, conflict and rebalancing driven by global technological innovation. *People's Forum Academic Frontiers*], 4(24), 46—59. (In Chinese). https://doi.org/10.16619/j.cnki.rmltxsqy.2019.24.004

Zhao, S. (2021). The US — China rivalry in the emerging bipolar world: Hostility, alignment, and power balance. *Journal of Contemporary China,* 31(134), 169—185. https://doi.org/10.1080/10670564.2021.1945733

Zinovieva, E. S. (2019a). Concepts of cyberdeterrence and digital security dilemma in the US academic literature. *International Trends,* 17(3), 51—65. (In Russian). https://doi.org/10.17994/IT.2019.17.3.58.4

Zinovieva, E. S. (2019b). *International cooperation to ensure information security: subjects and trends of evolution* [thesis]. Moscow: MGIMO publ. (In Russian).

Zinovieva, E. S., & Alborova, M. B. (Eds.). (2021). *International information security: A new geopolitical reality*. Moscow: Aspekt Press publ. (In Russian).

About the authors: *Ramich Mirzet Safetovich* — Assistant, the Department of Theory and History of International Relations, Peoples' Friendship University of Russia (RUDN University); ORCID: 0000-0003-1479-2785; e-mail: ramich-ms@rudn.ru

Piskunov Danil Andreevich — Student, the Department of Theory and History of International Relations, Peoples' Friendship University of Russia (RUDN University); ORCID: 0000-0002-4321-3191; e-mail: piskunov_da@mail.ru