Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty

Litvinenko, Anna

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Litvinenko, A. (2021). Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. *Media and Communication*, *9*(4), 5-15. https://doi.org/10.17645/mac.v9i4.4292

Media and Communication (ISSN: 2183–2439)
2021, Volume 9, Issue 4, Pages 5–15
https://doi.org/10.17645/mac.v9i4.4292

Article

Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty

Anna Litvinenko

Institute for Media and Communication Studies, FU Berlin, Germany; E-Mail: anna.litvinenko@fu-berlin.de

Submitted: 21 March 2021 | Accepted: 4 August 2021 | Published: 21 October 2021

Abstract
Over the past decades, internet governance has developed in a tug-of-war between the democratic, transnational nature of the web, and attempts by national governments to put cyberspace under control. Recently, the idea of digital sovereignty has started to increasingly gain more supporters among nation states. This article is a case study on the Russian concept of a "sovereign internet." In 2019, the so-called law on sustainable internet marked a new milestone in the development of RuNet. Drawing on document analysis and expert interviews, I reconstruct Russia's strategic narrative on internet sovereignty and its evolution over time. I identify the main factors that have shaped the Russian concept of sovereignty, including domestic politics, the economy, international relations, and the historical trajectory of the Russian segment of the internet. The article places the Russian case in a global context and discusses the importance of strategic narratives of digital sovereignty for the future of internet governance.

Keywords
digital sovereignty; internet governance; Russia; strategic narrative

Issue
This article is part of the issue "Media Control Revisited: Challenges, Bottom-Up Resistance and Agency in the Digital Age" edited by Olga Dovbysh (University of Helsinki, Finland) and Esther Somfalvy (Research Centre for East European Studies at the University of Bremen, Germany).

1. Introduction

Global internet governance, which has been evolving over the past decades in the spirit of the Declaration of the Independence of Cyberspace (Barlow, 1996), has apparently reached a bifurcation point where more and more national governments are introducing their concepts of internet sovereignty. In the 2010s, this term had a rather negative connotation in the global media (Woodhams, 2019). The internet isolation policies of China, Iran, and Russia were seen as a destructive trend towards a "Splinternet," which would undermine the global digital economy and violate the human rights of freedom of speech and information access. When the so-called "sovereign internet" bill was introduced in Russia at the end of 2018, it was criticized in the press as an "online Iron Curtain" (Schulze, 2019). The widespread criticism and protests against the policy even made Russian legislators and pro-state media change the wording in the description from "sovereign internet" to "sustainable internet" (see Shimaev et al., 2019).

However, within the last few years, democratic countries such as EU states have also begun to talk intensely about their digital sovereignty (Pohle, 2020). Do different political regimes mean the same thing when they plead for digital sovereignty? Apparently not. The term "digital sovereignty" remains a highly contested one, and its interpretation differs from country to country and thus has "conflict potential" (Thiel, 2021). Kleinwächter (2021) has called the current state of Internet governance a "digital cacophony in a splintering cyberworld." This situation makes a study of strategic narratives (Miskimmon et al., 2013) of digital sovereignty an important contribution to the debate over the future of cyberspace.

In this article, I aim to explore Russia's strategic narrative regarding a "sovereign internet." Drawing on the

analysis of the major doctrines and strategies of the Russian government concerning internet policy since 1999, as well as on five expert interviews, I reconstruct the Russian government's strategic narrative of internet independence and explore the major factors that have shaped its approach to digital sovereignty. The article places the Russian case in a global context, contributing to a better understanding of the current challenges and perspectives of internet governance.

I conclude that the Russian concept is based on its approach to internet security, whereby internet security is likened to information security, and where the state's control over information flows is placed at the forefront. The key elements of the Russian understanding of digital sovereignty are: (1) control over data (in the form of data filtering and data localization), (2) control over infrastructure (in the form of, among others, protectionism and a centralized system of monitoring equipment), (3) promotion of Russian internet governance initiatives at the international level.

Although foreign threats to information security play a central role in Russia's strategic narrative of digital sovereignty, it is domestic politics and the impetus of elites to control oppositional discourse within the country that have apparently had the biggest impact on the formation of Russian digital sovereignty policy. I conclude by discussing the role of strategic narratives in regard to digital sovereignty for the future of Internet governance.

The remainder of this article is organized as follows: First, I give an overview of the major approaches to digital sovereignty. Then I present the development of Russian internet policy during the last decade, followed by the methodology section, the presentation of results and their interpretation, and the discussion.

2. Approaches to Internet Sovereignty: Drawing Borders in Cyberspace

On the one hand, the internet has opened immense opportunities for different actors worldwide. On the other hand, it has undermined the sovereignty of nation states, challenging existing rules and reshuffling the world order by empowering new global players, such as large social media platforms. In the 1990s and 2000s, the benefits of global interconnectedness for nation states largely prevailed over concerns about cyberthreats. However, after the Arab Spring in 2011, authoritarian leaders worldwide realized that the mobilizing potential of social media had become a real threat to their rule, so they have increasingly tightened control over online communication in their respective countries (Richter & Kozman, 2021). In 2013, Snowden's revelations about internet surveillance by US intelligence have stirred up a discussion about, among other factors, technical autonomy in EU countries (Müller, 2017).

