CHANGING SOCIETY
Social structure, social institutions and processes

Original article
https://doi.org/10.53658/RW2022-2-2(4)-100-131

Sociological sciences

Information sovereignity: materials of scientific discussion

Nikolai P. Gribin[1a]✉, Irina N. Kohtyulina[2b]✉, Denis I. Sedunov[3c]✉, Egor I. Sobolev[4d]✉

[1] Moscow State Institute of International Relations (University) Russian Foreign Ministry, Moscow, Russia
[2] National Institute for Global Security Studies, Moscow, Russia
[3] Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia
[4] The National Communications Development Research Institution, Moscow, Russia
[a] n.gordin40@gmail.com, htpps://orcid.org/0000-0001-9141-445
[b] expobroker@yandex.ru
[c] DenisSedunov@list.ru
[d] 1032193499@rudn.ru

Abstract. The article contains the most significant and interesting materials of the scientific discussion on the problems of information sovereignty and information security in Russia held by the National Research Institute for the Communications Development. The authors identify the main threats and risks to the stability of the Russian Federation in the era of digitalization. Approaches to the definition of the concept of «information sovereignity» are considered, its criteria are defined. Problems of ensuring the information sovereignity of Russia are identified, in particular, relating to Russia's technological dependence on foreign technologies and equipment, weak security of the Russian information infrastructure. During the discussion, recommendations were developed: 1) significantly increase the financing of the Russian high-tech industry, support Russian research in the field of computer technology in order to reduce dependence on foreign products to a minimum and increase the security of critical infrastructure facilities; 2) to continue the development of a special direction in the sphere of cybersecurity in the Russian Armed Forces, increase military potential in the sphere of digital technologies; 3) to pursue an active information policy aimed at combating false messages; 4) to monitor the dissemination of illegal information in social networks; 5) to begin the implementation of state policy in the field of public education on information security, rules for safe interaction with digital technologies; 6) to strengthen control over illegal activities on the Internet.

Keywords: state, information sovereignity, information security, threats to information sovereignity

ISSN 2782-3067 (Print)

For citation: Nikolai P. Gribin. Irina N. Kohtyulina, Denis I. Sedunov, Egor I. Sobolev. Information sovereignty: materials of scientific discussion. Russia & World: Scientific Dialogue. 2022. No. 2(4). pp. 100-131. https://doi.org/10.53658/RW2022-2-2(4)-100-131

Introduction

The relevance of the scientific discussion about the problems and criteria of information sovereignty is due to a number of reasons related to the strengthening of international information confrontation, the tightening of the technology of information wars, and the increasingly unfriendly information policy of a number of foreign countries towards Russia. Despite the fact that for many years work has been carried out to create a legal framework that would regulate the international information space and the place of states in it, the problem of information sovereignty is only getting worse. The purpose of our discussion is to define the criteria for information sovereignty, identify the risks and threats to Russia's information sovereignty, discuss the experience of ensuring it in other countries, and identify possible ways to solve the problems of information sovereignty.

Materials and methods

The authors of this scientific discussion in their research applied systematic, institutional approaches, relied on the concepts of political realism, used the method of comparative analysis. The empirical base of the study was statistical data, materials of analytical reports, and regulatory legal acts: UN international reports (reports of a group of government experts on achievements in the field of informatization and telecommunications in the context of international security in 2013[1] and 2015[2]), national strategies and doctrines (National Security Strategy China in Cyberspace[3], US National Cyber Strategy[4], US Department of Defense Cyber Strategy[5], Information Security Doctrine of the Russian Federation[6], National Security Strategy of the Russian

1 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98. Available:http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.

2 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. Available:https://documents-ddsny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement.

3 National Security Strategy in Cyberspace. Available: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

4 National Cyber Strategy of the United States of America. Available: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

5 Department of Defense Cyber Strategy – 2018. Available: https://www.cybercom.mil/About/Mission-and-Vision/.

6 The Information Security Doctrine of the Russian Federation. Available: http://www.scrf.gov.ru/documents/6/5.html.

Federation[7], Military Doctrine of the Russian Federation[8]), laws related to ensuring information sovereignty.

Results

Threats and risks to the sustainability and stability of the Russian Federation in the era of digitalization (N.P.Gribin)

In the current situation of turbulent geopolitical processes, unforeseen explosive events and international conflicts, reflecting the growth of interstate contradictions, the confrontation between global and regional leading countries for hegemony in establishing the rules and principles of the world order, the uncompromising promotion of their own national interests, often to the detriment of other subjects of international law, all advanced technologies play a more prominent role. Along with the disclosure of unlimited opportunities for the accelerated development of human civilization and the rapid solution of many of the most complex problems in public administration, the economy, business and the social sphere, technological tools are becoming a key means of achieving advantages in armed clashes, economic and trade expansion, information and psychological confrontation between rival states and their coalitions.

On this side of the scientific and technological revolution taking place in our days drew attention the President of the Russian Federation Vladimir V.Putin, who declared in 2019 at the St.Petersburg International Economic Forum about "the first technological war coming in the digital age." The head of the Russian state singled out the quintessence of this war:

> Attempts to monopolize a new technological wave, to limit access to its achievements, bring the problem of global inequality both between countries and regions, and within the states themselves to a completely new, different level. Well, this is the main source of instability in the world[9].

The intensification of geopolitical tension and the uncertain prospects for its mitigation have necessitated the protection of the vital interests of the Russian Federation from external and internal enemies, including from unfriendly actions of foreign states. As a result, a new National Security Strategy of the Russian Federation was adopted, approved by Decree of the President of the Russian Federation on July 2, 2021. No 400.

7 Decree of the President of the Russian Federation No. 400 dated 02.07.2021 "On the National Security Strategy of the Russian Federation". Available: http://publication.pravo.gov.ru/Document/View/0001202107030001.

8 Military Doctrine of the Russian Federation (approved by the President of the Russian Federation on 25.12.2014 No. Pr-2976). Available: https://www.mchs.gov.ru/dokumenty/2940.

9 St. Petersburg International Economic Forum, St.Petersburg, June 7, 2019. Available: https://www.1tv.ru/news/2019-06-07/366537-vladimir_putin_vystupil_na_ekonomicheskom_forume_v_sankt_peterburge.

 ISSN 2782-3067 (Print)

The Strategy states that the main "goal of the scientific and technological development of the Russian Federation is to ensure the technological independence and competitiveness of the country." To achieve this goal, it is necessary to develop and implement perspective high technologies, such as nanotechnology, robotics, genetic engineering, information and communication technologies, artificial intelligence, technologies for processing colossal data arrays, and the creation of new materials.

The Strategy expresses confidence that the implementation of the outlined ambitious plans will lead to

> strengthening defense capabilities, modernizing the economy and developing industrial potential, strengthening the sovereign statehood of Russia, capable of pursuing an independent foreign and domestic policy, and of effectively resisting attempts by external pressure.

Seems like it would be frivolous not to notice the negative concomitant manifestations and limitations in the ongoing promising, rapidly developing technological breakthrough. Such manifestations and limitations have obvious signs of threats and risks in the event of reckless introduction of digital technologies into all spheres of the state and society, the advantages of which are presented today in the mass media mainly in enthusiastic tones. It is not difficult to assume that threats and risks that are not yet always obvious, will sooner or later affect the effectiveness of applied technological innovations.

In this regard, I believe it is useful to focus on some obvious threats and risks of the era of digitalization, which in the long run may negatively affect the stability of the state if measures are not taken to neutralize them, which directly affects the interests of ensuring the national security of the Russian Federation.

