POLITICAL IMPLICATIONS OF ASSERTIONS OF DIGITAL SOVEREIGNTY IN RUSSIAN STRATEGIC PLANNING DOCUMENTS

By
Kristina Boiakova

Submitted to Central European University
Department of Public Policy

In partial fulfilment for the degree of Master of Arts in Public Policy

Supervisor: Assistant Professor
Cameran Ashraf

Vienna, Austria

2022

Copyright notice

Abstract

This thesis sets out to examine assertions of digital sovereignty of the Russian Federation and its potential political implications. In this study strategic planning documents are investigated with a single case study as a research method. The study is designed according to the principles of the qualitative research design, the descriptive research strategy is chosen in this paper. The unique case of Russian information policy and formation of its digital sovereignty reflected in the official documents which constitute data analyzed in the empirical section of this study. The author finds that in relevant strategic documents including information security section of the National Security Strategy contains some ideological implications. It is suggested that new stage of digital security in the Russian Federation contains ideological implications and political views on the world order and cyberpshere.

Key words: Digital sovereignty, Russian public policy, information security, national security, public policy, information sovereignty.

Acknowledgments

I would like to express my gratitude in this section to people who helped me throughout the process of conducting and writing this study. First, I would like to thank my thesis supervisor Professor Cameran Ashraf for his help and guidance. I am indebted to Professor Cameran Ashraf for fascinating the Introduction to Cyberconflict course in Spring Term which encouraged me to look at the thesis from various perspectives. Also, I am thankful to my family and close friends who supported me during this academic year at Central European University and during the process of writing this study. I am grateful to Professor Thilo Bodenstein for the valuable advice for the fascinating lectures I had an opportunity to attend during the Qualitative methods for Public Policy course in Winter Term. Also, I would like to thank CEU Center of Academic Writing for the opportunity to improve my writing skills.

Table of contents

Introduction

In the past two decades the emergence of different kinds of information technologies has been witnessed by individuals, companies, and nation-states. Accelerated progress in the field of technologies has impacted not only everyday life, but has also attracted the attention of countries all around the world. Worldwide, the role of the state itself and its capacity even had been questioned – transnational global IT corporations (FAMGA, BAT, etc.) started to collect enormous amounts of data of individuals without regard to their nationality and some of them became much wealthier than some states. Interestingly, the leading IT giants were considered as independent actors in the global arena. Some similarities with the states were revealed – such as their governing bodies and the introduction of the corporate policies, however, the most important component, sovereignty, has not been obtained.

Sovereignty is still the main characteristics of a state. The ability to set their own policies on their territory independently has challenged the independence of the global IT corporations and the international technologies. The Internet, the global network, is not completely "global" due to the internet providers – satellites are owned by certain states. The new question appeared: how to secure the cyberspace? The international information security is an issue discussed on the international level – the United Nations as an international organization and arena organized the negotiations on the adoption of a resolution on the global cybersecurity. The European Union, for example, adopted the Digital strategy of the EU in February 2020. This document defines the digital borders of the political entity. Thus, the digital space can be divided not only between nation-states but also by supranational organizations which share political and economic space. Such initiative was discussed in the EAEU digital agenda in 2019 on Eurasian economic mission. Digital sovereignty and digital independency issues were raised on the agenda as well as the global digital rivalry. Thus, the issue of digital sovereignty is closely related to the subjectness of political entities, including international economic unions. From the technological perspective, the relevant critical infrastructure is supposed to support the digital ecosystem and digital space. However, in

this thesis the exploration of such infrastructure will not be implemented since this paper has the aim in the policy studies. One of the digital sovereignty prerequisites is, however, the level of digital maturity of the Russian digital economy. “Industry 4.0” as a new economic paradigm in Russia and other countries the digital realm became possible. Hence, the digital economy, at present, is considered as a separate direction of socio-economic development. And, at the same time, information security had been defined as a separate direction in the Doctrine of the national strategic security in 2015. We are witnessing the emergence of the conceptually new type of borders and state “control over information, communications, data, infrastructure related to the Internet” (Gueham 2017).

International information security with various projects proposed by the UN members has been discussed in recent years. The concept of international information security implies the adoption of international treaties approved by the UN countries. The decision-making process on the international level and the content of the proposal by states might be studied, but in this study, as it will be explained later in the methodology and research design section, the case study of Russian digital sovereignty policies will be investigated. Even though the “Foundations of the national policy of the Russian Federation in the international information security area” official document was adopted in April 2021. Thus, lack of regulation in cyber realm on the international level constitute another issue that might be studied in jurisprudence.

Another perspective on the topic is the existence of various understandings of the motivation of digital sovereignty formation of certain political entities (nation-states, unions, etc.) A comparison of such motivation was made by Dubin et. al (2021) based on the data by Efremov (2017) and Liputsov (2011). One of the criteria is targets of the digital sovereignty formation. The Russian Federation, the United States of America and the European Union were compiled in the academic article. The authors claim that these three actors have completely different targets: in the Russian case the technological independence from international IT companies and effective cyber security mechanisms against any attacks in the cyber realm.

I focus on the national policy in this new chapter of policy area in this study because it reveals valuable insights on the national information policy. The information security and information policy are closely connected in this area. Moreover, the concept of digital sovereignty itself has not been investigated in the Russian policy studies yet. The existing academic articles define the stage of the digital ecosystem of the Russian Federation and make attempts to conceptualize the new concept. Especially in the Russian discussion, there is a lack of publications on the defining the features and formation of digital sovereignty. Nevertheless, some attempts to distinguish the information sovereignty and digital sovereignty have been made. The original findings will contribute to the definition and the key features of the digital sovereignty formation of Russia. The contribution is primarily in nature cumulative because the deepened understanding of the phenomenon will be provided. After the "Landing Law" came into force in January 2022, Russian society started to pay attention and discuss the data protection and privacy policies, and also restrictions from the government which can be posed to the foreign global companies. At the same time, in the Russian society it was evident before that the Internet and access to the foreign content connects people to the global community (as the global village concept). However, the "Landing Law" raised discussion on the information space borders and the state power within its territory.

Thus, research problem of this study: despite the constitutive and strategic nature of digital sovereignty policies, some political implications are embedded in the documents. The secondary data for analysis consist of four current strategic planning documents: Doctrine of Information Security of the Russian Federation" (№ 646 December 5, 2016), "Strategies of the Information Society Development" (№203 May 9, 2017), "On the National Security Strategy of the Russian Federation" (№400 July 2, 2021), "On Approval of the Fundamentals of State Policy of the Russian Federation in the Field of International Information Security" (№213 April 12, 2021). Therefore, the following research question is proposed: what are political implications of assertions of digital sovereignty in strategic planning documents of the Russian Federation? Single

case study was chosen as a research method of thesis within the interpretive approach.

To answer the research question, the following objectives have been set:

1) to define the key concepts, including digital sovereignty and information security, and research gap in academic discussion;

2) to examine role of strategic planning documents in the Russian context;

3) to analyze the selected documents and its potential political implications;

4) to formulate contribution of the findings and fit thesis into the existing discussion.

