Control by infrastructure: Political ambitions meet technical implementations in RuNet
by Ilona Stadnik

Abstract
Discourse about sovereignty and Internet in Russia is predominantly focused on control of harmful content and information and its negative influence on the political regime and society. However, content control is not the only way to exercise sovereignty over digital media and the Web. Recently, the Russian government started to realize that without controlling Internet infrastructure, most strategies to filter and block Web sites and services are wasted. In the past five to seven years, Russia invested a lot of efforts in the development and adoption of new laws and regulations that deal with RuNet infrastructure, where the aim of centralized Internet traffic control was a real novelty, albeit a very ambitious political goal. This article tries to address the pitfalls of the control-by-infrastructure endeavor of the Russian government through four emblematic cases: the implementation of the “Revizor” system to control ISPs’ compliance to filter Internet resources from the blacklist; the battle to block Telegram messenger in Russia; the implementation of law FZ-90 (popularly referred to as the law “on Sovereign RuNet”); and finally, the ongoing experiment with free access to ‘socially significant Web sites’, which may have serious consequences in the future if used as a ‘white list’ of permitted Web resources. These four cases were chosen because they are deeply interconnected and show how the government has been gradually implementing infrastructure control in connection to content control.

Contents
Introduction
Discussion of literature and methodology
1. “Revizor”
2. The battle for Telegram
3. Implementation of the law on “on Sovereign RuNet” (FZ-90)
4. Free access to socially significant Internet resources
Conclusions

Introduction
During and after the World Summit on the Information Society (WSIS) in 2003–2005, scholars started actively elaborating on the role of the state in Internet governance (Drezner, 2004; Goldsmith and Wu, 2006; Eriksson and Giacomello, 2009; Mueller, 2010). The WSIS outcome documents explicitly delineated the areas of responsibility between multiple stakeholders — states, business, international organizations and
Control by infrastructure: Political ambitions meet technical implementations in RuNet

civil society [1]. However, the multistakeholder approach has been scrutinized (Dutton and Peltu, 2007; Carr, 2015; Raymond and DeNardis, 2015; Hofmann, 2016) and criticized, with what has been argued as a “return of the state” in Internet governance (Haggart, et al., 2021). Indeed, all over the world, states have become more prominent in the regulation and control of the Internet and related digital issues, especially those liberal democracies attempting to restrict and regulate the work of big tech giants that yield considerable power today and serve multiple roles: Internet/Web infrastructure providers, digital service platforms, data keepers.

States’ attempts to control the Internet have been theorized in multiple ways, with concepts such as information sovereignty, Internet sovereignty, digital sovereignty (Couture and Toupin, 2019), Internet fragmentation (Fehlinger, 2014; Drake, et al., 2016; Mueller, 2017) and others. This article will focus on the Russian interpretation of these concepts, connecting them to the role of infrastructure in RuNet (the Russian segment of the global network) governance policies (DeNardis, 2014), particularly focusing on the idea of control by infrastructure (Musiani, et al., 2016).

Sovereignty discourses about the Internet in Russia are still mostly focused on control of harmful content and information and their negative influence on the political regime and society. However, the government started to realize that without controlling infrastructure, most strategies to filter and block Web sites and services are wasted. Since 2014, Russia invested a lot of efforts in the development and adoption of new laws and regulations that deal with RuNet infrastructure, where the aim of centralized Internet traffic control was a real novelty, albeit a very ambitious political goal. Thus, the article will address the pitfalls of the control-by-infrastructure endeavor of the Russian government through four emblematic cases: the implementation of the “Revizor” system to control the ISPs’ compliance to filter Internet resources from the blacklist; the battle to block Telegram messenger in Russia; the implementation of the law FZ-90 (popularly referred to as the law “on Sovereign RuNet”); and finally, the ongoing experiment with free access to ‘socially significant Web sites’, which may have serious consequences in the future if used as a ‘white list’ of permitted Web resources. These four cases were chosen because they are deeply interconnected and show how the government has been gradually implementing infrastructure control in connection to content control.

Providing historical and political context for the development of Internet policy in Russia is necessary to explain this gradual turn to infrastructure. Kolozaridi and Shubenkova (2015) highlight two main periods in the official discourse of Internet representation in Russia’s social policy: Internet as a benefit and Internet as a threat. On the one hand, from 2000 to 2011, the Russian government consistently finances and implements national programs to build Internet infrastructure and increase the digitalization of state and other services for the benefit of public and economic development. On the other hand, starting from 2012 (the beginning of the third presidency term of Putin) the Internet becomes a “threat” to the security of the society and state. The Arab Spring and the role of social networks in the coordination of civil protests in the Middle East and north Africa region left an indelible impression on the Russian elite (Stepanova, 2011; Comunello and Anzera, 2012). Subsequent Russian mass protests during the State Duma elections in 2011 spurred restrictive policies towards the Internet, with a focus on surveillance and censorship (Soldatov and Borogan, 2015; Denisova, 2017; Gainous, et al., 2018; Pigman, 2019). It led to the creation of a blacklist of Internet sites and Web pages and constantly enlarging body of regulations for prohibited types of information, penalties for ISPs, search engines and users. Interestingly, while the government continued its development policy (The Russian Government, 2017), the threat discourse has been strengthened (doctrine 2016), including threats to RuNet itself. After the Snowden revelations of U.S. cyber activities (Greenwald, 2014) and, especially, the case of the alleged U.S.-led accidental Internet shutdown in Syria (Bamford, 2014) the Russian government started to seriously consider the possibility of an external RuNet shutdown (Ministry of Communications, 2014). The 2018 U.S. cybersecurity strategy only exacerbated the concerns of Russian lawmakers since it implicitly named Russia as an adversary and provided for the full spectrum of preventive measures in cyberspace. The U.S. cyber policy is often referred to as a trigger for the imminent adoption of sovereign RuNet law (State Duma, 2019. “Readings ...”).