While, in the 2000s, China with its Golden Shield program, also known as the Great Firewall, was a standalone example of internet isolation, in the 2010s, more and more countries started to follow this path. According to Mueller (2017), ideas about what we now call digital sovereignty were first introduced in different countries, including the US, long before 2013, but there has been no widespread rhetoric about the necessity of digital autonomy. Until recently, the term "digital sovereignty" has been associated mostly with authoritarian states, such as China and Iran.

These countries have, over the years, developed their national approaches to internet sovereignty. If we imagine a continuum, where openness of the net is on the right side and isolation on the left, the first from the left would be the case of North Korean, where the internet has been officially banned and replaced by a national intranet. The Chinese approach to internet sovereignty is much more sophisticated and apparently was able to solve the so-called "dictator's dilemma" (Kedezie, 1997). It implies that autocrats are usually faced with a choice between two paths that are both vital for the sustainability of their regime but, at the same time, contradict each other: the promotion of information technologies that bring economic benefits versus preserving control over the information space. The Chinese government manages to combine both these paths. It is, however, doubtful whether the Chinese case can be replicated, as the historical trajectory of internet development in China diverges from that of other countries. The internet in China was initially designed as a centralized network under state control. China's approach to internet sovereignty includes the Great Firewall, which filters undesirable content, and includes protectionism of Chinese IT companies and promotion of Chinese software and infrastructure worldwide (Steiner & Grzymek, 2020; Zeng et al., 2017). The Iranian approach is similar to the Chinese one, but it draws rather on a defensive strategy that was developed in reaction to international sanctions (Michaelsen, 2018). Exploring the factors that have shaped the current state of isolation of the Iranian internet, Michaelsen has highlighted the importance of international relations in this case.

Russia has joined the trend towards more state control over the internet rather late: The tightening of internet regulation there began after the protest movement "For Fair Elections" in 2011–2012 (Litvinenko & Toepfl, 2019). Russia's policy towards digital sovereignty has caused much discussion since the introduction of the 2018 draft of the bill on a sovereign internet, which was adopted in 2019 (Schulze, 2019).

For a long time, the EU has been rather reluctant to use the term "digital sovereignty" (Thiel, 2021), preferring the notions of "technical sovereignty" and autonomy (Pohle, 2020). Germany had a leading role in fueling the European debate on digital sovereignty by putting it on the agenda for EU digital policy during Germany's EU presidency in 2020 (Pohle, 2020). A year earlier, this term had been widely used in discussions about the project of the European data

cloud—Gaia-X—linking digital sovereignty to independence from externally produced infrastructure. German Minister of Economic Affairs and Energy Peter Altmaier said while introducing the project: "Germany has a claim to digital sovereignty. That's why it's important to us that cloud solutions are not just created in the U.S." (Stolton, 2019). In her speech at the opening of the Internet Governance Forum 2019 in Berlin, German Chancellor Angela Merkel gave the following definition of the concept: "Digital sovereignty does not mean protectionism, or that state authorities say what information can be disseminated—censorship….It describes the ability both of individuals and of society to shape the digital transformation in a self-determined way" (Merkel, 2019).

In her study of the European discourse on digital sovereignty, Julia Pohle has shown that, in the EU, the concept is linked to the democratic understanding of sovereignty as the people's right to self-determination (Pohle, 2020). It "encompasses the ability of individuals as well as state or commercial institutions to make autonomous use of digital technologies and to independently and securely exercise their roles in times of digitalization" (Pohle, 2020, p. 8). The existing definitions, however, are still too vague, as they need to be translated into tangible policy elements (Steiner & Grzymek, 2020).

So far, the term remains instead a metaphor that is interpreted in different ways by different political regimes. Kolozaridi and Muravyov (2021) have suggested understanding states' internet sovereignty claims as "performance, rhetorical acts whose primary function is to counter hegemonic tendencies." In a situation of a "digital cacophony in a splintering cyberworld" (Kleinwächter, 2021), the use of such a vague term might deepen existing controversies between states. At the same time, a better understanding of different states' narratives of internet sovereignty would bring more clarity to the ongoing processes of internet fragmentation.

Here, I suggest using the concept of strategic narrative that was shaped by Alister Miskimmon, Laura Roselle, and Ben O'Loughlin (Miskimmon et al., 2013). It is a theoretical framework for studying the persuasive communication of nation states in the international arena. By strategic narratives, they understand "a communicative tool through which political actors—usually elites—attempt to give determined meaning to the past, present, and future in order to achieve political objectives" (Miskimmon et al., 2013, p. 5). The authors distinguish strategic narratives at three levels: international system narratives, national narratives, and issue narratives (see also Roselle et al., 2014). The latter are meant to put governmental policies into context, and to explain why certain policies are necessary and how they can be successfully realized. Looking at the rationales that stand behind the use of the term "digital sovereignty" by different states will help us better understand the ongoing debate about the future of cyberspace.

3. The Russian Case: From an Underregulated Internet to Digital Sovereignty

The Russian segment of the internet, also called RuNet, remained largely unregulated until Putin's third presidential term, which started in 2012 (Vendil Pallin, 2017). In the 2000s, against the backdrop of increasing censorship in traditional media, the internet was celebrated as a free forum for political discussion (Richter, 2007). Scholars explained the absence of tight regulation over cyberspace by the fact "that the digital technologies do not offer a solution to issues of media control" (Richter, 2007, p. 206). However, as time has passed, new means to provide technological control over internet resources have emerged, which have been increasingly implemented by the Russian government.