This thesis has six chapters. First, general area of the thesis and justification are provided in the introduction. Academic discussion on the research problem is analyzed and overviewed in the literature review chapter. In the third section, methodology and research design are explained and justified. Also, conceptual framework and key concepts are described in the literature review part. In the empirical part of the thesis the Russian context is outlined and some insights from the history of the Russian cyberspace are delivered either. Moreover, the empirical part contains the conducted analysis of the selected strategic planning documents. Lastly, findings will be summarized the Discussion and Conclusions chapter.

Chapter 1. Literature Review

Digital sovereignty is a recent phenomenon in the political science and policy studies literature. In the Russian discussion it is also a new concept. In this chapter, I will review the existing publications on the issues of digital sovereignty and information policies both in theory and in the Russian context. The review allows to investigate what already scholars found on the issue and which key concepts have been used. Key findings from the mainstream studies are also provided, however, this comprehensive overview is rather analytical nature and aimed to reveal research gap in studying the issue.

1.1. State sovereignty in the digital realm

Nowadays there is no one established definition of the digital sovereignty in the digital realm at the international level. The concept of digital sovereignty is commonly used in technologically advanced countries. It is challenged whether the sovereignty in the digital sphere is equivalent to "digital sovereignty". And if it has become one of the essential attributes of states in the current world order. In information society it is undoubtful that data and information flows play important role at the supranational level. But internal sovereignty requires the governmental control over its territory. In this case, new policies might be initiated and formulated by states to achieve strategic autonomy in the digital sphere. This recognition by decision-makers to start formation of digital sovereignty is crucial and leads to the development of the strategic national documents. Progress in digital technologies challenged state capacity in digital realm, in a bulk of literature there is a theory of "cyber libertarianism" which explain this issue (Keller 2019). Two opposed approaches on the issue of traditional state sovereignty, hence, can be distinguished. First, it is a theory of "cyber libertarianism". According to the perspective, digital space is a qualitatively different and separate form of realm. The second approach denies the sovereignty in cyberspace (Tulikov 2016). It is named "multi-stakeholder internet governance", and it implies that states play only administrative role. Various non-sovereign stakeholders participate in consensual decision-making process on the wide internet realm (Klein 2002, Hofmann 2016) Defining cyberspace as

an autonomous phenomenon in relation to international law is problematic and discussed by law scholars. But the issue comprises the policy problem itself due to the obvious ongoing information and communication flows along with the cyber threats. In this case, critical infrastructure plays the strategic role in the state security. In this sense, the new nature of borders between states emerges, not only territorial but also in the digital realm. Consequentially, territory and sovereignty are not connected directly anymore, which have been noted by scholars (Anselmo 2006), (Benyekhlef & Gelinas 2001), (Marusitz 2014), (Adams & Albakajai 2016). The most relevant definition of sovereignty was written by Werner and de Wilde, even though it has been profoundly conceptualized. According to their definition, sovereignty means "a speech act to (re-)establish the claimant's position as absolute authority, and to legitimize its exercise of power" (Werner and de Wilde 2001, 287). In this definition, I believe the sovereignty discourse is referred. It is quite interesting that one can legitimize state's control over digital space by referring to digital sovereignty. Government interventions and regulation of digital space can be based on the protection of citizens (Leong et. al 2022). But I only partially agree with that idea because some states might prioritize the issue of critical information infrastructure which maintains national security.

What is meant by "digital"? In my opinion, it is described appropriately by Peters because it includes all the kinds of relevant technologies: "technologies, infrastructures, data, and content based on and/or using electronic computing techniques" (Peters 2016). Its application to sovereignty is a recent phenomenon due to the recent breakthroughs in technological progress. The acceleration of this progress brings new challenges to states which makes them adjust current policies to the new types of technologies. A political entity might set its own concept of digital sovereignty, for example, as it was done by EU Federal Chancellery: "Digital sovereignty describes the ability to shape the digital transformation in a self-determined manner with regard to hardware, software, services, and skills" (World Development Report 2021) This definition contributes to the state-centered approaches to digital sovereignty. Previous research has

established that there are aspects of digital sovereignty: national and individual.

1.2. Information sovereignty and digital sovereignty

There are various approaches associated with digital sovereignty concept in policy studies. In my opinion, it is important to distinguish information sovereignty and digital sovereignty because these concepts are very similar. Furthermore, the study by Stephane Couture and Sophie Toupin (2019) have shown that related to digital diverse concepts have been used in literature: "data sovereignty", "technological sovereignty", "information sovereignty (2019; 2307). In the study, the frequency of their usage in academic sources was calculated. Such variation proves that it is complicated to set one definition of digital sovereignty in the globalized and digitalized world. In non-academic literature reference to each notion varies even more. It is essential to refer and analyze academic literature because this study is a research thesis. Most frequently, scholars use concepts of information sovereignty and digital sovereignty, often equivalently. Interestingly, policies and discussion were initiated in some countries before the emergence of the concept in academic discussion – neither information sovereignty nor digital sovereignty, according to Mueller (2017). It means that the definitions capture almost the same affairs related to digital autonomy. As to data sovereignty concept, it is a narrower concept because it explains only national sensitive data flows (e.g. data confidentiality), as it was defined by Nugraha et al. in 2015. Regarding information sovereignty, there are two components of sovereignty, internal and external. So as the definition of information sovereignty because, according to Wenxiang Gong, it is a part of the state sovereignty. Internally, this concept means "the highest power of information policy-making, and the authority to maintain information order within the state" (Gong 2005, 120). Externally, one refers to "full legal equality with other states and the freedom from any external control with regard to the independent rights to the production and use of information" (Gong 2005, 120). The author also outlines that this concept is discussed among Chinese scholars within international relations field. Major characteristics of the term is its relation to production and use of information. It is important to note that the article was published in 2005 so the proliferation of

Internet and growing information flows across national borders had become a subject of discussion.

For this study, it is necessary to conceptualize digital sovereignty, hence, it is important to make a clear demarcation of these notions. I have not ruled out that in other areas of studies there is a concrete distinction between all these similar concepts. In some cases, there is no any rationale why a particular notion related to digital autonomy was used. Conceptualization of the digital sovereignty allows us to make justifications of data collection. Originally, the term appeared in 2000s but it was defined only in 2012 by Pierre Bellanger, it was a first attempt. But this definition was synonymous to digital autonomy of nation-states and non-state actors (such as companies, citizens). Its relation to national sovereignty was first proposed within the French National Digital Council two years later. By scholars later it was suggested that increasing power of GAFA led to imbalance between personal data policies and state power over citizens. Thus, it can be concluded that the term and necessity of regulatory policies by nation-states appeared as a reaction to digital trends and powerful non-state actors.

1.3. Studies of digital sovereignty in Russia

In the Russian discussion, academic literature on digital sovereignty is a new subject of interest in policy studies and political science. Some scholars use the concept of digital and information sovereignty as interchangeable concepts (e.g. Ashmanov 2013). His definition of digital sovereignty is the most discussed in the Russian scientific discussion: “the right of the state to determine its information policy independently, manage infrastructure, resources, ensure information security” (Ashmanov 2013). In general, discussion on these issues takes place since 2010. First, data sovereignty concept emerged, but further it became obvious that not only data comprise the digital realm. The digital sphere is more complicated than issues of data and with regards to the regulation, wider affairs should be captured either. It is widely discussed, what elements are included in the state sovereignty in digital realm in the case of Russia.