The threats and risks of digitalization (from the English word digital, and ization means an action or process), can be conditionally divided into two different blocks. The first block is formed on the basis of an indicator of the scale of the use of digital technologies that generate threats and risks of a general plan. The second block consists of threats and risks that arise in the process of using digital technologies in specific areas of the life of the state and society. From the point of view of external manifestation, threats and risks can be real and potential and manifest themselves in both blocks.

The main general threat to the implementation of the digital transformation of the entire country is seen in the fact that in the electronic equipment and software segments, almost all the needs of the domestic Russian market are met through imports. This fact is confirmed in the Strategy for the Development of Information Technologies in the Russian Federation for 2014–2020 and for the period up to 2025, approved by the Government of the Russian Federation on November 1, 2013 (No. 2036-r). According to experts in the field of information technology, today the situation has not changed significantly. As a result, foreign manufacturers of this class of products still occupy a dominant position in the domestic IT market, and this gives them the opportunity to dictate their terms. The current situation is especially dangerous due to the aggravation of external threats to Russia, the escalation of sanctions against our country, the illegal removal of information

from telecommunications systems, the real possibility of blocking purchased imported equipment and the deformation of software, and the increasing number of cyber-attacks on government agencies, corporations and private businesses. In such conditions, the question of the country's ability to ensure domestic sovereign digitalization is very important.

To remove the real threat of Russia's IT dependence on Western countries, it seems necessary to strengthen the regulatory role of the state, following the example in the electronics industry in the United States, China and South Korea, which, thanks to this decision, have advanced in this industry. In particular, it is desirable to do:

- increase direct budgetary support for Russian IT companies, create a preferential tax regime for them, provide them with affordable long-term loans;
- limit and in the future prohibit the use of foreign IT technologies in the Russian Federation;
- legally oblige state structures, corporations and businesses to purchase domestic IT technologies, which, according to experts, are not inferior in quality to foreign ones.

Another general threat is associated with artificial intelligence, which today is called "the main technology of the 21st century", it is a cross-cutting scientific and technological area. The range of application of artificial intelligence and robotization is unlimitedly wide. This is primarily production, the social sphere, education, science and culture. Artificial intelligence opens up unique opportunities for quickly analyzing a huge amount of data, for improving the quality of human life, for improving education and medical care, and for radically increasing labor productivity in almost all sectors of the economy. With the help of such innovations, people are freed from routine, difficult, labor-intensive and dangerous processes in production, fewer mistakes are made in labor activity, and costs in the course of manufacturing products are minimized. For example, artificial intelligence algorithms make it easier for doctors to quickly detect dangerous diseases, allow them to analyze the results of medical research with high accuracy, and make it possible to significantly improve the quality of diagnostics, which is especially important during the ongoing pandemic.

At the same time, it is impossible to ignore the completely justified fears that the unique technologies of artificial intelligence and robotization will lead to the loss of many jobs and specialties both in our country and abroad. Around 85 million people are expected to lose their jobs worldwide. People deprived of work and livelihood can join the ranks of protesters, illegal armed groups, terrorists and extremists, as well as increase uncontrolled migration flows, including from foreign countries to the Russian Federation. The idea of establishing total control over every step of a person with the help of "smart" technical means will hardly be welcomed by society. There is even a fantastic warning about a possible "revolt" of machines, which, of course, is hardly probable, since man will always keep machines under control. The disadvantages of using artificial intelligence and robotics are also seen in the high cost of maintaining high-tech and complex mechanisms created on the basis of such innovations, and in the high cost of repairing them.

Important is the risk of leakage of personal data of each person due to the participation of artificial intelligence in the processing of the entire array of information about the population of the country, becoming open and accessible. An important step in mitigating

this risk is the Federal Law "On the Unified Federal Information Register Containing Information on the Population of the Russian Federation", adopted on June 8, 2020 (No. 168-FZ). The law establishes criteria for admitting only competent state agencies to this kind of information. Currently, the issue of creating other regulatory, technical and organizational barriers that prevent the leakage of personal data of Russian citizens and their illegal use is being worked out.

Another issue concerns the dissemination of information about Russian achievements in the field of military technologies, the creation of ultra-modern strike combat systems, supersonic (with many strokes) aircrafts and missiles, which have no analogues in the West. Of course, you are proud of such successes of our scientists, designers, specialists and the country as a whole. However, it is impossible not to say that Russia's enemies warn about the alleged threat to Western civilization from our country. This topic is constantly present in the news of Western countries; unfriendly states psychologically process their population and negatively set it up against the Russian Federation and its citizens. Focusing on the threat from Russia motivates the ruling circles of Western states to annually increase their already huge military budgets, exceeding Russian defense spending. At the same time, the fake about the aggressiveness of our country is used to justify the demonstration of its own "defense" measures and military exercises in the countries adjacent to Russia and along the borders of the Russian Federation.

The second block of threats and risks manifests itself, as noted, in the process of using digital technologies in specific areas of socio-economic activity, primarily in public administration, the economy, energy, education, healthcare, urban economy, culture, science and statistics.

In a short speech, it is impossible to deeply and comprehensively highlight the features and nuances of threats and risks from the introduction of digital technologies in all areas of the life of the state and society. Therefore, for illustration, let me dwell on only some of these areas. In particular, discuss the state in economics and science.

In the economic, unfortunately, there is a slow introduction of digital technologies. This is especially noticeable if we recall that the President of the Russian Federation Vladimir V. Putin even in December 2016, signed the Decree "On the Strategy for the Scientific and Technological Development of the Russian Federation"[10], where were the measures provided for creating legal, technical, organizational and financial conditions for the development of the digital economy in the country. However, after more than five years, the digital economy in Russia, according to experts, is only 4% of GDP, while in the US this figure is 10%. One of the reasons for this situation is the lack of incentive mechanisms that promote the development of innovative activities of business entities, and this, in turn, keeps the Russian economy tilted towards the export of raw materials.

In this regard, the transfer of the country's economy to a qualitatively new level through digital technologies is again proclaimed a priority in the policy of mastering

10 Decree of the President of the Russian Federation "On the Strategy of Scientific and Technological Development of the Russian Federation" dated December 01, 2016 No. 642. Available: http://kremlin.ru/acts/bank/41449.

a non-raw material development model. But it is clearly not enough to confine ourselves to declarations about the accelerated development of digital technologies and their rapid introduction into everyday life, since the development, manufacture, testing and popularization in society and in business circles of the advantages of digital technologies require the efforts of large teams of scientists and specialists, as well as modern expensive material technical base. We have to state that today domestic science is in a situation that can hardly be called favorable, and primarily due to underfunding. According to the website of the Accounts Chamber of the Russian Federation, expenses on science in Russia are now about 1.1% of GDP. In the USA, 2.8% of GDP is allocated for science, in China – 2.2%, in South Korea – 4.8%. Due to the latest scientific and technological achievements, the Americans are reducing the price of shale oil, and our oil production in the North, especially on the shelf of the northern seas, may soon be uncompetitive.

Just a few words about the threats and risks when using digital technologies in education. So, with distance learning, there is no direct communication between students and teachers, social communication skills are not developed, the dialogue between them mutually enriching knowledge disappears, the perception of information decreases and the understanding of the material become difficult. Such a system of education is technically unable to control the independence of completing tasks and tests. Physical deviations in the health of distance learning participants are also recorded: visual impairment, headache, insomnia, irritability.

Conclusions

In conclusion, I would like to note that in this discussion I have identified only some of the most significant real and potential threats and risks to the state and society in the era of digitalization. By the way, some of them can hardly be qualified as threats. Rather, these are the shortcomings or costs of the development of digital civilization, and humanity is able to neutralize or at least reduce their negative impact, whether we are ready to the identification, in-depth study and comprehensive scientific understanding of the digital component of our life, as well as the thoughtful development and implementation of a set of effective and sufficient preventive countermeasures.