The turning point in Russian internet policy was, according to many scholars, the protests of 2011–2012, which, to a large extent, were fueled by online media (Vendil Pallin, 2017). For instance, Soldatov (2015) mentioned that, although the blocking of websites had already been a rather common measure for the Russian authorities since 2007, it had previously been applied following a court decision and occurred in a non-systematic manner: "Since November 2012, internet censorship acquired a systemic nature" (Soldatov, 2015, p. 1).

In 2016, the so-called "Yarovaya Package," a set of amendments to anti-terrorism legislation, was adopted, which became an important milestone in the tightening of state control over cyberspace (Lehtisaari, 2019). Among other things, the law obliged internet providers to store all data for half a year, which was barely even technically possible. It also introduced more severe punishment for the (re)posting of pro-terrorist or extremist content.

One of the core characteristics of Russian internet legislation is its vague wording as well as its selectivity regarding the implementation of restrictive laws (Oates, 2013; Vendil Pallin, 2017). As Vendil Pallin has noted, "most laws are not systematically implemented and by no means all opposition content that is posted on the internet leads to legal or other actions from the authorities" (Vendil Pallin, 2017, p. 17).

Vendil Pallin (2017) examined strategies that the Russian government had implemented since 2013 in order to gain control over cyberspace though ownership of domestic resources and to regulate international companies operating on the RuNet—the first steps towards Russian digital sovereignty. For instance, in 2016, the obligation of internet operators to store the personal data of Russian citizens within the territory of the Russian Federation was officially framed "as a measure to increase security and safeguard the privacy of Russian internet users" (Vendil Pallin, 2017, p. 27). Another law that came into effect in November 2017 restricted the activities of VPN services and anonymizers, prescribing them to block Russian users' access to content prohibited by the Federal Service for Supervision in the

Sphere of Telecom, Information Technologies and Mass Communications (or Roskomnadzor). However, in the two years after the enactment of the law, VPN companies did not follow the rules, and the Russian authorities did not try to punish them for not doing so. As Soldatov mentioned in 2015, analyzing the perspectives of blocking the anonymizer Tor in Russia, just legal prohibition would be not enough, "a highly efficient technological solution is required" (Soldatov, 2015, p. 8), and it seems to not have been found yet.

The next major step on the path towards placing Russian internet segments under state control was the legislative initiative on "sovereign internet" that came into effect in October 2019. It introduced a system of state-sponsored monitoring devices that had to be installed by Internet providers and that helped authorities filter, reroute, and block internet traffic (Epifanova, 2020).

Stadnik (2021a) has analyzed internet independence policy in Russia by applying Müller's (2017) categorization of methods of alignment of cyberspace to national borders: national securitization, territorialization of information flows, and efforts to control critical internet resources along national lines. She has concluded that all these methods are being implemented in Russia and that the Russian government seeks to provide "national security at any price" (Stadnik, 2021a, p. 162), to a large extent ignoring the interests of private stakeholders. In her other paper, Stadnik (2021b) examined four attempts of the Russian government to exercise control over information flows via internet infrastructure, including a blacklist to filter internet content, the law on "sovereign RuNet," the failed attempt to ban the messenger app Telegram in the country, and a list of "socially significant websites" that could potentially be used as a "white list" of accessible internet resources. She concluded that these measures "do not work as the government would wish" (Stadnik, 2021b) and that content filtering leads to, among other things, undesirable side effects for the whole network.

Ramesh and colleagues did an investigative study of technical censorship mechanisms employed by the Russian state and came to the conclusion that the design of Russia's internet censorship in a decentralized network "is a blueprint, and perhaps a forewarning of what national censorship regimes could look like in many other countries" that have a network design similar to Russia's (Ramesh et al., 2020, p. 13). This makes the Russian case of internet control of significant importance for global internet governance, as it is potentially replicable in other countries, in contrast to that of China, where the internet is centralized by design.

After the introduction of the "sovereign internet" bill, several reports emerged analyzing Russian internet policy (Epifanova, 2020; Gruska, 2019; Soldatov, 2019). However, there is still a lack of academic research on the Russian approach to digital sovereignty. This study aims to address this gap by answering the following research question: What is the strategic narrative of the Russian government on internet sovereignty, and what are the main factors that have influenced its development?

4. Methodology

In order to address the research question, I have analyzed the official strategy papers on internet policies in Russia, issued by the government in the period 1999–2019, and I have conducted five semi-structured interviews with experts, which helped reconstruct the government's strategic narrative and identify the key factors in its evolution over time. The Russian official strategies and doctrines "feature the official position in regard to aims, tasks, principles and the main directions" of governmental policies (Russian Federation, 2016). They can thus be seen as an articulation of strategic narratives that are applied as fundamental principles for future legislation. In accordance with the terminology of Roselle et al. (2014), the narratives of official internet strategies in Russia can be categorized as issue narratives and are targeted both at the domestic audience to legitimize policies and at foreign governments as official messages in international politics.

From 1999 to 2020, the following seven strategic papers on internet policies were issued: Strategies of the Information Society Development (1999, 2008, 2017), Doctrines of Information Security (2000, 2016), Basic Principles for State Policy in the Field of International Information Security (2013), and Development Strategy for IT Industry for 2014–2020 and until 2025 (2013). I have also included the 2019 Federal Law 90-FZ, known as the "sovereign internet" bill, in the analysis, insofar as it contains a memorandum explaining the official rationale for introducing the bill.