Discussion of literature and methodology

This article aims to contribute to the study of the Internet governance subfield defined by Musiani, et al. (2016) as a “turn to infrastructure”, where “points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the flow of money, information, and the marketplace of ideas in the digital sphere.” Furthermore, this paper looks at the so-called ‘dark side’ of Internet governance: approaches designed to restrict the flow of information or enact systems of surveillance and censorship (DeNardis, 2014). DeNardis introduced four major examples of these approaches: deep packet inspection (DPI) technology; Internet kill switches; delegated censorship through private intermediaries; and DDoS against civic advocacy and freedom of expression. They are instances of “governance” in local formats which, however, may have consequences at the global/macro level. Russia’s policy in this regard is a very intriguing case, because it definitely differs from the Chinese experience (which is often cited alongside the Russian one as an example of ‘authoritarian’ take on the Internet), especially in terms of infrastructure composition and internal digital market (Budnitsky and Jia, 2018). However, this makes it an even more interesting subject of inquiry, as well as an example for imitation by other states. English-language scholarship on this topic is still scarce, especially when it comes to the development of domestic narratives in the regulation of telecom and RuNet (Nocetti, 2015; Ermoshina and Musiani, 2017; Asmolov and Kolozaridi, 2017; Stadnik, 2021a, 2019a; Epifanova, 2020). Kovaleva (2018) describes as ‘information space’ the economic and legal tools used by the Russian government to influence content production and distribution, while Budnitsky (2020) considers Russian national identity and cultural approach to explain Internet-related policies, including the Russian stance on global Internet governance. Claessen (2020) looks at the increased importance of Internet infrastructure through the prism of security.

States always sought to establish strategic control points, and the Internet is not an exception; as we write, the general trend towards increased digital sovereignty for political, economic, privacy and security reasons concerns both authoritarian and democratic states. Historically, authoritarian regimes have shown a restrictive approach to the Internet; State involvement in Internet governance with national digital/telecom market protection and content censorship was opposed to approaches that advocated for commercialization, open markets, free movement of data and information and freedom of speech, until recently. In 2021, an increasing number of states have begun to discuss restrictive measures for digital platforms and content distribution, data flows and even ideas of isolated Internet clouds with law-abiding IT players, such as the European Internet [2]. Discussions during the Internet Governance Forum in Berlin in 2019 touched upon the theme of digital sovereignty and isolationism, trying to distinguish conceptions of sovereignty in cyberspace: “digital sovereignty does not mean protectionism, or that state authorities say what information can be disseminated — censorship, in other words; rather, it describes the ability both of individuals and of society to shape the digital transformation in a self-determined way.” [3]

Russia is often associated with the concept of Internet sovereignty both in the international arena (Stadnik, 2021a) and domestic Internet politics. To explain how Internet sovereignty and control by infrastructure are interconnected in Russia, a preliminary discussion of terminology is needed. Internet sovereignty as a term is not yet clearly established, as demonstrated by the diversity of its formulations; China is considered to be among the first states to articulate a cyber or Internet sovereignty notion. Similarly, there is no common definition of cyberspace, as well as information space: both terms are often interchanged with notions of the Internet, which is an excessive approximation. That is why different terms are used interchangeably to describe similar ideas: “Internet sovereignty”, “information sovereignty,” “network frontiers” (Zeng, et al., 2017). In Russia, a growing body of theoretical work is devoted to information sovereignty; Polikarpov, et al. (2014) defines information sovereignty through the analysis of threats coming from ICTs and ways to address them to maintain state sovereignty in the information space, while Vinnik (2014) considered information sovereignty in light of Internet filtering political and legal regimes. A more extended theory was proposed by Kucheryavyiy (2015): information sovereignty is the supremacy and independence of state authority in the formation and implementation of information policies in the national segment and the global information space. It includes three components:
“digital-technical” sovereignty — national production cycles of software and hardware, digital services, network protection equipment, payment systems;
“mental-psychological” sovereignty — high-level information culture of society, national ideology; and
“information-power” sovereignty — pro-government mass media, patriotic elites, solid state information policy.

Finally, Efremov (2017) has examined information sovereignty from a legal perspective. “The key to the realization of sovereignty is the possibility of regulating information relations within the relevant information space” [4]; information sovereignty, as a legal category, is the possibility for a state to regulate an information space through national law and international law developed with the participation of a given state. In its turn, state sovereignty in information space is realized through the information function of the state and its information policy. Information function is carried out primarily through legislative regulation of information relations. The development of digital technologies creates a need for expanding such regulation, but it can be carried out not only in the form of regulatory legal acts of a particular state, but also within the framework of documents of international organizations and self-regulation (Efremov, 2019).

Thus, discussions of information sovereignty in Russia mainly focus on content and information flows. Only Kucheryavyiy complements his concept with an infrastructure aspect, although he does not explicitly say that control of infrastructure is necessary to control content. If we turn to the Russian doctrine on information security, infrastructure is given little attention in contrast to direct and indirect impacts of harmful information on the Russian political regime and society (Doctrine, 2016). Though it indicates technological dependence on other countries and foreign IT vendors, unfair global DNS management and other problems, the document does not explicitly address infrastructure control for the sake of content control. Only in the mid-2010s, the government showed its concern about RuNet infrastructure and started the development of a bill aimed at copying routing databases and backup servers, and creating registries for IXPs [5]. With this bill came a narrative more focused on control of infrastructure. Only recently, the latest legislative innovation clearly traces the trend of control by infrastructure — law 90-FZ to ensure the resilience and information security of RuNet.