Previous literature focused on digital sovereignty of Russia in public administration

perspective. Work done by Leontyeva et. al (2021) was aimed at examination of spatial development differentiation. Phenomena of digitalization and digitization in public governance were evaluated in connection with the national sovereignty. However, the primary focus was at the national regulation of e-government services. National projects and public programs on Digital Economy development in Russia constitute implementation of strategic goals in the new policy area. But these technologies and processes ensure digital sovereignty in a technological sense, in my opinion. Digital sovereignty as a concept is not directly connected with the social-economic development and its implementation. The state of the national digital sovereignty was evaluated in the article considering the unequal regional development.

Recent research investigated internet sovereignty due to the recent tests of sovereign internet in the country of our interest (Litvinenko 2021). This group of studies is focused on the internet policies and contributes to the discussion of digital sovereignty policy due to several reasons. According to the author, "foreign threats to information security play a central role in Russia's strategic narrative of digital sovereignty" (Litvinenko 2021, 6). Hence, references to information security in the strategic narrative of the independent internet stipulates control over the internet. The author identified three elements of digital sovereignty, which are: "control over data, control over infrastructure, promotion of Russian internet governance initiatives at the international level" (Litvinenko 2021, 6). Interestingly, within this concept the special role of the internet policies within nation state is highlighted. Even though in the article the notion of "the authoritarian model of digital sovereignty" was mentioned in conclusions part, the distinction between democratic and authoritarian models are not clear. Whether these models are based on the types of political regimes of states and it undermines the model of digital sovereignty, it has not been explained. The difference between norms and practices of digital sovereignty are not emphasized either.

Substantial work has been carried out on the normative issues with the information and digital sovereignty in a legal perspective (Vinogradova, Polyakova 2021, Efremov 2020). Legal

foundations of the Russian sovereignty in information sphere were analyzed on the Constitutional Court of the Russian Federation resolutions as law enforcement acts. However, the authors concluded that strategic planning documents on the information security in Russia does not contain any concrete definition of the concept. The legal analysis of the acts revealed that there is no legal basic definitions related to information security. One of the major findings that is relevant for our study is the demarcation of information sovereignty and information policies. The first notion refers to the information space regulation by public authorities, the second – to concrete and limited ini time one of the public policies areas (Vinogradova, Polyakova 2021, 40). Efremov in his article also distinguished these two notions, furthermore, the author tried to collect and list relevant normative acts, including federal bills. It has conclusively been shown that digital transformation and digitalization make an impact on the regulation of information sphere, which consequently leads to the expanding tendency of information security regulation (Efremov 2020, 58). As result, increasing number of amendments to national laws (normative acts) can be noted.

Another area of research can be named as a technological perspective. Kucheryavy (2014) expressed in his paper concerns regarding growing interdependency among nation states due to proliferation of technologies all over the worlds. It leads to weakness of cybersecurity of a state. The author's main contribution to discussion is its emergence at the different levels, such as: technological, psychological, and political realms (Kucheryaby 2014, 12). For us, it is crucial to outline that digital sovereignty was used as a synonymous term to information sovereignty in information sphere, according to the scholar. In this narrow understanding of "digital sovereignty", it is meant that national payment system, searching system, and other technologies which altogether comprise information infrastructure and, thus, named as "digital". But for this study, even though we accept that technological component is crucial, explained definition is too narrow for our research question. Bukharin (2016) in his study on elements of digital sovereignty recognizes role of technological components, at the same time, the author employs information sovereignty and digital sovereignty as the equivalent notions. To conclude, his research

concentrated on digital autonomy which depends on national information infrastructure.

Investigation of the Russian national digital sovereignty without references to sovereignty in information sphere was conducted by Dudin et al. in 2021. This outstanding and coherent study aimed to evaluate digital maturity of Russia and parameters of digital sovereignty. We can see that motivation of digital sovereignty formation in different countries might vary same way as targets. The authors showed that motivation is based on the national interests in the international relations and concrete position in the world order. Moreover, strategic actions of potential military opponents are also considered by nation states when key decisions on digital sovereignty are made.

There are only a few studies on the political implications of contemporary digital sovereignty in policy studies and political science. The majority studies about digital studies issues is discussed from legal, technological or public administration perspectives. Overall, in policy studies there are few articles on the issues of digital sovereignty. Previous work has failed to evaluate potential political implications beyond strategic decisions on the digital sovereignty formation in the Russian context. Few studies have investigated the political connotations in the formation of digital sovereignty in the case of Russia. To sum up, the research gap has been found and illustrated in the literature review.

Chapter 2. Methodology and Research Design

This study is carried out in two stages. First, the literature review and conceptual framework will identify the relevance of the documents and their position in the digital sovereignty policies. Second, data for the analysis of documents was collected based on the concrete criteria. The strategic documents must contain the official views on the information policies and be approved at the federal level. Also, in the text the notion of sovereignty in the information sphere must be used.

To operationalize digital sovereignty, relevant existing publications in public policy literature were overviewed in the previous section. The analysis showed that there are many definitions of the "digital sovereignty".

Data collected in the research consists of the official documents published on the official Russian Federation websites: www.pravo.gov.ru and www.rg.ru. The official websites "Rossiyskaya gazeta" and "The official Internet portal of legal information" contain official decrees and orders, according to the Russian legislation (Decree of the President of the Russian Federation No. 763 of 23.05.1996). All the documents signed by President of the Russian Federation must be published in the defined by law online websites. Otherwise, such documents do not have legal force. Hence, the data collection stage was implemented by the online search commands in the listed official websites, according to the selection criteria. Most importantly, before data analysis special attention was paid to the sample of this study.

Qualitative inquiry and interpretative approach comprise a type of this research. Sample consists of secondary data. The official documents are the only secondary data that will be analyzed in the further section of this study. The following policy documents will be analyzed: "Doctrine of Information Security of the Russian Federation" (№ 646 December 5, 2016), "On the National Security Strategy of the Russian Federation" (№400 July 2, 2021), "On Approval of the Fundamentals of State Policy of the Russian Federation in the Field of International Information Security" (№213 April 12, 2021), "Strategies of the Information Society Development" (№203

May 9, 2017).

All documents are available in both Russian and English languages. The website of the Security Council of the Russian Federation contains the “Information security” section . There are other sections such: “International security”, “Economic security”, “Anti-terrorist security”, “Military-industrial security” and “State and public security” but they are not subject of interest of this study. Among the information security policy documents there is “Conception of UN Convention on international information security” which was proposed on the international level, as it was written in the introduction of this paper. This document was not included in data because it is a proposal.

The case study method was chosen as a relevant research method. Our study applies a single-case approach and is focused on the case of the Russian Federation only. The concept of digital sovereignty limits the boundaries of the case. Hence, international cybersecurity documents and any proposal will not be considered, as it was noted previously.

In literature on methodology, there are intrinsic, instrumental, and collective case study designs, according to Stake (1994, 1995). In my opinion, the intrinsic case study would be relevant in this study to choose. My research aim is to explore a concrete unique case, namely, the digital sovereignty of the Russian Federation. I believe that generalization and application of findings on other countries is not possible and appropriate. My personal motivation to study the case of Russia is to deeper understand intrinsic traits of the chosen case, as it was concluded in the literature review section – there are no studies with the same research questions in the academic literature. The contribution of this paper into the policy studies would be significant because there is a gap in the understanding the Russian national sovereignty in the digital realm. Mainly, the reason is the recent emergence and formulation of this concept in the policies of the Russian Federation.