The document analysis combined elements of content analysis and thematic analysis (Bowen, 2009, p. 32). It aimed at reconstructing the official state narrative in regard to independence in cyberspace by identifying the three elements in strategic narratives: problematized issues, claims of causality, and proposed solutions (Miskimmon et al., 2013; Szostek, 2017). In this particular case, it means focusing on the following categories: (1) key terms of internet policy, (2) rationales provided for policies in regard to independence in internet space, and (3) solutions—that is, policies themselves.

After completing the document analysis, I conducted five semi-structured interviews with experts on internet governance in Russia. The aim of the interviews was twofold: (1) to verify the findings of the document analysis and (2) distinguish the major factors that have led to changes in the strategic narrative on internet sovereignty over time.

The experts interviewed are representatives of different areas of expertise in Russian internet governance: Ilona Stadnik (Coordination Center for TLD .RU/.РФ), Michail Medrish (former head of the Coordination Center for TLD .RU/.РФ and member of the Council

of Europe's Committee of Experts on Cross-Border Flow of Internet Traffic and Internet Freedom), Andrei Soldatov (investigative journalist specializing in Russian internet policies), Polina Kolozaridi (researcher of the RuNet, associate professor at the National Research University Higher School of Economics), and Alena Epifanova (expert on Russia's domestic and foreign policy in cyberspace, German Council on Foreign Relations). In the interviews, I asked these experts to describe the Russian approach to internet sovereignty and how it differs from that of other countries, to name the milestones in the evolution of this approach, and the factors that, in their view, influenced this development. I also asked them to verify my conclusions from the document analysis. The interviews conducted via Skype were recorded, transcribed, and analyzed using NVivo software.

5. Findings

Below, I present the findings of the document analysis, according to the key areas of my inquiry: key terms of internet policy, rationales provided for policies in regard to independence on the internet, and solutions/policies.

5.1. Key Terms of Internet Policy

It is remarkable that the term "internet" is not mentioned in the strategic documents of 1999 and 2000 and is only mentioned three times in the eight pages of the 2008 Strategy of the Information Society Development. It was only in 2013 that the internet was mentioned prominently in the documents analyzed. The terms most widely used in all the documents are "information," "information sphere," and "information and communication technologies." In the 2000 Doctrine for Information Security, the role of the information sphere in the "strengthening of moral values of society" is emphasized. Here, for the first time, the necessity of "technological independence" for Russia in the IT sphere is mentioned.

The Information Society Development Strategy of 1999 sounds very optimistic and states that the main strategic goal of Russia in transition towards an information society is "the creation of a developed information and communication societal environment and Russia's integration into the global information community" (Russian Federation, 1999). In the 2008 strategy, the focus lay in the improvement of electronic governance, as well as in participation in international norm development and in the mechanisms of internet governance.

In both Doctrines for Information Security (2000, 2016), there is no mention of "cybersecurity," which is usually used in international documents. The focus is always on information, that is, on content, not on the channels of its transmission. According to these documents, Russia should counter "information threats," inter alia, information war. Although "information war" is an important term for the Doctrines, no clear definition of it is provided. Among the external threats to information security of the Russian Federation, "the development by a number of states of concepts of information wars" is listed, which implies "creation of means of dangerous impact on information spheres of other countries, violation of the normal functioning of information and telecommunication systems, safety of information resources, obtaining unauthorized access to them" (Russian Federation, 2016).

The 2017 Strategy of the Information Society Development places a bigger focus on the digital economy compared to those of 1999 and 2008. An important term in this strategy is "critical information infrastructure," which means information technologies used by state institutions and by different industries. In order to secure the critical information infrastructure, the state has to support and represent the interest of the national IT companies. In the 2017 document, one of the main aims of internet policy is a development in Russia towards being a "knowledge society," which is defined as a society "where the acquisition, preservation, production and dissemination of reliable information, while taking into account the strategic national priorities of the Russian Federation, are of predominant importance for the development of a citizen, the economy and the state" (Russian Federation, 2017).

In the 2013 Basic Principles for State Policy in the Field of International Information Security, "international information security" is defined as follows:

> A state of the global information space that excludes the possibility of violating the rights of an individual, society and the rights of the state in the information sphere, as well as destructive and illegal impact on the elements of the national critical information infrastructure. (Russian Federation, 2013a)

Following these principles, Russia should promote the establishment of an international legal order aimed at the "formation of an international information security system" (Russian Federation, 2013a).

5.2. Rationales and Solutions

The rationales behind the Russian internet policies in strategic papers have undergone a massive evolution over time. In the 1999 Strategy for Development of Information Society, the importance of preserving its independence in the process of globalization is mentioned, but the overall tone about globalization is optimistic and friendly towards the international community, which is even called a "family": "Russia has to join the family of technologically and economically developed countries as a full-fledged participant in the world civilizational development while maintaining political independence, national identity and cultural traditions" (Russian Federation, 1999).

According to this document, Russia has to find its own way in the information society, which would be

oriented to the Russian socio-cultural context and would require minimum financial investments from the state. This rather *laissez-faire* attitude of the state towards internet business is characteristic of the first decade of the 21st century.

In the 2000 Doctrine for Information Security, the list of the main threats to information security is not that long and is rather vaguely formulated: from threats to human rights to "the spiritual revival of Russia," to "information support of the state policy of the Russian Federation," and brain-drain of IT specialists. As a solution, the document emphasizes the importance of "information support of the policies of the Russian Federation," by providing the Russian and international audience with reliable information in this regard (Russian Federation, 2000). Support for Russian IT production is also highlighted.