International information security in new geopolitical realities (I.N.Kokhtyulina)

Humanity has entered the zone of total breakdown of the world order. According to a number of experts, information and communication technologies (ICT) and the info narrative as a whole play an increasingly subversive role in this process and in the process of desovereignization of nation states.

At the same time, the planet is seized by an unprecedented digital transformation. The coronavirus pandemic also gave a powerful impulse to the aggravation of geopolitical

 ISSN 2782-3067 (Print)

confrontation. Humanity is becoming more and more aware of its gigantic scale, leading experts compare it with the Great Depression and call it the greatest global challenge since the Second World War.

The COVID-19 pandemic has triggered both many of the benefits and threats of the digital world. Given the particular urgency of this problem, UN Secretary-General A. Guterres proposed on June 11, 2020 the Roadmap for Digital Cooperation: Implementing the Recommendations of the High-Level Panel on Digital Cooperation[11]. The impetus for this is Internet technologies, which caused and continue to cause tectonic shifts in the development of civilization. In fact, humanity has entered a new phase transition, comparable in significance, for example, with the creation of writing. At the same time, microelectronics has been replaced by a new technological order: nano-, bio-, info- and cognitive technologies, and based on the principles of Industry IV the digital economy, cyber-physical systems, artificial intelligence, quantum computing, blockchain, 5G generation communications and others are rapidly developing, radically changing the world, technologies.

Under these conditions, leading countries are developing and implementing a variety of doctrines and strategies for the implementation of these technologies with the aim of geopolitical dominance.

Because of this, the Fundamentals of State Policy in the Field of International Information Security approved by Decree of the President of the Russian Federation of April 12, 2021 No. 213[12] (further here - Fundamentals) are of invaluable and strategic importance in creating a secure global information space. This document is aimed at promoting Russian approaches to the formation of a system of ensuring international information security and Russian initiatives in this area, at promoting the creation of international legal mechanisms for preventing and resolving interstate conflicts in the global information space and at organizing interagency cooperation.

Among the threats to international information security, the Fundamentals highlight the following:

> a) the use of information and communication technologies in the military-political and other spheres for the purpose of undermining (infringing) the sovereignty, violating the territorial integrity of states, carrying out other actions in the global information space that impede the maintenance of international peace, security and stability;
>
> b) the use of information and communication technologies for terrorist purposes, including for promoting terrorism and attracting new supporters to terrorist activities;
>
> c) the use of information and communication technologies for extremist purposes, as well as for interference in the internal affairs of sovereign states;
>
> d) the use of information and communication technologies for criminal purposes, including for committing crimes in the field of computer information, as well as for committing various types of scam;

11 Official Documents System of the United Nations. Available: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/53/PDF/N2010253.pdf?OpenElement.

12 Fundamentals of the state policy in the field of international information security, approved by Decree of the President of the Russian Federation of April 12, 2021 No. 213 Available: http://kremlin.ru/acts/bank/46614

e) the use of information and communication technologies to carry out computer attacks on the information resources of states, including critical information infrastructure;

f) the use by individual states of technological dominance in the global information space to monopolize the market of information and communication technologies, limit the access of other states to advanced information and communication technologies, as well as to increase their technological dependence on the states that dominate in the field of informatization and information inequality.

Now the United States and its satellites have launched a total hybrid war against Russia. This is confirmed, in particular, by the report "NATO-2030"[13], published on November 25, 2020, the meaning of which is to strengthen the hybrid impact on Russia and its allies: political, diplomatic, economic, military and informational. At the same time, NATO centers in Riga, Tallinn, Helsinki play a key role in the information and psychological manipulation of the mass consciousness of Russians.

The development of cognitive and mental warfare in the information environment increases the risk of conflicts that can disrupt international peace.

Mental war is a war aimed at changing the worldview not only of the enemy's population, but also of its own population, in the countries of allies and partners, the main threat lies in the fact that its consequences do not affect immediately, but through generations[14].

Unlike cyberwar and direct information operations, mental warfare is implemented in the context of the emerging world of "post-truth", when people are "weaned" from critical thinking, from striving for the truth.

Today, the manipulation of public consciousness is already actively conducted both at the level of meaning, and at the level of emotions, and at the level of the subconscious.

At present, the United States and its satellites have launched an all-out hybrid war against Russia. This is confirmed, in particular, by the NATO-2030 report published on November 25, 2020, the meaning of which is to increase the hybrid impact on Russia and its allies: political, diplomatic, economic, military and informational. At the same time, NATO centers in Riga, Tallinn, and Helsinki play a key role in the information and psychological manipulation of the mass consciousness of Russians.

The development of cognitive and mental warfare in the ICT environment increases the risk of conflicts that can disrupt international peace.

Mental warfare is a war aimed at changing the worldview not only of the enemy population, but also in their own countries, in the countries of allies and partners, bearing a "generational" scale, the main threat of which lies in the fact that its consequences do not affect immediately, but through generations.

13 NATO-2030: United for a New Era. 25 November 2020. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

14 Ilnitsky Andrey. A mental war for the future of Russia. Available: https://zvezdaweekly.ru/news/20214211636-jxgHZ.html.

Unlike cyberwars and direct information operations, mental warfare is directed and implemented taking into account the actually emerging world of "post-truth", when people are "weaned" from critical thinking, from striving for truth.

Today, public consciousness is being actively manipulated both at the level of meaning, and at the level of emotions, and at the level of the subconscious.

In this context, it is relevant to analyze the documents concerning the information work of Great Britain on the territory of the former USSR. This archive[15], possibly hacked by the group Anonymous, contains links to internal documents of the British Foreign Office concerning its activities in Europe and Asia, while some of them are directly related to Ukraine and Russia.

Thus, the documents note that the British Foreign Office issued a secret form, which refers to the launch of a program to counter Russia's informational influence in the Baltic countries, Belarus, Ukraine, Georgia, etc.

The purpose of this program is to weaken the influence of the Russian Federation on its closest neighbors, and its macro-goal is to reduce the level of public confidence in the leadership of Russia.

The task of interaction, communication between ethnic Russians and local communities, as well as training, involvement of new participants in various projects was entrusted to the British Council, whose activities were terminated in Russia in 2018.

The British Foreign Office has focused on supporting independent media in the post-Soviet space, especially Russian-language media. As follows from the documents, since 2018, London has been ready to discredit any information disseminated by Russian state media if it did not correspond to British interests.

Anti-Russian publications in the media today are only a part of the large-scale information operation carried out by the UK throughout the post-Soviet space.

From March 2019 to March 2021, the UK spent about £9 million related grants on the implementation of the information expansion plan.

It is noteworthy that since the beginning of Russia's military operation in Ukraine, the topic of information confrontation has received a new development: the key element of information is precisely its "anti-Russianness", the question of its authenticity or falsity turns out to be secondary.

In total, according to the Safe Internet League, since February 24, 2022, about 6.5 million fake messages about a special military operation in Ukraine, as well as about Russia, have appeared on the Internet. The cost of an information attack on the Russian Federation reached $1.5 billion[16]. About $25 million is spent daily on the campaign, which is about 2 billion rubles a day. Messages are distributed from the territory of Ukraine, Poland, Latvia, USA, Great Britain and other countries.

15 "Weaken Russia's influence": how Britain was preparing Ukraine for an information war. Available: https://russian.rt.com/world/article/988503-britaniya-ukraina-finansirovanie-utechka-anonimus.

16 The Safe Internet League has identified about 6.5 million fakes about a special operation in Ukraine. Available: https://tass.ru/obschestvo/14463169?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru.