Drawing on insights from the literature noted earlier, and discussing case studies of attempts to control RuNet by infrastructure, this article argues that infrastructure often complicates the political ambitions of the state. While politics usually tries to keep up the pace of technology, technical actors display a great capability of adaptation to (and circumvention of) new policies. This is the result of multiple factors in each particular case: flexibility in decision-making; innovation without permission; and civil enthusiasm and volunteering. Instead, the government nominally has more resources, including power, but in fact, it is limited in its actions: it can adopt laws and regulations, monitor their implementation, issue fines for non-compliance or, on the contrary, adopts stimuli encouraging actors to abide. The problem for the government is its inability to directly initiate technological and infrastructural initiatives at the operational level. To do so, it has to rely on proxies — state-owned telecom companies or loyal IT businesses and platforms to push forward policy decisions or test new ideas that are rapidly overthrown by the RuNet hacking community or sabotaged by the Russian telecom community [6].

This article analytically describes four cases of governmental attempts to leverage Internet infrastructure to fulfill political goals and gain more control over RuNet. Empirical material for this article consists of bills, laws and regulations issued by the Government, the Ministry of Digital Development, Roskomnadzor (Роскомнадзор), as well as investigations by journalists and commentary from the Russian telecom community illustrating how technical realities are pushing state efforts back.

1. “Revizor”
The Russian history of building a blacklist of Internet resources goes back to 2012 when the law 139-FZ amended the existing law on information (149-FZ) with a provision that defined reasons for including Web sites in the blacklist. These reasons primarily included child pornography, manufacture or receipt of drugs and their precursors and information about ways as well as calls to commit suicide. Later, the list of reasons was extended to extremist materials, calls to mass riots and unlicensed content (398-FZ, 187-FZ).

Thus, 139-FZ established a blacklist that contained domain names, URLs and IP addresses of Web pages with unlawful content. Roskomnadzor (RKN, the Russian federal supervising agency in the field of communication, IT and mass communications) acquired the powers to run the blacklist and fine owners of Web resources, as well as ISPs, if they did not remove unlawful content during a timespan defined by law. Namely, when a site with prohibited information is found, RKN must determine its hosting provider and send him a notification about the need to remove prohibited information. If the site owner or hosting provider does not delete the information within three days, the site enters the blacklist registry, which must be updated twice daily. The ISP is obliged to restrict access to sites from the registry within 24 hours from the date of an update.

Historically, RKN has not been responsible for blocking resources, as its role was limited to maintaining the blacklist and notifying providers. In the meantime, ISPs were free to decide how they would execute blocking from a technical standpoint. Initially, fines for non-compliance did not amount to much, so, in the beginning, most of the hosts and ISPs tried to ignore RKN notifications; for some it was easier to pay these fines. Later, the fines would be raised significantly, and were, in particular, very problematic for small ISPs and hosts [7].

Simultaneously, RKN encountered a problem in supervising the execution of blockings. It had neither a normative framework nor effective mechanisms to control ISPs who continued to provide access to blocked resources. So, in 2015, RKN started to elaborate a dedicated system called “Revizor” to check ISP compliance in blocking banned resources [8]. The system includes both hardware and software components, which automatically check whether an operator blocks sites from the blacklist and if not, it is qualified as an administrative violation and can lead to a fine for an ISP. In December 2016 Revizor became obligatory for all ISPs [9].

However, the absence of official technical rules on how to block resources made it difficult for ISPs to meet Revizor’s requirements. Several reverse-engineering efforts showed how Revizor checked the availability of banned resources from an ISP network — the program pretends to be a “user” and sends queries to Web resources from the blacklist [10]. The blacklist contained URLs, domain names, IP addresses or subnets of IPs.

Revizor turned to be an imperfect instrument and caused many problems for ISPs and a snowball of fines being issued automatically. First of all, there was the problem of automatic resolving: obtaining the domain name by IP is difficult since many resources may change their IPs for different reasons. ISPs had to synchronize their filtering mechanisms with the blacklist registry. It led to the situation when law-abiding resources were caught in the blacklist simply because the owner of a blocked domain designated an arbitrary or particular IP address. This vulnerability will play an important role in our analysis. The second problem was the dysynchronization of domain name resolving between Revizor and ISPs since the blacklist is updated twice a day, which also led to administrative fines. According to an RBC study, by 2017 Revizor covered 95 percent of all ISPs in Russia [11].

The summer of 2017 was marked by the largest exploitation of a vulnerability in the RKN system of blocking. Expired or ‘dead’ domain names that were stored in the blacklist were purchased to have access to their IPs. Some ISPs associated those IPs with RKN or other sensitive Web sites, thus making them inaccessible after Revizor updated its register, and later ISPs did the same. The attack affected not only RKN itself, but also Revizor servers, other government sites and popular Web resources, and even the banking infrastructure for a couple of days [12].
To stop the chaos, by the end of June 2017 RKN issued recommendations for methods to block Web resources, pointing that blocking by IP address could only be done for those resources for which this type of blocking was marked in the register. It also stressed that ISPs were highly encouraged to use DPI systems or filter DNS queries [13]. Thus, Revizor had to change its algorithm slightly; however, this vulnerability could still be exploited, given the fact that the blacklist was full of ‘dead’ domain names that could be purchased and exploited to block a target resource for a while once again. Later, recommendations obtained normative status — now it is an Order with legal force [14]. However, methods in the Order still do not fully coincide with the reality of Revizor checks. Additionally, RKN continues to ignore the problem of the overloaded blacklist and ‘dead’ domains that can be used for similar DNS attacks once again (Kulin, 2019).

The implementation of Revizor constitutes a first attempt to establish control by infrastructure. The Revizor system, an infrastructure inclusive of both hardware devices and algorithms, was initially designed to check ISPs’ compliance to block prohibited information. The lack of clear rules and methods for blockings made ISPs adapt intuitively to Revizor algorithms, thus exercising extensive filtering to avoid fines: ‘the entire history of blocking implementation in Russia is the history of checking these blocks’ (Kulin, 2019).