The 2008 Strategy of the Information Society Development, which marked the start of the presidency of Dmitry Medvedev, was still optimistic towards information and telecommunication technologies, which, by then, had become "a locomotive of the socio-economic development" worldwide, so the state had to ensure "access of citizens to information" and develop e-governance services (Russian Federation, 2008).

The 2013 Strategy for Development of IT Industry for 2014–2020 mentions the increasing role of the internet in society: In 2012, the monthly audience of the internet in Russia reached more than 55 percent (Russian Federation, 2013b). "The absence of territorial borders on the internet" was seen as a chance for Russian IT companies to become leaders in the international market. Increasing the attractiveness of Russia as a jurisdiction for the operation of IT companies would positively affect the development of the domestic IT industry.

The 2013 Basic Principles for State Policy in the Field of International Information Security includes the promotion of Russian initiatives in the area of international information security. This is important, as ICTs can be used as, among other purposes, an "information weapon" for "discrediting sovereignty, violating the territorial integrity of states," and violating public order (Russian Federation, 2013a).

In the 2016 Doctrine for Information Security, the list of threats from ICTs become more articulate in comparison to the earlier 2000 document, and features, among other things, cybercrimes, terrorism, and the promotion of Russia-critical content by foreign actors. Moreover, according to the document, Russia runs a risk of being targeted by so-called "information weapons" due to "the intensive introduction of foreign information technologies" in Russian society. According to the 2016 Doctrine, these threats should be combatted by defending one's "own information sphere" from external influence. What exactly does this mean? For one thing, it means the so-called "import substitution" by national products and the protection of national interests in the market. Information security is to be provided not only by state authorities, but also by state media and telecom operators (Russian Federation, 2016).

The 2017 Strategy of the Information Society Development emphasizes the priority of "moral values traditional for Russia and social norms based on them when using technologies" (Russian Federation, 2017). This should be done by, for example, promoting information resources that are based on so-called "traditional Russian values." However, these values are not further defined.

The strategy papers starting from 2013 have increasingly mentioned various abstract foreign threats. The explanatory memorandum of the 2019 "sovereign internet" bill is more direct in its wording: It names the US as a threat to the sustainability of the internet in Russia. The bill was prepared "considering the aggressive tone of the US National Cyber Strategy adopted in September 2018" (Russian Federation, 2019). According to the memorandum, Russia was "groundlessly accused" by the US of commissioning hacker attacks and was threatened with punishment. The memorandum implies that this punishment could be the disruption of the country's internet. Therefore, according to the same document, in order to guarantee "a sustainable operation of the internet in Russia," preventive measures have to be taken. The bill implements technical means of countering "threats for integrity, sustainability and safety of functioning on the territory of the Russian Federation of the 'Internet' network" (Russian Federation, 2019). The so-called "sovereign internet" bill obliges internet providers to install devices provided by the state that can monitor and block internet traffic. These measures are thus presented as a preventive defense strategy against foreign threats.

5.3. Evolution of the Strategic Narrative on Internet Sovereignty Over Time

The analysis of strategic narratives on internet policies in official documents from 1999 to 2019 shows a shift that occurred around 2013: from perceiving the globalization of information primarily as a chance for, and source of, economic growth to focusing on threats that come with dependence on Western technologies and vulnerabilities of the open information space.

All documents emphasize that it is control over the content of information that matters first and foremost. According to the expert Andrei Soldatov, this constitutes a crucial difference from the Western approach to internet governance: "The Americans, the British, talked about cyber security, the security of wires, of power stations, that is, 'the iron.' And our officials have always used the term 'information security'… that is, content."

For Soldatov, the roots of the fundamental split in the understanding of the threat of the internet between Russia and the West lie in Russia's domestic affairs in the 1990s. According to the expert, at the beginning of the Second Chechen War in 1999, Putin had to explain

the government's failure in the First Chechen war, so he blamed it on the information interference of the journalists who covered the conflict. As a result, the Information Security Doctrine of 2000 stated the importance of the defense of the information sphere.

Based on the combination of the analysis of strategic narratives and expert interviews, the following elements of the Russian concept of internet sovereignty can be distinguished:

1. Control over data flows (i.e., filtering of content and data localization);
2. Control over infrastructure (i.e., protectionism of national software, centralized system of monitoring internet traffic);
3. Promotion of Russian initiatives at the international level.

The experts have distinguished the following factors, which, in their view, helped shape this approach: (1) domestic politics, (2) economic factors, (3) international relations, and (4) the historical trajectory of RuNet.

5.3.1. Domestic Politics

Inner political rationales were mentioned in the official documents and dealt with guaranteeing constitutional rights for citizens, as well as warranting stability, security, and economic progress in the country. However, as the experts confirmed, some of the important triggers for internet regulation were left out of sight in the official narrative. Thus, the protest movement "For Fair Elections" in 2011–2012 was crucial for the major shift towards the internet sovereignty that we observed in documents starting from 2013. The street protests broke out after the revelation of fraud during the parliament elections in December 2011 and demonstrated the power of social media in triggering an oppositional movement, which made the state reconsider its *laissez-faire* attitude towards regulation of online communication (Litvinenko & Toepfl, 2019). For the Russian government, said Alena Epifanova, this protest wave was apparently a more significant factor than the previous Arab Spring.

Another important trigger for the tightening of internet control was regional protests in 2017–2019. According to Andrei Soldatov, the blocking of the internet just in time in Russian regions in order to curb political dissent was one of the major aims of the "sovereign internet" bill.