At the same time, as the Minister of Foreign Affairs of the Russian Federation Sergey Lavrov noted in his speech at the plenary session "International Relations in the context of digitalization of public life" of the International Scientific and Practical Conference "Digital International Relations 2022" on April 14, 2022, the West, having given itself the title of "beacon of democracy", grossly violates its international obligations to ensure freedom of expression, equal access to information, blocking access to it. Thus, the West demonstrates totalitarian intolerance towards alternative points of view[17].

Under the Western repressions fall both individual users of social networks and large media with all the infrastructure for disseminating news that has been created over the years. Under the illegitimate sanctions fall the heads of domestic media operators and ordinary employees are being brought under the influence. Global Western, primarily American, Internet platforms are blocking the Russian information resource all over the world. They do it defiantly, without hesitation.

Thus, the YouTube video hosting, owned by the American IT company Google, restricted access to the briefing by the official representative of the Russian Foreign Ministry, Maria V.Zakharova in March 17 this year[18]. M.Zakharova called the incident as another act of censorship against Russian resources, and also suggested that the blocking could be related to the data on biological laboratories in Ukraine, which were discussed at the briefing and which are hidden in the West. Unreasonable restrictions are also imposed on the publications of the Russian Foreign Ministry and foreign agencies on the Twitter network only because these sources publish truthful information, supported by facts.

The channel of the State Duma of the Federal Assembly of the Russian Federation DumaTV was also blocked without the possibility of recovery, to which more than 145 thousand people were subscribed, and the number of video content views exceeded 100 million[19].

There are about 36 accounts under YouTube video hosting restrictions, including RT, Russia 24, Sputnik, Zvezda, RBC, NTV, etc.

Roskomnadzor called Youtube one of the key platforms for the dissemination of "false content" about Russia's special military operation in Ukraine. And the restrictive measures introduced by the YouTube video hosting administration against Russian media fundamentally violate the key principles of the free distribution of information and unhindered access to it[20].

At the same time, Russian state institutions, the media, critical information infrastructure facilities, and life support systems are almost daily subjected to serious

17 Speech by the Minister of Foreign Affairs of the Russian Federation Sergey Lavrov at the plenary session "International relations in the context of digitalization of public life" of the International scientific and Practical conference «Digital International Relations 2022», Moscow, April 14, 2022. Available: https://www.mid.ru/ru/press_service/video/view/1809294/.

18 Google called the reason for blocking the recording of Zakharova's briefing on YouTube. Available: https://www.m24.ru/news/politika/07042022/448857.

19 Google has blocked the Duma TV YouTube channel. Available: https://dumatv.ru/news/google-zablokiroval-youtube-kanal--duma-tv.

20 Roskomnadzor demands to immediately remove restrictions from YouTube channels of Russian state media. Available: https://rkn.gov.ru/news/rsoc/news74284.htm.

 ISSN 2782-3067 (Print)

cyberattacks using the latest information technologies. All this is part of a coordinated information aggression against Russia, which requires special attention to the tasks of protecting the information resources of state authorities.

In this regard, Russia is taking specific legislative and practical steps to further strengthen the country's technological digital sovereignty. On April 25, 2022, the head of the Defense and Security Committee of the Federation Council of the Federal Assembly of the Russian Federation, Viktor Bondarev, held a round table on the topic: «Mental wars: problems and countermeasures»[21]. The participants of the round table stated that the attacks of the West on our country are the part of an ever-increasing hybrid impact, anti-Russian information and propaganda campaigns discredit the leadership of the state and its domestic and foreign policy, form the prerequisites for destabilizing the socio-political situation, involve youth, including minors in extremist and protest activities.

The current situation requires the activity of all institutions of civil society and authorities, the participants of the round table emphasized. It is noted that the basic principle of the security strategy in the mental sphere should be considered proactive actions, within the framework of a unified system for forecasting and preventing hybrid threats and challenges in the information sphere.

Russia steadily stands for the speedy development of universal norms and principles of responsible behavior of states in the information space, for the development under the auspices of the UN of the Convention on Combating Crimes in the Sphere of the Use of Information and Communication Technologies, as well as for the internationalization of Internet management.

Information sovereignty of the State: criteria and indicators (E.I.Sobolev)

The idea of state sovereignty has been around for a long time. Without sovereignty, it is difficult to imagine a modern state that successfully and actively operates on the world stage. Its essence is the independence and supremacy of power in making and executing decisions both within the country and abroad. The concept of information sovereignty has long been absent from the world legal practice. The first steps towards developing a definition of information sovereignty were taken only in the last decades of the 20th century. This is due to the active development and implementation of technological innovations in people's lives, among which traditional and easy-to-use sources of information were replaced by more complex ones - cellular and satellite communications. The world wide web, the Internet, has become the crowning achievement of these technologies. The Internet has provided mankind with a new platform for interaction - a virtual space in which people could freely communicate with each other regardless of distance, exchange and receive the information they need. It was quite difficult to develop legal mechanisms for regulating the activities of participants in this space, for using data volumes. Nevertheless, active work

21 The SF Defense and Security Committee discussed ways to counter mental warfare. Available: http://council.gov.ru/events/main_themes/135291/.

was carried out to create legislative initiatives, also to comprehend the state presence in the virtual space. A.Efremov identifies 4 main stages in the formation of the concept of information sovereignty [2].

The first stage took place in the 1980s. At that time, the Internet was still at the development and testing stage. Due to the fact that the exchange of information through the use of satellites, television and radio has acquired a transboundary character, the researchers decided to consider the relationship between national sovereignty and the right to freedom of information [8]. After comparing the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966) with state restrictions on the flow of information, they concluded that there are differences in the interpretation of aspects of state sovereignty between developed and developing countries [2:205]. For the first category of countries, unlimited exchange of information is a component that strengthens their sovereignty, while for the second, freedom in the dissemination of data poses a danger to sovereignty [8:267]. This difference can be traced even today.

The second stage is related to the consideration of the Internet itself in the context of a threat to the sovereignty of the state. Its rapid development in the 1990s made it possible to analyze in detail the relationship between the international network and the state. For example, one of the Chinese researchers W.Gong put forward the idea of two components of information sovereignty: external and internal. External includes the legal equality of states and their independence in the creation and dissemination of information. Internal is the legal rule in ensuring the information order and the implementation of information policy [9]. It is said about the continuation of the tendency of developing states to protect their own sovereignty, and developed ones to call for a free exchange of data. In the works of American researchers, no emphasis is placed on the degree of development of the state, since the basis is the belief that the vast majority of countries are taking active steps to protect and strengthen their sovereignty. Moreover, their works indicate that the majority of citizens support these initiatives [2].

In the third stage, up to our days, researchers highlight the concept of data sovereignty. According to this concept, in a number of countries (Russia, France, Germany, Australia) legislative acts were adopted that obligated to save the storage of personal data of citizens on the servers of the country to which they belong [10]. Interaction with data volumes in these states became subject to the jurisdiction of the state in which these data were located. Modern researchers consider the desire of states to develop data sovereignty understandable and reasonable, since it is aimed at maintaining the confidentiality of information, protecting and protecting the interests of the state in the field of ensuring the integrity and availability of data. The concept is spreading not only among Western states, but also in the scientific works of researchers in China, South Korea, and Indonesia. Big data technology is also being studied, which since the early 2010s has been associated with the concept of data sovereignty.

The fourth stage in the development of the concept of information sovereignty is under study. It is associated not so much with the regulation of information flows, but with control over the information and communication infrastructure (IT infrastructure). It has

been reflected in a number of international studies. For example, according to the report of the group of government experts of the 68th session of the UN General Assembly, which was held in 2013, any state activity in IT and IT infrastructure, including their use, is subject to state sovereignty and the principles and international norms arising from it[22]. In addition to this report, two years later, at the 70th session of the UN General Assembly, that approach was developed and was proposed an approach that would allow in practice the application of international law in matters of the use of information and communication technologies by the state. It was approved that the state has jurisdiction over the IT infrastructure located on its territory. The principles of non-interference in the affairs of other states, sovereign equality, state sovereignty and the resolution of disputes through peaceful means were emphasized[23].