As to research strategy, a descriptive research strategy was chosen, in particular, the case research (McNabb 2020). With this exploration type, we capture the uniqueness of the Russian case (Lune & Berg 2017). Most importantly, it allows us to establish the overall framework of

digital sovereignty in the beginning. Consequently, theoretical orientation is defined in the chosen case study design before the empirical part (Lune & Berg 2017). The main advantage of the single case study research is the possibility to reveal deep description of the phenomenon (Fiss 2009). Moreover, classical case study allows to consider the context of the unit of analysis – in this research the Russian political context will be described in the next section.

The case of Russia is a unique case due to the several reasons. Russia might be considered as a trend-setter in cybersecurity and cyberspace. According to the Global Cybersecurity Index – GCI, Russia takes fifth place (2020) which proves the high level of commitment to cybersecurity comparing to the other countries all over the world. Russia gained 98,06 scores in the GCI index in 2020 and can be considered as a country with a special attention to the cybersecurity and measures in the cyber realm.

Chapter 3. The Russian Context

In this chapter of the study, the national context will be explained. First, I introduce and describe position of strategic planning documents in the Russian Federation. Secondly, the most influential events which took place in Russia and affected the digital sovereignty policies are also included in this chapter. Lastly, it was decided to conduct the historical analysis of the Russian cyberspace and its policies in the different periods of contemporary Russia. The aim of this section is to provide a general understanding of the current policies on the issue and to situate subject of study within the Russian public policy.

3.1. The nature and role of strategic planning documents in Russia

Strategic planning in Russia is considered an instrument of public administration. However, altogether these instruments do not constitute a coherent system of strategic planning because they are independently adopted number of documents. The complicated relationship between them was tried to be captured by Smirnova and Mitrofanova (2019). Strategic planning documents are closely connected with budget planning and state programs. But strategic planning documents per se are aimed at "goal setting, forecasting, planning and programming" (FB-No.172). Regulation on strategic planning documents is written in the federal law No. 172 "On Strategic Planning in the Russian Federation" (2014). There are clearly defined types of documents at each level: federal, regional and municipal levels. Since Russia is a federation, on the federal level there are concrete strategic documents which regulate the issues of national security. Moreover, it is worth mentioning that both the President and the Government coordinate issues of development and implementation. Thus, strategic planning documents on national issues are designed and signed at the highest level.

National security and strategic planning documents are interconnected because among federal level documents there is one out of four documents devoted to national security. Three of them set general strategies on social-economic development, fundamental technological development and annual message of the President (FB-No.172). I decided to focus only on national

strategies on national security. Unlike other types of documents in the mentioned federal law (FB-No.172), those related to the national security are not named.

According to the law, four mentioned types of strategic planning documents are developed for the goal-setting purposes on the federal level. Interestingly, strategy on national security is the only document which is listed in particular, whereas others are just written as "foundation of public policy, doctrines and other documents on the endurance of national security" (Article 11, FB-No. 172). In my opinion, it means that the number of documents and adoption of new types of strategic documents are not limited due to the phrase "and other documents".

The existence of the adopted approach in Russia (planning and project management) has its roots in the idea of strategic state. Setting strategic goals and listing concrete means for their achievement is rooted in the idea of state planning functioned in the Soviet Union (Kudryashova 2014). The planning also covers all sphere of social life as in contemporary Russia, according to the author. Strategic management is labeled as "centralized strategic planning in the public sector" (Kudryashova 2014). It is evident that in the strategic planning documents, its design and development are supervised at the highest level. State-planning framework, as the author explains, requires that the state does not only set goals, etc. but also controls the implementation of the strategies. The concept of project management component in public governance, is limited in time and sets concrete indicators, goals and spheres. At the same time, as it is deliberately described by Smirnova and Mitrofanova (2019) these documents of project management are not linked to the strategic planning at all. Even though social-economic and other forms of societal development are separate from the national security issues, there is an obvious gap in Russian legislation due to the absence of linkages between short- and mid- term planning and general planning. Legislation gap causes the lack of compliance with achievement of the national strategic goals. To sum up, Russian strategic planning documents are supposed to have a guiding role in the short- and mid-term written with accordance of the budget constraints.

3.2. Important political events

It is worth briefly covering some significant events which had an impact on the digital sovereignty formation. Beyond the adoption of strategic planning documents in Russia (2016, 2017 and 2021), indeed, there were several important events in Russian history and political life. To better understand the national context I have been investigating, in this subsection several events were depicted in a chronological sequence and with connection to particular important stages of digital sovereignty policies.

A major turning point was mass protests in Russia in 2011-2012 which occurred after the State Duma (Parliament Chamber) elections. People protested the results of the State Duma elections (VI Congress), and the Presidential elections (4th of March 2012). Before 2012 there were a freedom of expression on the Internet because of the lack of specific regulation in the online sphere. Many scholars agree that those protests were escalated by online media (Pallin 2017) and social media. It was a turning point regarding the internet and information policies. In the mass protests, hundreds of thousands of people were involved in Russia and abroad in some cities. Before these events authorities had a right and practiced the blocking of particular websites, but only after the official decisions of courts. To sum up the above written, as was concluded by Soldatov: "since November 2012, internet censorship acquired a systemic nature" (Soldatov 2015, 1).

The "May" Decrees of the President in 2012 had set new public policy approach of achievement of strategic national goals in Russia. The new system with a new Presidency term employed the target-oriented approach in public administration for a concrete period of time: 2012-2020 with responsible governmental bodies. Most importantly for this study, it was stated that information security should be based on entirely on the national technologies and achievements.

Undoubtedly, sanctions towards Russia in 2014 had an impact as well. The Western sanctions had not only economic impact, but also political. As Rutland (2014, 6) claims in his article, sanctions were used in the public rhetoric as a proof that the West aims to weaken the

country. Consequently, special approach should be given to the national security.

Lastly, the historical event that changed the political environment was the adoption of the amendments to the Constitution of the Russian Federation in 2020. In 2020, along with other amendments, approach to the state sovereignty changed. In particular, in Article 67 of the Constitution, it is said: "The Russian Federation ensures the protection of its sovereignty and territorial integrity" (Constitution). In total, two amendments on the state sovereignty were adopted, both aimed at the strengthening of national sovereignty (Shashkova et. al 2020). For instance, an amendment to the Article 79 stated that interstate bodies' decisions might be enforceable in the Russian Federation if there is a contradiction with the Constitution.

3.3. Historical analysis of the Russian cyberspace

The purpose of this subsection is to conduct a short but coherent historical analysis of the Russian cyberspace. As it was mentioned earlier, Russia is considered as a trend-setter of cybersecurity technologies and cybersecurity strategies.

The emergence of the Russian cyberspace at the beginning of scientific discussion was associated with the Internet, namely, RUNET. RUNET – is a Russian-domain segment of the Internet (.ru). So, the important political events, in particular, the color revolutions in the 2000s was perceived as signal for the controlling the cyberspace (Deibert & Rohozinski 2010). The reason was the potential of the Internet for mobilization of people and increase in the probability of protest success, including the change of political regime, according to the article by Deibert and Rohozinski. As it was outlined by Fedotov, the importance of setting the national domain within a state means that the boundaries of the internet zone under the sovereignty of the Russian Federation (Fedotov 2016). The author of the article expressed concerns regarding this step in the Russian cyberspace policies because it became possible to use the national domain as a term in the law proposals. It would allow to set any rules and/or restrictions within it. Most importantly, the distinction between national and foreign domain zones became possible.