Ilona Stadnik mentioned the case of the failure to block the Telegram messenger app in 2018–2020 as a catalyst for developing new mechanisms of control over the internet infrastructure. Telegram was officially blocked after the presidential election in 2018, but regulating institutions failed to stop its work. Citizens continued to use Telegram via VPNs, and it became even more popular, so the government decided to officially unblock it in July 2020.

Three experts also mentioned the role of elite power struggles within the Russian government, the so-called "war between the Kremlin towers." The first decade of internet development in Russia was dominated by more liberal elites, who were calling for Russia's modernization, especially under Medvedev's presidency in 2008–2012. Starting from the Putin's third presidential term in 2012, the role of *siloviki* (members of the ministries in charge of national security) has been increasing significantly. For them, security is more valuable than progress, and they tend to be in favor of internet blockages and other restrictions.

However, the government still cannot afford to simply cut Russia's access to global social media platforms, as it would most probably trigger major social unrest. Over the decades, people have gotten used to free communication online, and many users have built their businesses using the monetization models of YouTube or Instagram. According to Soldatov, this, among other factors, constitutes an important difference between the internet in Russia and in China. Thus, the government has to balance between its urge to control the information space and the risks of putting too much pressure on civil society.

5.3.2. Economic Factors

In the 2000s, the liberal approach to internet legislation was inspired by the perceived benefits of digitalization, which is reflected in the documents analyzed. An internet isolation policy, on the one hand, would mean losing many of those benefits. According to expert Ilona Stadnik, Russia cannot afford the risk of being disconnected from the global digital economy.

On the other hand, the aspiration of Russia to be independent in regard to internet infrastructure contradicts the current potential of the Russian IT industry. Despite the protectionism policy towards Russia's IT companies, Russia has no capacities to substitute all the imported IT products with Russian equivalents. Epifanova poses the question: "Will Russian Internet sovereignty be made in the US or in China?"

Over the past decade, Russian IT companies have been increasingly subjected to more control and compliance by the state. In 2016, the introduction of the Yarovaya law package, which obligated providers to store all communication data for six months at their own expense, stirred up a large protest within the IT industry. In 2019, the "sovereign internet" bill mandated that providers install equipment that would monitor internet traffic. However, Soldatov pointed out, this time the measure was to be paid for by the state, so the IT industry did not voice as much discontent as it had with the law of 2016. According to the expert, the IT companies realized that "with the current Russian image, they do not have many chances abroad anyway, so they have to develop the domestic market."

5.3.3. International Relations

This factor plays a crucial role in the state rationale behind the necessity of internet independence. Already in the 2000 Doctrine for Information Security, dependence on foreign IT companies is listed as one of the threats to national security. In 2019, the sovereign internet bill was framed as a reaction to the "aggressive tone" of the 2018 US National Cyber Strategy. The experts emphasized that the international relations factor was used rather as a tool to frame restrictive policies for the Russian audience.

The experts agreed upon the following international milestones, which had an influence on the Russian approach to internet sovereignty: (1) Edward Snowden's revelations in 2013, (2) international sanctions against Russia after the annexation of Crimea in 2014, and (3) the accusation of Russia in the interference in the US elections of 2016. Interestingly, as experts Kolozaridi and Stadnik point out, the Snowden revelations seem to have had less of an impact on Russian internet governance compared to the consequences they had in the West. In Russia, the digital sovereignty discourse started to evolve intensely after the introduction of economic sanctions in 2014 and the subsequent policy of import phaseout.

The scandal around the alleged interference of Russia in the US elections and around the data breach in Cambridge Analytica made the West reconsider its attitude toward cybersecurity. In the framework of fake-news debates, internet security is now also discussed in the West in terms of having control over content of information. Russia has perceived this as a window of opportunity to promote its understanding of information security, which it has already been sharing with China for a long time. According to Soldatov, legislation on fake news in different countries has given Russian authorities an opportunity to promote its narrative on information security.

Interestingly, dependence on global online platforms, which is central to digital sovereignty debates in the EU, has not been specifically thematized in the analyzed documents. However, this aspect has recently started to play a big role in public discourse and may be included in the strategic narrative on internet sovereignty in the future.

5.3.4. Historical Trajectory

In the interviews, all the experts mentioned the importance of the legacy of the historical development of RuNet, both from the technological and from the societal perspective, in shaping internet policies. According to Michail Medrish, the infrastructure of the Russian internet was initially designed to be highly decentralized, so it is hard to gain centralized control over RuNet. Soldatov elaborates that the liberal phase in internet regulation that lasted until 2012 shaped the country's online market as well as users' habits, and the state has been forced to take this into consideration on its path towards digital sovereignty. Epifanova concludes that the historical trajectory of RuNet makes the Russian model of digital sovereignty potentially attractive to other regions of the world, in contrast to the Chinese model, which is considered to be non-replicable.

6. Discussion and Conclusion

The Russian strategic narrative on internet policy has been changing over time, depending on the elite's evaluation of the benefits that global connectivity brings versus its perceived threats. The crucial element in Russia's understanding of internet independence is the concept of information security, which is content-oriented, in contrast to the Western concept of cybersecurity, which initially was more infrastructure-focused. This means that control over the content of data flows lies at the core of the Russian approach to internet sovereignty, and control over the infrastructure is seen as a tool to achieve this goal.