In the research works, various terms are used: digital sovereignty, cyber sovereignty, sovereignty in the information sphere, the Internet of sovereignty. Various definitions are also given to that phenomenon. For example, E.Zorina distinguishes two aspects of information sovereignty, ideological and technical. The ideological aspect includes a developed national idea or national ideology, the achievements of high-level mass culture, the presence of propaganda and legislation in the information sphere. The technical aspect includes the existence of national software, own social networks, search engines, national electronic payment system [4]. V.Bukharin in his work supplements the technical aspect with the presence of microelectronics, network equipment, the national segment on the Internet, cryptographic algorithms and protocols, a functioning navigation system and its own means of protection [1].

In the work of E.Zorina, such criteria of information sovereignty [3] are given. The first is the state's high level of computer and communication systems. They are responsible for the creation and dissemination of information. Without the proper level of provision with these systems, the potential for sovereignty in the network space is limited. The second is the availability of means to protect the above systems: antiviruses, firewalls, etc. Their absence threatens to leak or steal personal data of users and information constituting a state secret. Data protection tools must be created by the state, otherwise there is a risk of dependence on external providers. The existence of a national Internet infrastructure is an important indicator of a state's sustainable information sovereignty, since its own search engines and social networks open up opportunities for state control over processes in cyberspace. One of the criteria is also considered a national payment system, which avoids the risks of external political pressure. In Russia, such a payment system already exists and continues to develop.

Also, the state must have a developed propaganda mechanism and a developed media network, not only within the country, but also must have channels for broadcasting

22 Report of the Group of governmental experts on developments in the field of information and telecommunications in the context of international security.A/68/98. Available: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.

23 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. Available: https://documents-ddsny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement.

in foreign countries. The purpose of these channels is to provide domestic and foreign audiences with information that meets national interests. The role of the media, both through the usual forms of broadcasting and through the Internet, is enormous. No wonder the media is called the fourth power. They can present the main news in a neutral way; they can give their own assessment of them, keep silent about incidents that negatively characterize the official position. Therefore, the media, as the most proven political tool, carry out propaganda.

The next feature is the creation and dissemination of products in the field of culture at the state level. For example, products of the cinema or the music industry. Popularization of these products can contribute to the formation of a positive image of the country among citizens of foreign countries. This also includes the creation of the image of the state through mass culture and the Internet. Good examples are the Winter Olympics in Sochi in 2014 or the FIFA World Cup in 2018. Increasing the attractiveness of the country not only meets the interests of information security, but also allows attracting additional investment and making new partners. In diplomacy, the formation of a positive image of the state by the above methods is called «soft power». Another sign of information sovereignty is the active use of the Internet space for the dissemination of ideas that meet the interests of the state. They can be embedded in videos and other publications. Their focus is to discredit negative information and influence the mass consciousness. As an example, E.Zorina cites Wikipedia, one of the most popular sources of information on the Internet [3]. Speaking of criteria, we should not forget about the issues of institutionalization. The information field requires the state to create institutions with assigned responsibilities, such as ministries and departments. Institutionalization requires a legal framework - this is the next criterion. Legal mechanisms of influence provide not only protective functions, but also allow the state to take adequate actions to ensure the integrity of its information sovereignty.

An analysis of the experience of ensuring information sovereignty in China, the United States and Russia shows a number of distinctive features. China has a number of specific features in information and communication technologies. Today, China is one of the leaders in the use of cyberspace. A characteristic feature of the Chinese development of the network segment is the active borrowing of foreign technologies. Only in the last decade, China has moved to the development of its own products. Nevertheless, the tendency to actively attract foreign innovations continues. The Internet for the Chinese government is not only a part of the sovereign space, but also a means for exercising almost total control over its own citizens, actively cultivating online ethics in the spirit of Confucianism and the Chinese model of socialism. The National Cyber Security Strategy, approved in 2017[24], highlights both the opportunities and threats presented by the evolution of information technology. Security is a priority in any form of cyberspace development: “security is a necessary condition for development, and any development that occurs at the expense of security is unsustainable. Development is the basis of security, and failure to develop is the greatest danger.”

24 National Cyberspace Security Strategy. Available: www.cac.gov.cn/2016-12/27/c_1120195926.htm.

China has been deeply involved in security issues since the early 2000s. The terrorist acts that shook the world on September 11, 2001 forced many countries, including China, to reconsider and tighten their policies in the information environment. The Internet in China is under the vigilant supervision of relevant structures. There is even an Internet police that monitors the incoming data flow to websites, forums and social networks [5]. One of the most famous Chinese inventions for the protection of information sovereignty is the so-called "Golden Shield", better known in the West as the "Great Firewall of China". This project, which has been operating since 2004, is responsible for filtering content on the Internet and blocking dangerous sites. It consists of 3 technological components. The first one is the technology of accumulating statistical information, checking and filtering network packets by their content. The second is a merger between the filtering mechanism and the proxy server. The third component is an advanced data filtering mechanism, featuring a wider range of information analysis. The Golden Shield project is successfully fighting terrorists, quickly detecting their cells in the network. Its effectiveness is evidenced by the number of terrorist attacks in China and neighboring Asian states [7].

The Chinese Internet blocks foreign websites and social networks such as Wikipedia, Facebook, Twitter. Western media is also inaccessible to Chinese users. Since 2017, online anonymity has been banned. The use of Internet became available only after registration with an indication of your real name and contact information. Anonymous commenting, discussing or creating Internet posts is not possible. Moreover, technologies to protect information sovereignty are actively used to control public behavior. In 2020, a previously experimental social credit system was introduced throughout China, rewarding or punishing citizens depending on the nature of their activity both in life and on the Internet. For its implementation, several hundred million new generation cameras are planned to be installed throughout the country. Depending on the high or low amount of social loans, a person will receive benefits when using transport, shopping, traveling around the country, or restrictions on using the Internet, quality medicine, and purchasing expensive real estate, respectively. Those who lose a significant amount of their credit risk is going to be completely isolated, since communication with such marginalized persons of the social system will not be encouraged by the government.

The Chinese themselves are calm about the introduction of the new system, as they are quite disciplined in matters of control over their personal lives. China is not only using means to protect its information sovereignty, but is also trying to prevent potential threats. The country has its own army of Internet trolls, consisting of government-funded bloggers (their total number is from 300 thousand to 2 million people), and cyber troops separately from them. The former are responsible for maintaining the pro-government line in controversial issues on the Internet in difficult times for the country, during periods of various crises and upheavals. Internet trolls leave a lot of comments in support of the ruling party, skillfully change the topic of discussion and never attack the opponent directly. Chinese cyber troops are acting more seriously in the Internet space. Their activities are often covered by foreign media. The main activity of this type of armed forces is cyber espionage and hacker attacks. Thus, China, despite its technological lag behind the leading

countries of the world, has provided its information sovereignty with serious protection based on an obedient society under state supervision, total filtering of information on the Internet and the actions of law enforcement agencies. However, the authoritarian methods of this country are not suitable for everyone.