However, vulnerabilities in infrastructure forced RKN to change the rules subtending blockings so as not to end up harming itself and its objectives. Since opportunities for new DNS attacks through Revizor still exist, we cannot talk about full control of blockings by infrastructure.

After the adoption of the Federal law 90-FZ in 2019, the fate of blockings becomes unclear; such measures are supposed to be achieved without ISPs’ active participation, through Deep Packet Inspection (DPI) solutions provided by RKN. This means that the blacklist will be removed from the public, thus making it unclear (even for ISPs) whether a particular resource is unavailable due to technical errors or because it is blocked. Here, the ambition of the task seems superseded by the scale of the infrastructure necessary for its implementation. Who will develop and provide sophisticated DPI that will be able to filter all traffic? How much will it cost? How will this affect the speed and quality of services? Is it sensible to filter all traffic, especially encrypted traffic? How will plans to deploy the necessary equipment throughout the country change due to the COVID-19 crisis?

2. The battle for Telegram

In March 2018, Moscow’s Tagansky District Court ruled to block access to the Telegram messenger in Russia [15]. Telegram had refused to provide decryption keys to the Federal Security Service (FSB) under the provisions of Yarovaya’s anti-terrorists amendments [16] to the law on Information (149-FZ). RKN immediately started to block millions of IP addresses associated with Telegram, banning entire subnets and cloud providers like Amazon, Hetzner, Digital Ocean, and others. In chasing down Telegram, RKN affected the work of other services like Google, gaming Web sites, educational and other resources. The number of complaints from users and companies was in excess of two thousand [17]. Telegram continued to function due to the high level of community engagement in helping to develop proxies and masking of messenger traffic (see Ermoshina and Musiani’s article in this issue). The latter eventually led to the disruption of online banking operations, as they were using a protocol similar to the one Telegram used to mask its traffic, so RKN had to downplay its coercive activity.

This war against Telegram made the messenger even more popular in Russia and increased the number of active users. For the next two years, the inability to block Telegram became a reputational blow for RKN. It led to a double-standard policy: the messenger was officially blocked, but its use was de facto not prohibited — indeed, this is how high-ranking officials or state agencies justified themselves if they were themselves ‘caught in the act’ of using Telegram. Simultaneously, Telegram anonymous channels became a part of the new strategy of disseminating state propaganda and conducting political PR wars [18].

The culmination of this double standards policy happened during the COVID-19 crisis, when the Russian
Control by infrastructure: Political ambitions meet technical implementations in RuNet

Ministry of Foreign Affairs and Ministry of Digital development opened several official Telegram channels and groups to communicate with, and assist, Russian citizens abroad who were stuck in various countries because of the closed borders and awaited evacuation flights [19]. Having this practice in mind, State Duma deputies from “Fair Russia”, Fedot Tumusov and Dmitry Ionin, put forward a legislative initiative to make an amendment to the law on Information that would prohibit to block services used by the government to communicate with its citizens, implying Telegram [20]. “Further declarative blocking of the messenger thus causes damage, not to its development, but the prestige of the state power,” explained the deputies [21]. A majority of Russian users bypassed the blocking of messenger with a variety of technical tools. This move seemed to be very contentious since the draft law could not reverse the court’s decision to block Telegram — all court decisions are appealed to higher courts, but not to the Parliament. For perhaps obvious reasons, the draft was not further developed.

However, the Telegram affair unexpectedly ended in June 2020, when RKN published a post on its Web site saying RKN “positively assesses the readiness expressed by the Telegram founder to counter terrorism and extremism. In agreement with the Prosecutor General’s office of the Russian Federation, RKN removes the requirements for restricting access to the Telegram messenger.” [22] It is still unclear how the agreement with Prosecutor General cancels the 2018 court decision, but in several days RKN removed a considerable amount of IP addresses (including Digital Ocean and Microsoft Azure) from the blacklist. There were a lot of hypotheses on why this happened, ranging from the recognition by the authorities of the futility of such a block, to the possible consent of Pavel Durov (Telegram founder) to cooperate with Russian law enforcement. Another reason came from recent personnel replacement in RKN. The new head of the agency decided to rebuild RKN’s reputation and one of its moves in this regard was to lift the ban of messenger [23].

Importantly, Tagansky District Court’s decision on blocking of Telegram covered only its domain and some related resources. However, RKN also blocked individual IP addresses used by the messenger and entire subnets, at the request of the Prosecutor General’s office. It had the right to request blockings in order to fight the spread of extremist materials. Thus, the Prosecutor’s office put forward several such requests in 2014–2015, and initially, they were not related to messenger, but this later turned into a precedent for blocking in other instances. Ultimately, RKN and the Prosecutor General’s office could have an agreement to lift a ban of IP addresses since it is the execution of the request, but whether the decision of the Tagansky District Court would be reviewed or cancelled is unknown.

The Telegram case is a clear loss for the state in its battle for Internet infrastructure. Its elaborated blocking mechanism, tied to Revizor algorithms and the reluctance of ISPs to pay large fines, faced quick reactions from the community. The Telegram case seems to indicate that RKN could not keep up with all technical, and importantly, protocol innovations, while “carpet blocking” of IP addresses only worsened RKN’s reputation. Formally, the messenger was blocked, but it continued to work, so the government had to manage its own double standards. Finally, there were attempts to remove the service from this gray zone by inventing legislative proposals of seemingly difficult implementation. In the end, the government, represented by RKN, made a rollback and strangely announced that the service was now legal.