This contradicts the European understanding of digital sovereignty, which is based on the concept of the self-determination of the people (Pohle, 2020). As Europe has only recently coopted the concept, we are currently observing a global struggle of strategic narratives on digital sovereignty: a state-centered approach represented by Russia and China, where online borders are drawn maximally near the offline ones, and the individual-centered approach of the EU, where the people are called "sovereign."

However, the democratic interpretation of internet sovereignty appears, so far, to be even more vague than the authoritarian one, as democratic mechanisms of the self-determination of its netizens are still underdeveloped. Given the power of narratives in shaping the behavior of actors in international relations (Miskimmon et al., 2013), it seems to be important for international actors now to have an articulate vision and rationale for their approach to this widely used term. In a situation of struggle between strategic narratives around digital sovereignty, the promotion of a country's narrative at the international level becomes one of the key elements of internet sovereignty. This, among other things, helps build regional alliances among countries that hold similar positions on internet governance and thus gives more weight to arguments in favor of certain regulatory decisions on a global level.

The Russian case of internet sovereignty is of special importance for global internet governance, as it is an attempt to subject a highly decentralized network to tight state regulation via a series of measures, including control by infrastructure (Stadnik, 2021b). On the one hand, it has a direct influence on some post-Soviet countries where RuNet plays an important role, such as Belarus or Kazakhstan, and an indirect impact on many other segments of the global network through diffusion of legislative norms and practices. The global effects of

national approaches to digital sovereignty are still to be explored in future studies.

On the other hand, the Russian case reveals the weaknesses of the authoritarian model of digital sovereignty, which causes side effects for the network in the country. This model is also challenged by infrastructure-based resistance, as in the case of the attempted Telegram ban (Daucé & Musiani, 2021). Further study of the discrepancies between the norms and practices of digital sovereignty would help us better understand the mechanisms that shape today's internet governance.

Overall, we have observed that a strategic narrative on digital sovereignty is more than just an issue narrative, as it deals with a vision of the future of national segments of the internet as well as that of global internet governance. Comparative studies of national approaches to digital sovereignty are needed in order to define common ground for collaboration, as well as to distinguish between decisive divergences in envisioning the future of the global network.

Acknowledgments

This work was supported by the German Federal Ministry of Education and Research, funding code 16DII114, in the form of a fellowship of the Weizenbaum Institute for the Networked Society.

Conflict of Interests

The author declares no conflict of interests.

References

Barlow, J. P. (1996). A declaration of the independence of cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Daucé, F., & Musiani, F. (2021). Infrastructure-embedded control, circumvention and sovereignty in the Russian internet: An introduction. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11685

Epifanova, A. (2020). Deciphering Russia's "Sovereign internet law": Tightening control and accelerating the Splinternet. *DGAP Analysis*, *2020*(2). https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

Gruska, U. (2019). *Taking control? Internet censorship and surveillance in Russia*. Reporters Without Borders. www.reporter-ohne-grenzen.de/russiareport

Kedezie, C. R. (1997). *Communication and democracy: Coincident revolutions and the emergent dictator's dilemma*. RAND.

Kleinwächter, W. (2021, January 8). Internet governance outlook 2021: Digital cacaphony in a splintering cyberspace. *CircleID*. https://www.circleid.com/posts/20210108-internet-governance-outlook-2021-digital-cacaphony

Kolozaridi, P., & Muravyov, D. (2021). Contextualizing sovereignty: A critical review of competing explanations of the internet governance in the (so-called) Russian case. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11687

Lehtisaari, K. (2019). Formation of media policy in Russia: The case of the Iarovaia law. In M. Wijermars & K. Lehtisaari (Eds.), *Freedom of expression in Russia's new mediasphere* (pp. 57–73). Routledge.

Litvinenko, A., & Toepfl, F. (2019). The 'gardening' of an authoritarian public at large: How Russia's ruling elites transformed the country's media landscape after the 2011/12 protests 'For Fair Elections.' *Publizistik*, *64*(2), 225–240.

Merkel, A. (2019). *Speech opening the 14th Annual Meeting of the Internet Governance Forum in Berlin on 26 November 2019* [Speech transcript]. Press and Information Office of the Federal Government. https://www.bundeskanzlerin.de/bkin-en/news/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494

Michaelsen, M. (2018). Transforming threats to power: The international politics of authoritarian internet control in Iran. *International Journal of Communication*, *12*(2018), 3856–3876.

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). *Strategic narratives: Communication power and the new world order*. *Routledge studies in global information, politics and society* (Vol. 3). Routledge; Taylor & Francis Group.

Müller, M. L. (2017). *Will the internet fragment? Sovereignty, globalization, and cyberspace*. Polity.

Oates, S. (2013). *Revolution stalled*. Oxford University Press.

Pohle, J. (2020, December 15). Digital sovereignty: A new key concept of digital policy in Germany and Europe. *Konrad Adenauer Stiftung*. https://www.kas.de/en/single-title/-/content/digital-sovereignty

Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., Sprecher, S., Ikram, M., & Ensafi, R. (2020). Decentralized control: A case study of Russia. In D. Xu & A.-R. Sadeghi (Eds.), *Proceedings 2020 network and distributed system security symposium* (pp. 1–18). Internet Society. https://doi.org/10.14722/ndss.2020.23098

Richter, A. (2007). *Post-Soviet perspective on censorship and freedom of the media*. UNESCO Moscow Office.