The Russian elites between 1990s and 2000s had experienced various reconfigurations

which finished with the election of the Vladimir Putin as the President of the Russian Federation starting on the 7th of May 2000.

The beginning of the new millennium simultaneously occurred with the first steps of cyberspace control – SORM. The national security at that time still had not been tied yet with the existing technologies. The development and later, adoption of the Doctrine of Information Security in 2001 was the first attempt to set general principles of information space. For the first time it was stated that information sphere was considered as vital national asset. As Giles (2012) claimed, the first cyber issues were incorporated in the document and, at the same time, their (norms and provisions) nature was liberal. At that time, back in 2001, of course, the state of digital development was mainly associated with the information flows, but some scholars presumed that it has a lot in common with the Western countries. Supportive evidence of this might be the following quote from the Doctrine: "ensure the constitutional rights and freedoms of man and citizen to freely seek, receive, transmit, produce and disseminate information by any lawful means" (Article 1, 2000). Hence, we can conclude that the Doctrine of Information Security set the start of the Russian cyberspace recognition and the necessity of its protection. The latter became possible because information sphere was closely linked with the national security.

The document titled "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space" was published on December 22, 2011. It is the first time when the official document stated the role of Armed forces in cyberspace (Giles 2012). The scholar purposively named that step as "Russian military cyber proto-doctrine" (Giles 2012). The concrete list of military activity in cyber realm was listed and explicitly included in the document: "includes measures by headquarters and actions by troops in intelligence collection, operational deception, radioelectronic warfare, communications, concealed and automated command and control, the information work of headquarters, and the defence of information systems from radioelectronic, computer and other…" (2011). Most interestingly, it was also stated that there is another type of the military's role which is not directly associated with the defensive role. The need for

"supporting the necessary moral and psychological condition of personnel" (Views 2011) were included as well. What is important is the fact that there are no any specific norms regarding the means of countering that type of threats towards the society.

A remarkable step of Russia towards digital sovereignty rules at the international arena had been made in 2011. The proposal titled "Draft Convention on International Information Security" which was released in Yekaterinburg, Russia in 2011. The implicit intentions of the Russian authorities were summarized by Giles (2012). According to Giles, Russia remains committed to the idea of state sovereignty within its physical borders (territory). So willingness of the state to control all the internet sources within a particular borders are evident from the following quote of the Convention draft: "each member state is entitled to set forth sovereign norms and manage its information space according to its national laws" (Article 5.5).

Illustrative evidence about the actors involved in cybersecurity is depicted in the following official document. Decree of the President of Russia of 2013 No. 31c "On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation" puts duties on the FSB (Federal Agency of Security). There are information, information-communication and authorized systems included in the notion of information sources of the Russian Federation. The Decree states that only FSB controls and responsible for the cybersecurity of the national information sources. Presumably, it was purposively not listed the specific list of information sources and the focus was on the governmental body and its duties due to the security reasons. The wide definition of issues related to cyberattacks on the Russian Federation information system can be found in the text of the Decree.

A breakthrough in the Russian regulation of cyberspace was the adoption of "the Decree of Information Security of the Russian Federation" on December 5, 2016. For the first time in the Russian history, it was clearly defined that in information sphere the following is included: "complex of software, IT systems, Internet websites, communication networks, and information

technologies" (Decree 2016). As it was conceptualized by scholars, cyberspace since the doctrine had been published including the Internet (Dnelyan, Gulyaeva 2020). In addition, it became possible to set the borders and define the nature of cyberspace. Finally, cyberspace captured the diverse technologies, not simply the Internet because the proliferation and storage of data is possible within different technologies but in cyber realm. This conceptual achievement allows to employ other related notions, such as cyber and information war. Only after the recognition of existence and definition of cyberspace, according to Warden, it is possible to "achieve political goals trough ICT" (Warden 1995). Overall, one needs to distinguish the state regulation of cyberspace and activity of the Military forces in the sphere because the mechanism of digital sovereignty formation, as Dudin et al. (2021) declared in their outstanding article, implies participation of governmental bodies and defined infrastructure actors (state corporations, private provider firms). Engagement of non-state actors in the digital sovereignty policies became possible after the adoption of the Strategy on national security in 2016. As authors claim in the publication, the adaption control system in which mentioned type of actors participate targets not only information flows but also threats of cyber attacks towards Russia.

At the federal level there were expressed concerns regarding the cyberattacks and its consequences (financial, etc.). For example, it was estimated that by 2016 approximately 203,3 billions of rubles were lost due to cybercrimes targeted the Russian economy (Kardava 2018). Furthermore, one can also notice another tendency – the increased amount of cybercrimes, the rise was significant, for example, between 2015 and 2017 (Kardava 2018). It was calculated the number increased in six times more than before period before 2015.

The "Conception of the cybersecurity strategy" of the Russian Federation was the first and so far, the only proposal in which cyberspace as a notion had been clearly defined in the content of strategic document. Even though the document remains as a proposal and at present, the document still is at the stage of the project, the importance of the document is crucial for the Russian public policy. The adoption of the Conception was supposed to be the first official

document where the cybersecurity was separated from information security. The idea of the development and necessity of such strategic planning document indicates the existence of gap in the Russian legislation regarding the cybersecurity issues.

Chapter 4. Analysis of the Documents

In this empirical part of the study, the analysis of selected strategic planning documents is written. Previously, it was explained how strategic planning documents are classified and what type of documents I am interested in. In order to answer the research question, each document is separately analyzed in the first part of this part. Second, it was decided to summarize and find meaningful connections between documents. As it was revealed in the previous section, the issues of digital sovereignty policies are not drafted in one document, in contrast, they are found in the various strategic planning documents.

4.1 The analysis of the selected strategic planning documents

In "Doctrine of Information Security of the Russian Federation" adopted December 5 in 2016 the definition and components of information sphere are clearly stated. The Internet, according to the law, is considered as the informational communication network "the Internet" and included in information sphere. By information sphere in the strategic planning document, is meant the cybersphere concept we discussed in the first chapter.

Besides the definition of the basic notions used in the documents, such as information security threats, instruments of information security maintenance, there are official views on the cybersecurity issues. These views are described by Russian legislators based on the analysis and evaluation of the modern and revised state of information technologies' capabilities.

In the second section, the role and impact of information technologies are briefly explained. But the items about that topic are delivered not as like legal provisions in other sections of the document. The second section of the Doctrine is dedicated to the national interests of Russia, and it opens with the general worldview of the state on the information technologies. Fundamental understanding of the role of information technologies is explained in the strategic planning document. Along with the supra-border nature, their application is formulated. The instrumental and service role of technologies is implicitly defined. Indeed, there are two demanded outcomes of the information technologies presence in the Russian case: "economic development of the state

and information society development" (item 7). At the same time, the information sphere plays strategically different role, namely, realization of national priorities set by the Russian authorities. To sum up, cybersphere and information technologies play different role in the Russian policy. We can see the highlighted importance of cyberspace as well as the vision of technologies' role in the case of Russia.