The United States, being one of the leaders in technology and global control over information flows, has been developing concepts for ensuring its own information sovereignty for a long time. Today, the main document responsible for the practical application of measures to ensure information sovereignty is the National Cyber Security Strategy, adopted by President Donald Trump in 2018, and the US Department of Defense Cyberspace Strategy of the same year[25]. These documents put the protection of American democratic values at the forefront, therefore, a distinctive feature of the US information sovereignty (according to the official government line) is openness and accessibility in receiving and exchanging information. The US government guarantees free access to the Internet and other channels of social communication. It is the unlimited movement of data, according to the authors of the strategy that ensures the security of the American society, its stable development, financial well-being and technological superiority

The main role in ensuring information sovereignty is assigned to the federal government. The strategy describes the prospects for further centralization of the management and control of the security of the civilian sector in cyberspace by increasing transparency in interdepartmental affairs, eliminating duplicative actions that complicate the procedure for fulfilling the tasks assigned to the government in the information environment. The strategy gives equal responsibility to the government and the private sector in ensuring the security of critically vulnerable infrastructure. IT vendors play an important role in the US economy, so to keep them productive, the federal government is committed to actively work with them to counter hacker attacks together.

The United States is actively working to improve its laws in order to provide law enforcement agencies with additional opportunities to track illegal actions on the Internet. These include both criminal activity using computer systems inside the country, and hacker attacks from outside in the form of hacking, data theft, organization of leaks, attacks on information infrastructure. The United States is open to cooperation with foreign countries in matters of security in cyberspace. Through cooperation, joint projects with its partners, including both entire countries and representatives of individual industry groups (industrialists, scientists), civil society, America cannot only strengthen its digital sovereignty, but also spread its influence, which would provide the United States with a leading position in development of information and communication technologies. The government actively promotes the development of creative potential in the information field, providing financial support for projects such as artificial intelligence and quantum informatics. To improve the effectiveness of digital sovereignty, it is planned to upgrade the existing IT infrastructure with next-generation technologies.

25 Department of Defense Cyber Strategy – 2018. Available: https://www.cybercom.mil/About/Mission-and-Vision/.

The actions of the United States to ensure information sovereignty must coincide with the content of all international norms. The Government will encourage compliance with these standards and prove by its own example the need to comply with them. In case of violation of these norms, as well as a threat to digital sovereignty, the United States has the right to use all the tools at its disposal to influence those whose activities in cyberspace are dangerous: diplomatic, informational, military (kinetic and digital), financial, intelligence, law enforcement capabilities. Thus, the protection of its own information sovereignty in the United States is closely intertwined with the principles of deterring potential adversaries in the information field at the global level. A major role in achieving these goals is played by American intelligence, which online identifies the sources of information campaigns, disinformation, hacker attacks and transmits this information to the federal government. The loudest example of recent US actions in the information space has been the campaign to accuse Russia of interfering in the US elections in 2016 as a direct encroachment on the country's sovereignty in cyberspace. Thus, the United States has created one of the most complex systems to ensure its information sovereignty.

A serious technological base, a powerful intelligence apparatus and the geopolitical position of the leader of the Western world allow the US government to implement its goals quite effectively, to solve the tasks to protect state interests in cyberspace set in doctrinal documents, to impose its own rules of the game on weaker participants and to expand its influence. The emphasis of the US actions on the Internet is on close cooperation with its partners, openness and respect for human rights. However, after the events of September 11, the American government significantly expanded the powers of law enforcement agencies in matters of information control, which became equivalent to monitoring the actions of its citizens. On this basis, scandals periodically occur, the loudest of which are connected with the confessions of the escaped employee of the American special services Edward Snowden and the Australian journalist Julian Assange. The data that they provided to the public hit hard on the image of the United States and shook the position of this country as the leader of the free world.

The Russian Federation is actively developing the concept of state sovereignty in the digital space. Nevertheless, now Russia does not have such a detailed strategy as the United States or China. However, it is impossible to say that information sovereignty is not paid attention to. On the contrary, improving security in this area is one of the priorities of our country.

In 2016, the Information Security Doctrine of the Russian Federation was adopted[26], which details measures to protect information sovereignty, as well as to defend Russia's national interests in the information sphere. National interests include actions to protect the constitutional rights and freedoms of citizens in obtaining and using information; to ensure the uninterrupted operation of the information and communication infrastructure, where priority is given to critical infrastructure facilities; as well as to develop knowledge-intensive branches of information technology and the electronics

26 The Information Security Doctrine of the Russian Federation. Available: http://www.scrf.gov.ru/documents/6/5.html.

industry, to improve current activities; to convey to internal and external audiences relevant and reliable information about the policy pursued by Russia and the official position of the country on significant issues; to use of IT technologies to ensure national security in culture; to cooperate in creating an international digital security system, to strengthen an equal strategic partnership in the information sphere. These measures are aimed at creating a sustainable and protected from any form of influence information infrastructure, stable development of the country, protection of the rights and freedoms of citizens.

The protection of information sovereignty is achieved through ensuring information security in the following areas:

- in the field of defense through conflict prevention using digital technologies, detection of information threats;
- in state and public security by combating the propaganda of extremism, calls to undermine sovereignty and change the constitutional order using information technology; countering the activities of foreign intelligence services on the territory of the country; increasing the security of critical information infrastructure, its functioning; improving information protection mechanisms and increasing the effectiveness of information policy implementation;
- in economics by eliminating the technological dependence of domestic industry on foreign countries; improving the competitiveness of the Russian information services sector; developing its own electronic database;
- in science, technology and education through the development of scientific research, the creation of promising information technologies; the formation of experienced personnel in the field of digital technologies;
- in strategic stability and partnership through the implementation of an independent policy to realize of national interests; assistance in the formation of international legal mechanisms in the field of information technology and the system of international information security; coverage of Russia's position on digital security; development of the national segment of the Internet.

The doctrine identifies the vulnerable sides of Russia's information sovereignty. These include: the weak competitiveness of domestic digital technologies, the state's dependence on foreign innovations, especially the electronic computing base, the low level of education of citizens in matters of personal information security, the weak pace of equipping production with Russian information technology components, the serious struggle of the leading states in the information sphere to maintain their dominant position in the world. In his article, which assesses the state policy in the field of information security, D.Litvinov supplements the list of weaknesses with sanctions imposed by the West, the lack of an orderly structure in the regulatory framework, the lack of budget funds to implement the declared actions [6]. The digital security doctrine is a component of the National Security Strategy of the Russian Federation adopted in 2021. It summarizes the above measures to achieve a secure information environment. Thus, Russia considers the protection of information sovereignty to be one of the components of ensuring national security. Despite the current number of

problems in the practical implementation of the measures enshrined in the doctrines for the state protection of its sovereignty in all areas, we can assume that the development of information sovereignty in our country is actively engaged.

Ensuring the information sovereignty of states (D.I.Sedunov)

The need to ensure information sovereignty was clearly manifested in the events related to Russia's special operation in Ukraine. To compare Western and Russian approaches to ensuring information sovereignty, we propose three main criteria according to the technologies used: the speed of the impact (how quickly the technology is used), the cost of the impact (the resources necessary for the application of the technology), the duration of the impact (the prolongation of the result of the applied technology).

In the "Western" approach to ensuring information sovereignty, using the example of the current conflict "collective West against Russia", the following three key technologies for ensuring information sovereignty can be identified:

Strict censorship of information, blocking of any information other than state policy. Technologically, this is manifested in the ban of official media belonging to the opposing side (RT, Sputnik, and other channels of the Russian Federation were closed); in the strict censorship of social networks (removal and blocking of any information from the Russian Federation from the information field in FB, YouTube, Twitter, Instagram); a ban on the dissemination of official information in the media from the Russian Federation (blocking interviews, broadcasts, publishing only interpretations that are beneficial to Western politicians in isolation from the context).).

2) Creating false content aimed at discrediting Russia and its allies. Technologies of fakes, publications of false analytics; active provocations to create false stories and informational occasions in the media are widely spread; as well as links to unreliable and unverified sources containing information necessary for Western politicians to justify their actions to their citizens.