3. Implementation of the law on “on Sovereign RuNet” (FZ-90)

The government’s efforts to establish control of RuNet infrastructure appeared several years earlier than the FZ-90 law adopted in 2019. Previously, another bill attempted to define components of the RuNet critical infrastructure and its basic elements like IXPs, national top-level domain registries, IP addresses and ASNs [24]. Interestingly, it provided for the creation of a state information system that would contain similar data that RIPE NCC (the regional Internet address registry for Europe and Middle East) was currently providing about routing policies and other databases in the region. That bill aimed to duplicate databases with numbering resources and root servers in case of an external Internet shutdown for Russia. Thus, in case of
emergency, all ISPs should use a state information system to maintain operations for Russian users. The bill was highly criticized for its language by Russian telecom industry representatives and experts and, eventually, was never put on the agenda for the State Duma for consideration and approval (Stadnik, 2018).

A completely new bill appeared by the end of 2018 with the clearly stated aim of protecting RuNet from targeted attacks by strategic enemies and make it stable and secure. Notably, this bill was adopted in a record six months after its first introduction and became FZ-90 on the ‘stable RuNet’. The speed of adoption signified the importance of the government’s desire to create a legal framework to control RuNet infrastructure, and as we will see further — control by infrastructure. We will look closer at particular parts of FZ-90 which were partly implemented, though FZ-90 has already come into force as of 1 November 2019.

FZ-90 consists of a set of amendments to the laws “on Communications” and “on Information” and establishes a broad framework for further steps to be taken by RKN, the Ministry of Digital Development and the Government. Briefly, it provides that:

- ISPs and owners and/or proprietors of: (1) technical communication networks (used for operations of transport/energy and other infrastructures, not connected to the public communication network), (2) Internet exchange points, (3) communication lines crossing the state border and (4) autonomous system numbers (ASN) are the main subjects responsible for the stable operation of RuNet.
- RKN will keep specialized registries for the last three categories.
- All subjects must participate in the regular exercises for testing the stability of RuNet.
- RKN will execute centralized control of communication networks in the event of threats to the stability and security of RuNet, by defining routing policies for ISPs and other subjects and coordinating their connections.
- ISPs are required to ensure the installation in their networks of technical means for countering threats (TMCNT) to ensure stability, security and integrity of RuNet (“black boxes” with deep packet inspection (DPI) functions [Stadnik, 2019b]). These TMCNTs will also serve the purpose of traffic filtering and blocking access to prohibited Internet resources. TMCNTs are provided for free by RKN.
- RKN will supervise the work of the newly established Center for monitoring and control of public communication networks. The Center will take over the traffic routing in case of an emergency.
- The law creates a National Domain Name System (NDNS).

FZ-90 has several blind spots that had to be filled by additional regulatory acts and orders by the Government, Ministry of Digital Development and RKN by 1 November 2019. By the date of enactment, roughly one third of these regulatory acts were ready, though with serious procedural violations. Namely, these acts had to reveal concrete procedural and technical measures for FZ-90 implementation. For example, define a list of threats to RuNet and the principles of centralized traffic control; establish technical parameters and rules for installation and operation of TMCNTs; form procedures for providing information from ISPs, autonomous system number (ASN) owners and other subjects to RKN about their network parameters; figure out the sense of the NDNS for ISPs and users; and several more nuances.

Those acts, that had already been approved, were poorly formulated from a technical standpoint, while others were still under discussion. Our aim here, however, is not to explore the peculiarities of Russian legal language for Internet regulation, but to analyze what is a “sovereign RuNet” from the perspective of control of/by infrastructure.

First of all, there was a need to establish an inventory of all elements of RuNet infrastructure and fill in databases about networks architecture, routing policies, etc. This need was fulfilled by registries run by RKN [26]. Further, there was a need to process the gathered information and, according to the law, execute monitoring and control, which was accomplished by means of a designated Center [27]. However, currently, the Center cannot fulfill its functions because there is no unified rule or systems for network control that could be scaled countrywide. The regulatory act under discussion tries to put this burden on
ISPs [28], a move that overturns the provisions of FZ-90. The Center must be responsible for a RuNet-wide system for public networks control, but without the harmonized data from ISPs (which they are quite reluctant to submit, using legislative loopholes to postpone submissions) it makes no sense. Besides, there were no strict rules for building Internet communication networks, as well as universal standards to execute monitoring and control. Most of the ISPs have decentralized control of their networks, while many of them do it manually through admin scripts. Thus, it is unclear how the Center could fulfill its mission stipulated in FZ-90.

Potentially, the Center could execute control by using TMCNTs, whose purpose is twofold. First, RKN intends to use TMCNTs to route traffic in case of any serious threat to the stability of RuNet. Second, the same means will be used to execute filtering and blocking of Web resources. Here, the idea of Internet sovereignty is clearly manifested — threats are no longer considered only technical, but informational since such is paid to automated traffic filtering to prevent access to prohibited information, which is the main point of the “secure” RuNet. Obviously, TMCNTs imply a sophisticated DPI solution which the government started to test before the FZ-90 adoption. In August 2018, there was a closed competition between DPI vendors where RKN together with FSB and Ministry of Digital Development chose a winner for the nation-wide testing [29]. So far, there are no further actions and associated regulatory acts [30] do not specify further details on TMCNTs. Obviously, the DPI system able to filter all ISP traffic would have high costs and slow speed dramatically. Another problem is its inability to distinguish traffic packets with 100 percent accuracy, thus risking crashing the operations of “right” resources (Stadnik, 2019b). Additional uncertainty is added by the free provision of TMCNTs to all providers given the fact that such systems are enormously expensive. But what is more important, the governmental Decree that approved the rules for centralized control of the public communication network does not refer to TMCNT in the section that defines the ways to determine technical capability to execute instructions for such control [31]. Finally, the government is trying to make the policies on filtering content and blocking access opaquer for other actors — ISPs, business, users. FZ-90 stipulates that ISPs are immune from legal responsibility for future network crashes.