In the list of national interests, "the usage of information technologies in the interests of protection of cultural, historical and spiritual and moral values of the multinational people of the Russian Federation" is listed. First, the concept of multinational people of the Russian Federation is referral to the term of nation. In addition, such term is not used in other legal provisions throughout the Doctrine because the concepts of "human" and "citizen" with relation to protection of rights is usually used. But the emergence of new subject – the multinational people of the Russian Federation is not a subject of protection of its rights, but the political entity. This political entity, according to the strategic planning document, has its certain values, including moral ones. It is highlighted that a state can use information technologies to protect them, thus, the notion of multinational people is the justification for the usage of information technologies by authorities. Furthermore, there are no any specific purposes for the usage, only the following the national interests. Item 29 states the protection of digital sovereignty as one of the main directions of information security protection. Interestingly, we can claim that cyber security policies are supposed to be as an independent public policy aimed at the achievement of national interests. There are no any specific titles of the actions can be initiated by a state but all of them are justified because of the "multinational people" concept.

According to the fifth section of the Doctrine, involvement of information security into the national security is declared. Hence, information security is separated as a component of national security but at the same time one can conclude that there is no special nature or special status of this component. Even though in the organizational foundations of information security maintenance governmental bodies at all levels: federal, regional, and local are included, non-state

actors are also engaged. The maintenance of information security of the Russian Federation implies the involvement of the owners of critical information infrastructure objects, mass media, public associations and other actors (item 33). Thus, it is not only critical information infrastructure which has hot special attention and regulation (specific federal law) in Russian legislation but wide range of actors. Such actors must have been assigned with the objectives related to the information security maintenance.

Such maintenance must be state-centralized, including public management as it can be concluded based on the objectives imposed on the governmental bodies (item 36). Based on the item 37 of the Doctrine, its implementation foundations must comply the sectoral strategic documents mentioned in the second chapter of the thesis. Such characteristics of the Doctrine also indicates the centralized nature. Consequently, the principle of territory (regional strategic planning documents) are not applicable to the information security issues, even its implementation. Furthermore, at the highest level (the President and Security Council Secretary of the Russian Federation) results of implementation must be presented annually (item 38).

The thrive for the progress in the means of information security maintenance is also imposed on the state bodies. Remarkably, the similarities with the military affairs also persist in the information security field but without the engagement of the Armed forces of Russia. One cannot find any military trainings in the cyber affairs, but the necessity of regular trainings is highlighted in the Doctrine. There are no any specifications on a state actor which is responsible for such trainings in the cyber realm. But the goal of these trainings is defined openly: ongoing cyber threats to the national security of Russia. The persistent cyber threats are the subject of state's awareness, and it is implicitly outlined.

In "Strategy of the Information Society Development" published on May 9 in 2017, we can see a concrete time period of that strategic planning document 2017 – 2030. It is not typical for strategic planning documents as the chapter 2 revealed because project management approach does not include strategic planning.

Among the list of principles in the first section of the Strategy the "traditional Russian spiritual and moral values" are prioritized (item 3). The protection of the Russian citizens' rights in digital realm is not highly prioritized, however, the right to access information is the major priority in the document. We can see that in "g" item containing information on Russian values also includes qualitatively new term. References to traditional values are not limited, "patterns of behavior based on the values with application of information and communication technologies" are included in the principles (item 3 "g"). The broadened principles related to the values can be noted. Remarkably, that there is no concrete evidence on what precisely constitute those traditional values and why behavior based only on them must be protected remains unclear.

One can reveal some insights about the vision of the Russian position in information society in the second chapter of the Strategy. Information and communication technologies are separated, whereas in the Doctrine we examined earlier, they are not distinguished. But their application is possible in the cyberspace. The importance of these technologies contributes to the economic development. Especially to its new stage – digital economy.

The recognition of the digital economy as a stage made possible to formulate national interests within it. Digital economy has been considered as a sphere in which Russia defined the list of concrete national interests. Those related to the economic development are not the subject of interest but one of the listed national interests illustrate the assertions of digital sovereignty. The item 42 "d" states the maintenance of technological independence as well as Russian infrastructure protection. By the latter critical or information infrastructure in general are not meant. Instead, the wide range of infrastructure related to goods and services provision

A section named "the development of information and communication infrastructure of the Russian Federation" contains the intention of national information infrastructure formation. The "imported technologies" and "national analogues" highlights dependency on the hardware imported in Russia at some extent. At the same time, "information security" depends not on the efficient exploitation of the best technologies, but rather on the belonging to the inclusion to the

national information infrastructure. The necessity to create Russian software is recognized for the completely independent information system. Thus, we can conclude that special attention paid to the technological independence, and the information infrastructure as a wide range of software and technologies needs to be established.

The strategic planning document titled "On the National Security Strategy of the Russian Federation" signed by the President on July 2 in 2021 the new vision of the challenges and world itself are presented. They differ from those written in the Doctrine of Information Security we analyzed earlier in this chapter. The position of Russia in the world is explained in the second section of Strategy and some significant changes can be found.

First, the international world order has been changed, in particular, political shifts are captured. "Modern world" is unstable and the contradictions between nation states take place. "The West" appears in the lexicon of Russian legislators in the Strategy and in the negative connotations. Ambition to maintain the "hegemony" is highlighted, and the countries which belong to "the West" are willing to remain in hegemonic position (item 7). Concerns about the growing role of the transnational organization are expressed in the section as well. The political conflicts probability within a country borders occur due to the interests of transnational organization to limit the states. Hence, a leading and primary role of a state at the international level is recognized, whereas the international organization threaten them.

Second, the digital sovereignty strength leads to the technological advantages and leadership of the Russian Federation at the international arena. Not only economic development but also technological aspect has been recognized in the document. This aspect is an asset of national security protection and "international recognition of Russia". At the same time, we can conclude that in addition to "tradition spiritual and moral values of Russia" there are several new valuable concepts. Namely, "Russian uniqueness" and "patriotic education" is listed, in contrast to the analyzed Doctrine of Information Security adopted four years before the Strategy. In the text we see the forces which confront "Russian uniqueness" and traditional values: "the Western

liberal model". This almost bipolar model of international world order includes unlisted "unfriendly countries" which make attempts to destroy "unity" of Russia. At the same time, moral leadership at the supranational level remains topical and the Western model depicted as threating the national security. Due to inclusion explained values into national interests, threats from "unfriendly countries" target the national security, including the information security as well.

As a document of strategic planning "On Approval of the Fundamentals of State Policy of the Russian Federation in the Field of International Information Security" (№213 published on April 12, 2021) establishes not only the global information space vision but also the digital sovereignty traits of Russian within it. Moreover, the document continues the principles and provisions of the National Security strategy and Doctrine of Information security we had already analyzed (item 4). It illustrates the unity of the policies on digital sovereignty and other strategic relations on the national security protection.

As in the other strategic documents examined earlier, one might find the essence of key subject of regulation, namely: international information security and threats. Along with the "terrorist" and "extremist" usage of information and communication technologies, there are some more sophisticated potential threats. Particularly, item 8 contains cyber attacks on critical information infrastructure. Most interestingly, concerns about "technological domination" of some countries are listed with references to "monopolized market of information and communication technologies" (item "e"). To sum up, the necessity of digital independency from the non-Russian software in Russia are based on the assumption that countries where the transnational corporations are located have a right to use its technologies for political and military goals.