3) Emotional presentation of information: emphasis on affect, not on rationality, ignoring logic and facts.

The Russian approach to ensuring information sovereignty differs from the Western one:

1. Detailed exposure and analysis of fakes by both official state authorities and the patriotic blogosphere. In particular, we are talking about the channels of the Ministry of Foreign Affairs of the Russian Federation, the Ministry of Defense and others in the Telegram; about providing reliable information in the form of stories from the scenes of events and interviews with eyewitnesses, about the publication of official documents of foreign countries confirming hostile intentions towards Russia and the population of the DPR and LPR.

2. Russia blocks hostile actions and restricts the work of anti-Russian aggressive media and new media, social networks that openly pursue aggressive information policy on FB and Instagram; gives symmetrical responses to the ban of Russian media abroad; expand

the number of non-profit organizations and media in the group of foreign agents; adopt the regulatory legal acts to ensure the information sovereignty of Russia.

3. Russia activates the patriotic blogosphere.

Conclusions

Comparing the Russian and Western approaches according to the previously identified criteria, we can draw the following conclusions. Severe censorship in the field of information works quickly, only a prepared point of view is communicated to the population, and alternative points of view are completely excluded. At the same time, maintaining and maintaining the necessary infrastructure for censorship activities requires significant financial costs. Violation of the information blockade over a long period of time leads to a violation of information sovereignty (an example from history is the Iron Curtain of the USSR).

The joint use of false information technologies with "emotional mobilization" quickly brings results, but requires high financial costs for the preparation and presentation of information. This, as with strict censorship of information, sooner or later may lead to a violation of information sovereignty.

The specifics of the technologies used in the Russian version are the work for a long time perspective with minimal investment of financial resources. This approach makes it possible, under conditions of financial constraints, to build a promising information policy and strengthen information sovereignty.

Discussion

Having studied the approaches of China, the United States and Russia to the issue of organizing and protecting information sovereignty, it is possible to determine the current trends. First of all, the development by various countries of a set of measures to create a stable and secure information environment is caused by the increased role of information and communication technologies in all spheres of people's lives at the same time. If thirty years ago only a narrow circle of specialists thought about the existence of such an extensive, multifunctional and high-tech data exchange system as the Internet, today the use of the Internet has become an integral part of our daily routine. Its capabilities in the modern world clearly exceed all the expectations of those who were involved in the development of this innovation at the initial stages. The widespread digitalization of economic, social, political, cultural processes implies the existence of legal and technological mechanisms for their implementation, as well as tools for protecting the transformed information.

Secondly, the coronavirus pandemic that began two years ago has accelerated the introduction of information technology into people's lives, especially in the organization of

 ISSN 2782-3067 (Print)

work. It required additional costs and additional decisions to form its sustainable structure. Today, as deaths from new strains of the virus have fallen, many experts are of the opinion that the pandemic will end soon. However, the end of the epidemic is unlikely to affect the desire of the global elite to deprive themselves of all the advantages created by information and communication technologies in recent years, as they have become a good platform for additional supervision over the activities of their own citizens.

Thirdly, cases of cyber espionage, hacker attacks and the use of the power of social networks to control social consciousness have increased. Countries with underdeveloped cyber infrastructure have little to offer against technologically advanced competitors.

The first and perhaps the key vulnerability of Russia's digital sovereignty lie in technological weakness in the face of external dangers. In the case of a planned large-scale hacker attack, information infrastructure objects can be disabled. The situation is complicated by the strong dependence of the state on imports of high-tech products. If these supply channels stop, not only the further improvement of digital sovereignty, but also the technological development of the country as a whole can significantly slow down and cause a number of problems. The potential for the production of domestic analogues of Western electronic components is at a very low level. It is no secret that in the third decade of the 21st century, the most developed countries are actively waging cyberwars around the world. The targets of such attacks are strategically important objects in the digital space and vulnerable at the same time. Thanks to the developed malicious programs that penetrate the devices, their functioning is disrupted or completely stopped.

The consequences can immediately affect the economic, political, energy, and defense spheres. Another threat to the information sovereignty of our country is the information war, which is actively waged by some foreign states. Its essence lies in the juggling of facts, the manipulation of data and the formation of a distorted picture of the world, where the image of Russia is negative. A clear example of this war was the propaganda of the Western media about the imminent start of a large-scale war between Russia and Ukraine. Specific dates were given for the beginning of the invasion, but on these days the declared invasion did not occur[27].

Despite this significant miscalculation, the information war has an impact: an unstable market, the growth of anti-Russian sentiment in Europe and the escalation of the situation around Ukraine. As a source of threat to information sovereignty we note the use of social networks as a platform for organizing illegal activities. One example is the use of the Telegram messenger to coordinate protest movements on the territory of Belarus in summer and autumn of 2020. The high level of anonymity provided by this messenger allows not only to hide your identity, but also to ensure security and confidentiality in the transfer of information, which was used by the organizers of the protests. The most famous channel on Telegram during the turmoil was NEXTA[28].

27 There is a cloudless sky over Ukraine. How the West waited all night for Russia's «invasion». Available: https://www.gazeta.ru/army/2022/02/16/14541109.shtml.

28 How four people created the main Telegram channel of the Belarusian protest with an audience of 2 million subscribers. Available: https://www.forbes.ru/tehnologii/407119-kak-chetyre-cheloveka-sozdali-glavnyy-telegram-kanal-belorusskogo-protesta-s.

Of course, even good Telegram protection can be bypassed and real participants can be identified, but this requires higher technologies and, most importantly, time. And in a period of political instability, we have no enough time. During the crisis in Kazakhstan in January this year, this messenger was also used, not only by local opposition forces, but also by foreign participants leading remote control of the riots that broke out [29]. The problem of social networks is not only the organization of opposition movements. Anonymity is also enjoyed by terrorist cells, traffickers of illegal substances; distributors of child pornography and other prohibited content[30].

The uncontrolled circulation of cryptocurrencies is another threat to Russian sovereignty in cyberspace. Bitcoin is one of the most common today. Since the cryptocurrency is not secured by anything, which means it is not capable of being managed, this creates a certain risk for the state economy. Despite the decline in the value of key cryptocurrencies, the threat emanating from them does not disappear, and their market requires legal regulation by the state. Among the additional threats to information sovereignty, one can single out scam on the Internet, which includes offenses and crimes of various scales. Cybercrime continues to evolve, and the costs of it continue to grow.

Each of the above threats can either be solved or its risk can be reduced. It would be good to take the following measures:

- significantly increase funding for the domestic high-tech industry, and most importantly, support Russian research in the field of computer technology in order to reduce dependence on foreign products to a minimum; increase the security of critical infrastructure facilities;
- continue to develop cybersecurity in the Armed Forces of the Russian Federation, build up military potential in the field of digital technologies, use the experience of foreign states in similar conditions and thereby more successfully resist their attacks in cyberspace;
- pursue an active policy in the information sphere aimed at combating false reports; form a clearly articulated official point of view on vital issues and timely communicate it to a wide audience inside and outside the country; refute provocative statements, defend our interests in a balanced and reasoned manner;
- be attentive to publications in social networks that may threaten information sovereignty; track illegal and other prohibited by law activities;
- ensure a clear and consistent state policy in the field of cryptocurrency circulation;
- develop and implement the state policy in the field of educating the population on information security issues, the rules for the safe interaction of citizens with digital technologies, their skillful use (pay special attention to older people as the group most at risk of Internet scam);
- strengthen control over illegal activities on the Internet.

29 According to NEXTA patterns: Who is behind the Telegram channel from Kiev, which called for a revolution in Kazakhstan. Available: https://life-ru.turbopages.org/life.ru/s/p/1462931.