Regular exercises to test the stability of RuNet should be carried out. Currently, they were conducted only once, in December 2019, with procedural violations, without a clear threat model and allegedly in the absence of concrete outcomes (Stadnik, 2019c). The next exercises were scheduled for March and June 2020 but were cancelled due to the pandemic crisis [32].

As for the final part of 90-FZ — the national domain name system — the law does not specify what it is nor what is its purpose. Eventually, RKN’s published Order provided a list of domain name groups that comprise the Russian national domain zone: top-level domains (TLDs) .ru, .рф, .su and other TLDs that are managed by Russian legal entities [33]. It also provided requirements and procedures for NDNS creation, including information it contained and rules for its use [34]. The general sense of the document is to create a ‘state DNS-resolver’ for all RuNet users. It is assumed that NDNS will gather information about TLDs from “open sources” (sic) and provide it to ISPs, ASNs owners and other subjects of 90-FZ to “identify the network address corresponding to the domain name on the Internet” [35]. Conceptually, NDNS is a set of different information systems and equipment. The wording of the Order is as vague as possible, so it is not clear how the NDNS will be filled with necessary information to ensure accurate resolving.

The idea for NDNS is to ensure that RuNet sites will still be accessible from Russia in case of any problems with global DNS, including targeted actions inspired by hostile states. The national domains are in great demand: by the end of 2020 there were more than five million domains registered in .ru, .su, .рф in total. It places the Russian national domain zone at sixth place in world for the most popular domains [36]. But NDNS — in the form in which it is described in the Order — is very incomplete and unlikely to be able to give Russian users full access to Internet resources, as they will either be unavailable or resolved with errors. Furthermore, it is unclear whether its use is mandatory or optional for both providers and users. Currently, there are several ways to send DNS queries — use an ISP DNS server, public DNS servers like Google, or a resolver on a PC. The new NDNS should make DNS queries for national domains going through a “state-controlled resolver”, and it is not clear how this centralized solution will be scaled RuNet-
wide and maintain its availability for providers and users. At the same time, resolving other TLDs is supposed to happen in a traditional manner. Given the complexity of the current architecture of Web resources that use CDNs, third-party scripts and libraries that may be placed in other domain zones than RuNet, the idea of NDNS is highly controversial.

Overall, FZ-90 is the most eloquent example of Russia’s political aspirations to control RuNet by infrastructure. According to the legislators, these measures are necessary to protect RuNet from various external threats, including a complete Internet shutdown, the removal of ccTLDs from the global DNS and manipulation of Russian Internet traffic [37]. But the logic of the proposed measures seems to indicate a complete contradiction, as the centralization of RuNet networks management leads to the creation of a point of potential failure, and deterioration in the quality and speed of Internet connections due to extensive filtering does not de facto provide for a stable and resilient RuNet.

According to Laura DeNardis (2014), DPI is a yet-largely unexplored technique that provides the broadest possibilities for managing and filtering a network [38], and which states would sooner or later try to harness for their purposes. The failure of the Telegram ban is considered to be one of the key factors in the rapid adoption of the 90-FZ law, as it showed the problems related to traditional blocking methods. Since traditional blocking methods did not work well with Telegram protocols, but destroyed associated services, it was decided that filtering at the transport layer could potentially solve this problem. The necessary level of sophistication of DPI equipment to fulfill this task makes it impossible to deploy such technology over the networks of all RuNet providers, but RKN reported on successful DPI bench tests and the imminent choice of a future contractor (Stadnik, 2019b).

The Domain Name System is historically an important control point of the Internet [39], and while the contours of NDNS are not clear so far, the envisaged idea is to ensure the operations of RuNet in the event of its forceful “separation” from the global network and DNS servers, whether it is due to a targeted action by strategic enemies or to random technical problems. Here, too, the scale of the task is overlaid by the complexity of the required infrastructure. How will NDNS be implemented and deployed for providers and users? How will it work with new protocols like DoH? How much will the entire NDNS cost and where will the funds come from? If the government finds an effective way to implement NDNS, it will be a strong temptation to oblige users and providers to use only the ‘state’ DNS at any time, and not just in case of emergency. This scenario opens the perspective of turning RuNet into a very limited and closed segment of the global network.

On the other hand, FZ-90 is the government’s attempt to build and impose its own infrastructure with a centralized structure that is convenient for management, and use it to control ISPs and other participants in RuNet’s infrastructure. However, the process of drafting regulatory acts shows that those ambitious goals manifested by FZ-90 are gradually disappearing from drafts because they are technically impossible to perform today with the current level of available hardware solutions and topology of RuNet.

---

4. Free access to socially significant Internet resources

The final section of this article does not address infrastructure per se; however, further developments may lead to several infrastructural rearrangements. Our literature review showed that the idea of free access to particular Web resources, important for society, was not a globally discussed issue. Only two Russian authors wrote about particular models of “socially important Internet resources”, however, the focus of their article concerned the classification of different resources, with an emphasis on social media and other interactive services.

Russian public discourse on free access appeared in early January 2020. In his speech to the Federal Assembly, President Putin introduced a new project “Affordable Internet”: “The Internet has become a
must-have for people today. Russia is one of few countries in the world which has its own social networks, messengers, e-mail and search engines and other national resources. Given all the things I’ve just mentioned, I suggest that the ‘Affordable Internet’ project be developed and carried out and that free access to socially important domestic Internet services is available across Russia. I repeat that in this case, people will not have to pay for Internet service, for Internet traffic.” While this apparently noble gesture hardly had a counterpart in reality, its core idea was to show how the state is taking care of its citizens by any means.

Later, the speech led to the Presidential Assignment “to provide citizens with free communication services for data transmission and access to the Internet on the territory of the Russian Federation for the use of domestic socially significant Internet services, having determined, in agreement with The Administration of the President, the list of such services and the procedure for providing these services.”