Several concerns about lack of information regulation on cybersecurity are expressed in the implementation of information security policies. But the necessity of regulation with a dialogue at the supranational level with international organization and states is recognized. Existing "national security standard on information security (item 11) does not meet any legal application. The awareness about cyberthreats. The "global system" and "global cybersphere" are opposite

concepts. The reason is following: the absence of adopted international principles of cyber space. Hence, cyber attacks and any information attacks (including the communication technologies impact on “Russian traditional values”) target the digital sovereignty of the Russian Federation. We can clearly follow the logic of the national borders’ idea and commitment to the information security interests expressed in the documents of strategic planning. International peace, according to the document, is based on the territorial integrity principle of states. Unlike the Doctrine’s conceptual framework, we can claim that in the Fundamental the term “information and communication technology” also has been applied. But in addition to the “undermining intentions” we can see the word “infringement” used with assertions of digital sovereignty.

Discussion and conclusions

The conducted analysis of strategic planning documents where the assertions of digital sovereignty of the Russian Federation incorporated showed that there are not only legal formulation of policies but also political implications. These political implications can be summarized and collected only with relation to other documents related to digital sovereignty formation.

The progress in technological sphere and sophistication of information technologies in general is a fact, and it is implicitly included in the strategic planning documents' conceptual foundations. While the notion of national interests, national security and other not specific to digital area terms remain the same in all strategic planning documents, new understandings of technology's types and role have been emerging. From information technologies there is a shift towards information and communication technologies, and lastly to their convergence. With a technological progress, certain concerns are expressed in the documents. These concerns are based on the awareness of more sophisticated means of international intervention in the digital realm limited to national borders of Russia.

The national borders' role reveals several findings of political nature that have been summarized in this chapter. The highlighted incorporation of infrastructure and information sources into the information security has concrete demarcation and inclusion into the competence of the Russian Federation.

The selected strategic planning documents contain legal provisions which include information space and information infrastructure (including information infrastructure with critical importance) definitions, but in fact their application is equivalent to the cyberspace affairs. The evaluation of the technological developments is implemented regularly for the national security protection. At the same time, there is a clear commitment to the information security concept, which includes digital affairs, but the revision has not been done. Information security is a broad concept which is a part of national security. Remarkably, its protection and even implementation

is highly centralized, despite the federal system.

To sum up, political implications are mainly formulated in the first chapters of strategic planning documents where the official views on the world order and position of the Russian Federation are located. The official views' formulated by Russian legislators have changed, the global cyberspace is perceived as dangerous realm due to the lack of regulation and cyber attacks threats. Initially, the technological progress made possible international cooperation in the field of digital technologies and digital economy, but later the terms "the West" and "unfriendly countries" have been applied. As to non-state actors, the strengthening role of transnational corporations is perceived as actors who have a power to threaten digital sovereignty of any country, including the Russian Federation. Moreover, the commitment to idea of the traditional idea of state sovereignty with territorial principle is implicitly formulated either.

Findings of this study contribute to the discussion on sovereignty discussion in Russia in policy studies and political science. Understanding of the digital sovereignty and a recently emerged cybersphere varies from country to country. Political implications reflect the features of the political regime in contemporary Russia. Also ideological findings contribute to the academic discussion on the modified political regime after 2018. The new political environment and its characteristics are embedded in the strategic planning documents which opens a discussion on the established values approved and set at the federal level. This study made an attempt to summarize different political implications in different strategic planning documents, and this approach can be applied further by other scholar.

Bibliography

Ukaz Prezidenta RF ot 12.04.2021 g. N 213 «Ob utverzhdenii Osnov gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti» [Decree of the President of the Russian Federation of April. 2021. N 213 «On Approval of the Fundamentals of State Policy of the Russian Federation in the Field of International Information Security»]. URL: http://government.ru/docs/37669/ (date of access: 01.16.2021). (In Russ.)

Ukaz Prezidenta RF ot 05.12.2016 No. 646 "Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii"[Decree of the President of the Russian Federation dated December 5, 2016 No. 646 «On approval of the Doctrine of Information Security of the Russian Federation»]. – Sobranie zakonodatel'stva Rossiiskoi Federatsii [Collection of the Legislation of the Russian Federation]. December 12, 2016. No. 50. Art. 7074. (In Russ.).

Ukaz Prezidenta RF ot 09.05.2017 g. N 203 «O Strategii razvitiya informatsionnogo obschestva v Rossiyskoy Federatsii na 2017 - 2030 godyi» [Decree of the President of the Russian Federation № 203 May 5, 2017 «Strategies of the Information Society Development»]. URL: https://base.garant.ru/71670570/ (date of access: 01.16.2021). (In Russ.)

Ukaz Prezidenta RF ot 02.07.2021 g. N 400 «O Strategii natsionalnoy bezopasnosti Rossiyskoy Federatsii» [Decree of the President of the Russian Federation № 646 July 2, 2021 «On the National Security Strategy of the Russian Federation»]. URL: http://www.kremlin.ru/acts/bank/47046 (date of access: 01.16.2021). (In Russ.)

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

Afinogenov D.A., Polyakova T.A. Sistema dokumentov strategicheskogo planirovaniya: problemyi i perspektivyi // Vestnik Akademii prava i upravleniya. 2017. # 3(48). pp. 22–32.

Alpeev A.S. Terminologiya bezopasnosti: kiberbezopasnost', informatsionnaya bezopasnost' // Voprosy kiberbezopasnosti.-2014.-№5. – S. 39-42.

Beltrán NC (2016) Technological sovereignty: what chances for alternative practices to emerge in daily IT use? Hybrid. Revue des arts et médiations humaines. Available at: https://www.semanticscholar.org/paper/Technological-Sovereignty%3A-What-Chances-for-to-inBeltran/b26e0d1f1c21497b2980f8515d6ce7948d9c892f.

Berg, B. L. (2009). Qualitative research methods for the social sciences / Bruce L. Berg. Allyn and Bacon.

Biryulin R. Stremlenie k tsifrovomu suverenitetu [Elektronnyiy resurs] // Krasnaya zvezda.

2017. 5 dekabrya [sayt]. URL: http://www.redstar.ru/index.php/newspaper/item/35303-stremlenie-k-tsifrovomu-suverenitetu.

Bratton BH (2015) The Stack: On Software and Sovereignty (Software studies). Cambridge, MA: The MIT Press.

Buharin V.V. Komponentyi tsifrovogo suvereniteta Rossiyskoy Federatsii kak tehnicheskaya osnova informatsionnoy bezopasnosti. Moskva. Izd-vo: Vestnik. 2016 g.

Bukharin V.V. THE RUSSIAN'S DIGITAL SOVEREIGNTY AS A TECHNICAL BASIS OF INFORMATION SECURITY. MGIMO Review of International Relations. 2016;(6(51)):76-91. (In Russ.) https://doi.org/10.24833/2071-8160-2016-6-51-76-91

Council (2014). "The Strategic Concept of Cyber Security of Russian Federation".

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital?. new media & society, 21(10), 2305-2322.

Damon L. 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. 1986. Vol. 10. Issue 2. P. 262–287.

Danelyan A.A., Gulyaeva E.E. International Legal Aspects of Cybersecurity. – Moscow Journal of International Law. 2020. No.1. P. 44–53. DOI: https://doi.org/10.24833/0869- 0049-2020-1-44-53 Кардава, Н. В. (2018). Киберпространство как новая политическая реальность: вызовы и ответы. История и современность, (1-2 (27-28)), 152-166.