Richter, C., & Kozman, C. (Eds.). (2021). *Arab media systems*. Open Book Publishers. https://www.openbookpublishers.com/product/1281

Roselle, L., Miskimmon, A., & O'Loughlin, B. (2014). Strategic narrative: A new means to understand soft power. *Media, War & Conflict*, *7*(1), 70–84. https://doi.org/10.1177/1750635213516696

Russian Federation. (1999). *Kontseptsiya formirovaniya informatsionnogo obshchestva v Rossii* [Concept of development of information society] (No. 32). http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/37cd5e6756dce634c32568c000474a8a

Russian Federation. (2000). *Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsi* [Doctrine of information security of the Russian Federation] (N Pr-1895). http://base.garant.ru/182535

Russian Federation. (2008). *Strategiya razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii* [Strategy of the information society development in the Russian Federation] (N Pr-212). https://rg.ru/2008/02/16/informacia-strategia-dok.html

Russian Federation. (2016). *Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsi* [Doctrine of information security of the Russian Federation] (N 646). http://ivo.garant.ru/proxy/share?data=q4Og0aLnpN5Pvp_qlYqzjK_xqrzXt9W_qeqZArb1tcalo_yf8-aowbnJtcvygADzs-CA4ZPhgf2P5pb8nfPvvualzLXQpdG50wLqneeE5LXnseO8rQ

Russian Federation. (2013a). *Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti na period do 2020 goda* [Basic principles for state policy in the field of international information security to 2020] (N Pr-1753). http://www.consultant.ru/document/cons_doc_LAW_178634

Russian Federation. (2013b). *Strategiya razvitiya otrasli informatsionnykh tekhnologiy v Rossiyskoy Federatsii na 2014–2020 gody i na perspektivu do 2025 goda* [Strategy for the development of the information technology industry in the Russian Federation for 2014–2020 and for the future until 2025]. https://digital.gov.ru/ru/documents/4084

Russian Federation. (2017). *O strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody* [On the strategy for the development of the information society in the Russian Federation for 2017–2030] (No. 203). http://publication.pravo.gov.ru/Document/View/0001201705100002

Russian Federation. (2019). *Zakonoproyekt № 608767-7 O vnesenii izmeneniy v Federal'nyy zakon «O svyazi» i Federal'nyy zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii"* [Draft Law No. 608767-7 on amendments to the federal law on changes in the federal law "On communication" and the federal law "On information, information technologies and information protection"]. https://sozd.duma.gov.ru/bill/608767-7

Schulze, E. (2019, November 1). Russia just brought in a law to try to disconnect its internet from the rest of the world. *CNBC*. https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html

Shimaev, R., Peletayeva, P., & Rumyanzeva, A. (2019, April 16). "Otklyuchit' rubil'nik uzhe ne poluchitsya": Gosduma utverdila zakon o bezopasnom i ustoychivom internete ["Turning off the switch will no longer work": The State Duma approved the law on a safe and sustainable internet]. *Russia Today*. https://ru.rt.com/dbxj

Soldatov, A. (2015). Ukroshtshenie interneta [Taming the internet]. *Contrapunkt*, *2015*(1), 1–11.

Soldatov, A. (2019). Security first, technology second: Putin tightens his grip on Russia's internet—With China's help. *DGAP Policy Brief*, *2019*(3). https://dgap.org/en/research/publications/security-first-technology-second

Stadnik, I. (2021a). Russia: An independent and sovereign internet? In B. Haggart, N. Tusikov, & J. A. Scholte (Eds.), *Power and authority in internet governance: Return of the state?* (1st ed., pp. 147–167). Routledge. https://doi.org/10.4324/9781003008309

Stadnik, I. (2021b). Control by infrastructure: Political ambitions meet technical implementations in RuNet. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11693

Steiner, F., & Grzymek, V. (2020). *Digital sovereignty in the EU*. Bertelsmann Foundation. https://www.bertelsmann-stiftung.de/en/publications/publication/did/digital-sovereignty-in-the-eu-en

Stolton, S. (2019, September 12). Altmaier's cloud initiative and the pursuit of European digital sovereignty. *Euractiv*. https://www.euractiv.com/section/data-protection/news/altmaiers-cloud-initiative-and-the-pursuit-of-european-digital-sovereignty

Szostek, J. (2017). The power and limits of Russia's strategic narrative in Ukraine: The role of linkage. *Perspectives on Politics*, *15*(2), 379–395. https://doi.org/10.1017/S153759271700007X

Thiel, T. (2021, January 25). Das Problem mit der digitalen Souveränität [The problem with digital sovereignty]. *Frankfurter Allgemeine Zeitung*. https://zeitung.faz.net/faz/unternehmen/2021-01-25/4b6c5ef358b56fe3c17d9912315df988/?GEPC=s3

Vendil Pallin, C. (2017). Internet control through ownership: The case of Russia. *Post-Soviet Affairs*, *33*(1), 16–33.

Woodhams, S. (2019, April 23). The rise of internet sovereignty and the end of the world wide web? *The Global Post*. https://theglobepost.com/2019/04/23/internet-sovereignty

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "internet sovereignty." *Politics & Policy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202

About the Author

Anna Litvinenko (PhD) is a researcher in the Digitalization and Participation Department at the Institute for Media and Communication Studies, FU Berlin, Germany. After receiving her PhD in 2007, she was associate professor in the Department of International Journalism at St. Petersburg University, Russia. Her research focuses on political communication in the digital age, comparative media studies, and the role of social media in various socio-political contexts.