Additionally, the COVID-19 crisis also hit the country, making the Internet an even more vital infrastructure for people’s daily lives in quarantine and remote work to maintain the economy. Thus, the President established another Assignment to “provide citizens with free access to Russian Internet resources, including for obtaining public services, distance learning, and remote ordering of medicines.”

The Ministry of Digital Development promised to prepare free access to all government Web sites by 1 March 2020, but it failed to obtain approval for the necessary corresponding decree — the draft not only aimed to provide access to the government sites but to “socially significant” commercial resources. The Federal Antimonopoly Service and the Ministry of Economic Development criticized the document, while ISPs complained about potentially significant financial losses.

Meanwhile, the Ministry of Digital Development launched an experiment to test free access to the ‘socially significant’ Web sites, which covered the largest ISPs in the country and included only fixed Internet access in households (not mobile). It started in April 2020 and tested around 400 Web sites that formed the first list of socially significant Web resources. Order № 148 specifies that the Web sites were chosen by demand based on publicly available traffic data. The list is divided by categories: social networks and communities; e-mail and cloud services, messengers; weather; search engines; online media and news aggregators; maps and navigation; auto; literature, art and culture; education; health; science; sports; government agencies and services; jobs; finance; delivery services; marketplaces; social and volunteer services. The experiment had some limitations: for example, Web sites should not include heavy content with video and images, and transmission speed has to be decreased too. Thus, online media had to prepare lite versions of their sites. In July, the Ministry continued the experiment until December 2020 and additionally requested participating ISPs to keep track of results: static and dynamic IP addresses of Web sites, availability of video content, average number of unique users per day, session duration, access speed and volume of Internet traffic.

Interestingly, the initial list of socially significant resources was revised: several “unpopular” ones were removed, while categorization was rearranged completely to include communication services; services demanded in daily life and emergency; aggregators of socially significant information; auto, national culture and traditions; continuous education and professional development; sites of state authorities and key services for feedback from the population; social services (job aggregators); delivery; marketplaces; volunteering.

In parallel, the Government published a draft law to amend the law on Communications (FZ-126) with provisions about free access to Internet resources. The draft law requests the creation of a register of socially significant Internet resources; access to them will be provided for free only to authorized Russian citizens. Criteria for Internet resources to be included in the register must be developed by a special commission. The draft does not take into account the ongoing experiment, it does not restrict video content for Web sites and require ISPs to provide the same quality of service as for paid traffic. Thus, ISPs revenue can be significantly reduced. Given that the experiment was prolonged until the end of the year, the
Control by infrastructure: Political ambitions meet technical implementations in RuNet

Government may rework the draft in 2021.

Interim results of the experiment showed that more than one million unique users used free access during the experiment [50]. The problem is that the majority of users kept paying for Internet access and may not have noticed that traffic to particular resources was not tariffed. The proposed amendments stipulate that free access must be provided, no matter whether the customer paid for the services under the contract or not. If there are enough free Web sites, some will stop paying at all. How will ISPs continue to operate in the face of falling revenues? The burden to replace losses will be likely placed on those customers who continue to pay for full access.

Finally, in August 2020, the Ministry of Digital Development announced its work on another draft law, amending FZ-126 to determine the procedure for creating, maintaining, and using a list of socially significant sites. Since the draft has not been officially published for public discussion, the media uncovered criteria for Web sites to qualify as such [51]:

- must have a domain in .ru, .рф, .su, .дети;
- must be created and located on the territory of Russia;
- must be owned by a Russian legal entity;
- the share of foreign capital is no more than 20 percent;
- at least 50 percent of the audience must have access to the resource from the territory of Russia;
- must not contain video, audio, or advertising content;
- must consist primarily of Russian content;
- the main language must be Russian or one of the official languages of the regions;
- it is forbidden to publish paid services or links to them (except for the state or municipal ones);
- must be included in the Register of information distribution organizers;
- must be available at a single static IP address.

This list of criteria has technical and formal parameters, but it does not provide details about social significance. The ultimate aim might be to gather the most popular RuNet sites while neglecting resources on other TLDs. The last condition allows us to speak about the potential creation of a ‘white list’ of Internet resources. Previously, a similar idea has been discussed and found some support. The national program “Digital economy” signed by Prime Minister Medvedev in summer 2017 contains a provision to prototype a national system of Internet traffic filtering for children using information resources by 2019 (National Program, 2017). The League of Safe Internet (a Government NGO organized in 2011 to lobby for Internet filtering for the sake of child protection) proposed two possible options to enforce this provision: traffic filtering can only be enforced in educational institutions, or it can be spread to all RuNet users, which amounts to the introduction of “white lists” for parental control. The League of Safe Internet has its own “white list” of sites, which contains more than one million resources [52]. The current situation might provide the government with an opportunity to implement this provision; however, given the plans of FZ-90 and TMCTs, the government might take the path of least resistance and filter traffic according to the white list, not the black, thus limiting Russian users’ access to Internet resources significantly.

Conclusions

This article has examined four attempts by Russian institutions to exercise control by Internet infrastructure. Taken as a whole, these cases seem to indicate that the Russian government learns from its mistakes — and, at the same time, it does not. There is an understanding that content filtering and blocking access to Web resources by existing means do not work as much as the government would wish. The Revizor case showed that the automatization of ISPs’ checks leads to extensive filtering and leaves open several vulnerabilities that can be used against the system itself. On the other hand, as the Telegram case indicated, the existing framework for blocking and filtering causes considerable network effects. Other Web resources may be
affected because of the extensive blocking of a particular service due to the complexity of the Internet transport layer. This, in turn, may do a lot of harm to other sensitive sectors of a country’s digital economy.