30 In Russia, terrorists actively use Telegram for communication, the FSB said. Available: https://ria.ru/20170626/1497271423.html.

Conclusions

Technological and legal understanding of the concept of information sovereignty began more than 40 years ago and continues up to this day. The development of the concept is closely related to the development of technologies in general from cellular and satellite communications to the global Internet and cloud storage technology. This concept affects not only issues related to all possible types of information, but also its relationship with international standards in the field of human rights protection, in protection of state sovereignty, in matters of the use of information and communication infrastructure.

In the 21st century, it is difficult to imagine a country that would not take care of its information sovereignty and, in particular, security in cyberspace. Despite the fact that today information sovereignty has not yet been given due attention by scientists, the participants of that scientific discussion express confidence that in the near future we will see new, deep research and scientifically reasoned managerial decisions. The moral and legal side of the issue also should be discussed. Of course, the sovereignty of the state is an integral part of the modern world and a guarantee of the security of society. However, in striving to achieve this security, it is important not to forget about the basic human rights enshrined in dozens of international documents, and not to try to ensure security solely for the sake of one's own unilateral benefit.

Summarizing the opinions of the participants in the discussion, we draw a number of conclusions:

- The concept of information sovereignty has been developing for more than 40 years, overcome four stages of its formation from technical and legal understanding of the position of the state among data flows to international standards in the field of control over digital infrastructure.
- The signs of information sovereignty are: availability of a technological base and means for its protection, the existence of a national payment system, the implementation of propaganda and improving the image of the country in the information space, the dissemination of ideas that meet the interests of the state in it.
- Countries that differ from each other, such as China, the United States and Russia, demonstrate different approaches to the organization of their information sovereignty. In China, it is achieved due to total control over information, lack of full access to foreign sources and a powerful network protection system. The United States enjoys its leading position in the field of technology, actively involves the private sector in cooperation and has equipped cyber forces to protect information sovereignty. In Russia, ensuring state sovereignty in the information space is achieved through the Information Security Doctrine and National Security Strategy. The doctrine names the following tasks: the development of the domestic segment

of the Internet, increasing the resilience of strategic facilities to hacker attacks, the development of information technology and international cooperation to create legal documents that ensure fair and secure use of cyberspace.

- Among the trends affecting the development of ideas about the information sovereignty of the state, one can single out: the rapid growth of research in the digital industry and the creation of high-tech products; the coronavirus pandemic, which caused a leap in the use of these products in everyday life, the fact that many forms of interaction between people have switched to online mode, the use of cyberspace as a platform for fighting in the form of hacker attacks and espionage.
- Russia's information sovereignty faces such serious challenges as technological dependence, cyberattacks, information wars, and the use of social networks to ensure anonymity while committing illegal actions, unregulated cryptocurrency markets, Internet scam.
- The threats existing for our country can be solved if additional measures are taken to develop and introduce domestic high-tech products, equip the Russian army with the necessary means to repel possible types of attacks in cyberspace from foreign states; to create technologies to combat fake news and information, to monitor social networks for the placement of information threatening sovereignty in them, ensuring the policy in the field of cryptocurrencies and promoting the safe use of the Internet among citizens.

References

1. Buharin V.V. (2016), Components of the Digital Sovereignty of the Russian Federation as a Technical Basis for Information Security, MGIMO Review of International relations. No. 6. p. 76–91. (in Russian)
2. Efremov A.A. (2017), Formation of the Concept of Information Sovereignty of the State, Law. Journal of the Higher School of Economics. No. 1. P. 201-215. (in Russian)
3. Zorina E.G. (2017), Information Sovereignity of the Modern State and the Main Tools to Ensure It, Izvestiya of Saratov University. New Series. Series Sociology. Politology. Vol. 17, No. 3. P. 345–348. Doi: 10.18500/1818–9601–2017-17-3-345-348. (in Russian)
4. Zorina E.G. (2017), Distortion of the Meanings and Senses of Political and Historical Events in Multilingual Versions of Wikipedia Articles, Vlast. Vol. 25, No. 3. P. 211-214. (in Russian)
5. Ibragimova G. (2013), China's Strategy in Cyberspace: Issues of Internet Governance and Information Security Ensuring, Security Index. No. 1 (104). P. 169-184. (in Russian)
6. Litvinov D. A. (2019), Assessment of Russia's Cybersecurity Policy and Possible Options for its Improvement, Vestnik nauki I obrazovaniya. No. 19-2 (73). P. 76-82. (in Russian)
7. Chekmenyova T.G., Ershov B.A., Trubitsyn S.D., Ostapenko A.A. (2020), China's Information Security Strategy: Political and Technical Aspects, Bulletin Social-Economic and Humanitarian Research. No. 7 (9). P. 78-97. (in Russian)
8. Damon L. (1986), Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Date Flow Problems, Fordham International Law Journal. Vol. 10. Issue 2. p. 262–287.
9. Gong W. (2005), Information Sovereignty Reviewed, Intercultural Communication Studies. Vol. XIV. Issue 1. p. 119–135.
10. De Filippi P., McCarthy S. (2012), Cloud Computing: Centralization and Data Sovereignt, European Journal of Law and Technology. URL: http://ssrn.com/abstract=2167372.

11. About the authors

GRIBIN Nikolai P. DSc (Law). Professor. Leading Researcher, Institute of International Studies of the Moscow State Institute of International Relations (University), Russian Foreign Ministry. htpps://orcid.org/0000-0001-9141-445. Address: 76 Vernadsky Avenue, Moscow, 119454, Russian Federation. n.gordin40@gmail.com.

KOKHTYULINA Irina N. CandSc (Polit). Scientific Secretary of the Scientific Council of the National Institute for Global Security Studies. Address: 8 Dvintsev str., office 1, Moscow, 127018. expobroker@yandex.ru.

SEDUNOV Denis I. Postgraduate student of the Russian Presidential Academy of National Economy and Public Administration. Address: 82 Vernadsky Avenue, Moscow, 119571. DenisSedunov@list.ru.

SOBOLEV Egor I. Intern of the National Research Institute for the Communications Development, student of the Peoples' Friendship University of Russia. Address: 119034, Moscow, korobeynikov lane, 22, p.1. 1032193499@rudn.ru.

Authors contributed

GRIBIN Nikolai P. DSc (Law). Professor. Leading Researcher, Institute of International Studies of the Moscow State Institute of International Relations (University), Russian Foreign Ministry. htpps://orcid.org/0000-0001-9141-445. Address: 76 Vernadsky Avenue, Moscow, 119454, Russian Federation, n.gordin40@gmail.com.

KOKHTYULINA Irina N. CandSc (Polit). Scientific Secretary of the Scientific Council of the National Institute for Global Security Studies. Address: 8 Dvintsev str., office 1, Moscow, 127018, , Russian Federation, expobroker@ yandex.ru.

SEDUNOV Denis I. Postgraduate student of the Russian Presidential Academy of National Economy and Public Administration. Address: 82 Vernadsky Avenue, Moscow, 119571, , Russian Federation, DenisSedunov@list.ru.

SOBOLEV Egor I. Intern of the National Research Institute for the Communications Development, student of the Peoples' Friendship University of Russia. Address: 22, p.1, Korobeynikov lane, 119034, Moscow, Russian Federation, 1032193499@rudn.ru.

Conflicts of Interest Disclosure

The authors declare that there is no conflict of interest.

Article info

Submitted: Mart 28, 2022. Approved after peer reviewing: April 5, 2022. Accepted for publication: April 27, 2022. Published: 27.06.2022.

The authors read and approved the final manuscript.

Peer review info

«Russia & World: Scientific Dialogue» thanks the anonymous reviewer(s) for their contribution to the peer review of this work.