De Filippi P., McCarthy S. Cloud Computing: Centralization and Data Sovereignty (October 26, 2012) //European Journal of Law and Technology. Vol. 3. No 2. 2012 // http://ssrn.com/abstract=2167372.

Deibert, R. J., & Rohozinski, R. (2010). Control and subversion in Russian cyberspace.

Draft United Nations Convention on Cooperation in Combating Information Crimes. URL: https://www.rusemb.org.uk/ fnapr/6394 (accessed13.09.2019).

Dudin M.N., Shkodinsky S.V., Usmanov D.I. Digital sovereignty of Russia: barriers and new development tracks // Market economy problems. – 2021. – No. 2. – Pp. 30-49 (In Russian). DOI: https://doi.org/10.33051/2500-2325-2021-2-30-49Ашманов И. Информационный суверенитет России: новая реальность // Россия навсегда. 13.05.2013. [Элек¬тронный ресурс]. URL: http://rossiyanavsegda.ru/read/948/ (дата обращения: 07.10.2016).

Dulock, H. L. (1993). Research design: Descriptive research. Journal of Pediatric Oncology Nursing, 10(4), 154-157.

Efremov, Alexey A. 2019. State sovereignty in the conditions of digital transformation. Pravovedenie 63 (1): 47–61. https://doi.org/10.21638/spbu25.2019.103 (In Russian).

Fedotov, M. A. (2016). Konstitutsionnyie otvetyi na vyizovyi kiberprostranstva. Lex russica, (3 (112)), 164-182.

Giles, K. (2012, June). Russia's public stance on cyberspace issues. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-13). IEEE.

Grant P (1983) Technological sovereignty: forgotten factor in the “Hi-Tech” Razzamatazz. Critical Studies in Innovation 1(2): 239–270.

Gueham, Farid. 2017. Digital Sovereignty – Steps Towards a New System of Internet Governance. Paris: Fondapol.

Haché A (2014b) Technological sovereignty. Mouvements 79(3): 38–48.

Haché A (2017) Technological Sovereignty, vol.2. Barcelona. Available at: https://www.ritimo.org/IMG/pdf/sobtech2-en-with-covers-web-150dpi-2018-01-10.pdf.

Hinsley, F.H. (1986), Sovereignty, 2nd ed., Cambridge University Press, Cambridge, MA, 258 p.

Hollis DB (2012) Stewardship Versus Sovereignty? International Law and the Apportionment of Cyberspace (ID 2038523, SSRN scholarly paper, 19 March). Rochester, NY: Social Science Research Network. Available at: https://papers.ssrn.com/abstract=2038523.

Irion K. Government Cloud Computing and National Data Sovereignty // Policy and Internet. 2012. Vol. 4. Issue 3–4. P. 40–71.

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

Kucheryavyiy M. M. (2014). Gosudarstvennaya politika informatsionnogo suvereniteta Rossii v usloviyah sovremennogo globalnogo mira. Upravlencheskoe konsultirovanie, (9 (69)), 7-14.

Kudryashova, E.V. (2014). State Planning and Budgeting in the Russian Federation. In: Joyce, P., Bryson, J.M., Holzer, M. (eds) Developments in Strategic and Public Management. IIAS Series: Governance and Public Management. Palgrave Macmillan, London. https://doi.org/10.1057/9781137336972_10.

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

Kukutai T. and Taylor J. (eds) (2016), Indigenous Data Sovereignty: Toward an Agenda (CAEPR), Research monograph, no. 38, pp. 139-156, Centre for Aboriginal Economic Policy Research, College of Arts and Social Sciences, The Australian National University, Canberra.

Leontieva L.S., Kudina M.V., Voronov A.S., Sergeev S.S. 2021. Creating National Digital Sovereignty in the Context of Spatial Development Differentiation. Public Administration №84.

Maurer, T., Skierka, I. and Morgus, R. (2015), “Technological sovereignty: missing the point?”, 7th international conference on Cyber conflict: Architectures in cyberspace (CyCon), pp. 53-68. IEEE, available at: http://ieeexplore.ieee.org/abstract/document/7158468/

(Accessed: 11.05.2022).

McNabb, D. E. (2021). Research methods for political science quantitative, qualitative and mixed methods approaches.

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

Nesterov A.V. — Internet-pole VS kiberprostranstva // Voprosyi bezopasnosti. – 2015. – # 4. – pp. 13-27. DOI: 10.7256/2409-7543.2015.4.16743 URL: https://nbpublish.com/library_read_article.php?id=16743.

Nugraha, Y.K. and Sastrosubroto, A.S. (2015), "Towards data sovereignty in cyberspace", 3rd international conference on information and communication technology (ICoICT), pp. 465-471, available at: https://ieeexplore.ieee.org/document/7231469 (Accessed: 11.05.2022).

Perritt, Henry H. Jr. (1998), "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance", Indiana Journal of Global Legal Studies, vol. 5, issue 2, pp. 423-442.

Pohle, J., & Thiel, T. (2021). Digital sovereignty. In Practicing Sovereignty: Digital Involvement in Times of Crises (pp. 47-67). Bielefeld: transcript Verlag.

Polyakova T., Afinogenov D., THE ROLE OF STRATEGIC PLANNING IN IMPROVING PUBLIC ADMINISTRATION SYSTEM IN THE RUSSIAN FEDERATION

Powers S. Towards Information Sovereignty // BEYOND NETMUNDIAL: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem. Philadelphia: Center for Global Communication Studies, 2014. P. 90–99.

Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. Anna Litvinenko. Media and Communication (ISSN: 2183–2439) 2021, Volume 9, Issue 4, Pages 5–15 https://doi.org/10.17645/mac.v9i4.4292.

Rutland, P. (2014). The impact of sanctions on Russia. Russian Analytical Digest, 157(1), 1-8.

Shashkova Anna, Verlaine Michel, & Kudryashova Ekaterina (2020). ON MODIFICATIONS TO THE CONSTITUTION OF THE RUSSIAN FEDERATION IN 2020. Russian Law Journal, 8 (1), 60-83.

Smirnova O.O., Mitrofanova I.V., 2019. Balance of Strategic Planning in Russia: On the Systemic Approach to Documents, Programs and Projects. Regionalnaya ekonomika. Yug Rossii [Regional Economy. South of Russia], vol. 7, no. 3, pp. 14-24. (in Russian). DOI: https://doi.org/10.15688/re.volsu.2019.3.2.

Tan, K. L., Chi, C. H., & Lam, K. Y. (2022). Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization. arXiv preprint arXiv:2202.10069.

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

The World Bank, “World Development Report 2021,” 2021. [Online]. Available: https://wdr2021.worldbank.org/stories/crossing-borders/

Timmers P., “Challenged by “Digital Sovereignty”” in Journal of Internet Law, December 2019

Vinogradova, E. V., & Polyakova, T. A. (2021). O meste informatsionnogo suvereniteta v konstitutsionno-pravovom prostranstve sovremennoy Rossii. Pravovoe gosudarstvo: teoriya i praktika, (1 (63)), 32-49.

Wu TS (1997) Cyberspace sovereignty? The Internet and the international system. Harvard Journal of Law & Technology 10(3): 647–666.