The new law (FZ-90) and supporting regulations are aimed to exercise a more sophisticated form of Internet traffic control, using TMCTs and NDNS. Given the speed of their adoption, from a technical standpoint, these regulations either introduce excessive regulation for ISPs or lack clarity and logic in connection to other laws regulating telecommunications in Russia.

At the same time, Russia’s ultimate goal is not to control infrastructure per se; given the Russian understanding of information sovereignty, Russia’s reach on infrastructure is rather a consequence of plans to control content and information in RuNet. On the other hand, we can see a trend towards the complexity of the task being replaced by formal requirements to keep dozens of registries and information systems filled with sensitive information from ISPs. The reasons for that are simple: the government faced a big challenge with FZ-90 implementation, as the costs assumed for implementing the measures were not sufficient with what needed to be achieved. Either there is too much to accomplish and too many actors to involve in the process, or at some point, it no longer becomes necessary — as with the Telegram case.

The last case we examined — free Internet access to socially significant Web sites — seems to stand out from this article’s main narrative, since it was voiced by the President only in early 2020 and focuses on Web content. If this idea is further developed after the ongoing experiment, it may have serious consequences for the RuNet landscape due to its attractiveness as an easy way to define a nation-wide white list of Web resources.

Overall, the discussed cases add a new layer of meaning to the understanding of Internet governance — in Russia, infrastructure control is a way to reach more efficient content and information flows control. The improvement of data transmission technologies, together with huge amounts of information, makes this task difficult for both legislative regulation and technical implementation. However, the considered cases can be taken into account in neighboring countries, especially those where the Internet topology is more centralized. Comparative study of legislation and practice in such countries as Belarus, Kazakhstan, Kyrgyzstan, Azerbaijan, Uzbekistan and Tajikistan can become a new promising area of research in the ‘control by infrastructure’ field.

About the author
Ilona Stadnik is an assistant professor at Saint-Petersburg State University, Russia.
E-mail: i [dot] stadnik [at] spbu [dot] ru

Notes


6. From a methodological standpoint, I follow several Telegram channels that serve the telecom community as a tool to share legislative novelties, and I infer elements of the community’s attitude towards them, e.g.: Эшер-ИI at https://t.me/usher2; ЗаТелеком at https://t.me/zatelecom; ОрдерКом at https://t.me/ordercomru.

7. Until March 2017, ISPs received a warning or a fine amounting 30 thousand rubles for non-execution of blockings. Then the fines were raised up to 50–100 thousand rubles (18-FZ, 22.02.2017).


15. “Court case file № 02-1779/2018,” Tagansky District Court of Moscow, at https://www.mosgorsud.ru/rs/taganskij/services/cases/civil/details/2cc72aea-39e7-4f8e-adc9-37d170966efa

16. “Yarovaya Package” — a set of amendments to anti-terrorism laws. In addition to requiring all service providers to store the content of voice calls, data, images and text messages for six months, and the
metadata of communications for three years, it requires messengers and social networks that use encrypted communication to permit the FSB to access and read their encrypted messages on request.

17. “During 15 hours of operation of the ROCIT hotline, 2,250 complaints about IP address blocking were received,” ROCIT, at https://rocit.ru/news/2250-complaints-about-blocking.


Control by infrastructure: Political ambitions meet technical implementations in RuNet


34. Roskomnadzor, 2019. “Roskomnadzor order of July 31, 2019 № 229 ‘On approval of The regulations on the national domain name system, requirements for it, the procedure for its creation, including the formation of information contained in it, as well as the rules for its use, including the conditions and procedure for providing access to information’,” at http://www.garant.ru/hotlaw/federal/1303349/, accessed 20 March 2021.

35. Roskomnadzor order of July 31, 2019 № 229, article 3.


44. Ministry of Digital Development, 2020. “Order of the Ministry of Communications of the Russian Federation № 148 ‘On conducting an experiment on providing citizens with free communication services for data transmission and providing access to the information and telecommunications network ‘Internet’ on


51. Ibid.

52. V. Zykov, 2017. “Russia will have a national Internet filtering system. For Russians will be prepared ‘white lists’ of trusted sites,” Izvestiya (2 August), at https://iz.ru/627080/nacionalnaia-sistema-filtratcii-internet-trafika-poiavitsia-v-rossii, accessed 20 March 2021.

References


Control by infrastructure: Political ambitions meet technical implementations in RuNet


**Russian bills, laws, regulations and other official recordings**


Ministry of Digital Development, 2020. “Reporting form for participants of the experiment conducted in
Control by infrastructure: Political ambitions meet technical implementations in RuNet


accordance with the procedure established by FZ-149 [Rekomendatsii po ograniicheniyu dostupa u informatiki, rasprostranyayemoy posredstvom seti Internet s pomoshchью ustanovlennym FZ-149],” at https://rkn.gov.ru/docs/11111_Rekomendacii_15.pdf, accessed 20 March 2021.


Media and other sources


M. Kolomychenko, 2018. “Russia tests new Telegram blocking technology [Rossiya testiruet novuyu teknologiyu blokirovki Telegram],” Reuters (30 August), at https://www.reuters.com/article/orutp-russia-
Control by infrastructure: Political ambitions meet technical implementations in RuNet


Y. Stepanova, Y. Tishina and D. Shestoperov, 2020. “The social Internet is frozen. Free access to significant sites remained without a resolution. [Sotsial’niy internet zavis. Besplatniy dostup k znachimym saytam ostalsya bez postanovleniya],” Kommersant (2 March), at


---

**Editorial history**

Received 2 April 2021; accepted 7 April 2021.

---

Copyright © 2021, Ilona Stadnik. All Rights Reserved.

Control by infrastructure: Political ambitions meet technical implementations in RuNet by Ilona Stadnik.

*First Monday*, volume 26, number 5 (May 2021).

doi: https://dx.doi.org/10.5210/fm.v26i5.11693