Surveillance and Censorship of Internet Infrastructures: Markets, Regulation, and Black Boxes

Ksenia Ermoshina, Benjamin Loveluck, Francesca Musiani

2 SURVEILLANCE AND CENSORSHIP OF INTERNET INFRASTRUCTURES: MARKETS, REGULATION, AND BLACK BOXES

Ksenia Ermoshina, Benjamin Loveluck, and Francesca Musiani

From the early 2010s, the development of the Russian internet has characteristically featured strong state interventionism, in terms both of legal instruments and of technical infrastructure. In the context of the Sovereign Runet doctrine, an important part of the authorities' strategy has been to encourage the development of Russian-made technical solutions for censoring and intercepting internet traffic. This has created a thriving market for Russian providers of software and hardware solutions for monitoring and filtering traffic. This chapter offers an analysis of this industry and its effects on internet service providers (ISPs). We look at the controversies surrounding the various technological assemblages that actors of the Russian internet must adopt to comply with current regulations, which are costly and complex to implement and raise many ethical and political concerns.

We first present our approach, which is rooted both in political economy and in the sociology of technology and innovation, and the mixed methods that have been mobilized to collect empirical data. We then draw a distinction between two strategies of information control: online surveillance ("lawful interception") on the one hand and censorship ("traffic filtering") on the other. We thus present two types of devices that were central to the 2016 Yarovaya Law and discuss their influence on the ISP market: surveillance systems called SORM (system for operative investigative activities) that establish a direct link with intelligence agencies and traffic-filtering solutions used to block access to websites blacklisted by the federal media and telecommunications regulatory agency Roskomnadzor (RKN).

We then discuss the additional step that was taken with the 2019 Sovereign Internet law, as all operators must now install a new type of device called a TSPU (technical means for countering threats) on their networks. This includes a deep packet inspection (DPI) filter that can analyze data packets, throttle or block access to certain resources, and, as the 2019 law prescribes, limit data traffic within Russia. In 2021, for example, a DPI filter was used to slow down Twitter and to block the voting assistance application that the opposition had offered during the elections. This filtering can be activated remotely, does not require network operators to cooperate, and entirely evades citizen surveillance. This new constraint on ISPs represented a decisive tightening of the authorities' grip on digital infrastructures.

In this chapter, we also analyze the effects of these measures on the balance of the Russian internet market and on its relations with foreign networks and services, and we assess the possibilities of circumventing this system through an array of legal and technical ruses. Finally, we analyze the impact of Russia's invasion of Ukraine on these information-control technologies, showing how international sanctions have exposed the role of major international manufacturers in the techno-legal project of the Sovereign Runet. With the departure of Nokia, IBM, Intel, and Cisco from the Russian telecom market, what is left of these surveillance and censorship boxes?

A SOCIOECONOMIC STUDY OF THE RUSSIAN INTERNET'S "BLACK BOXES"

With over 6,326 licenses issued in 2020 (and 3,461 to 3,940 of them active[1]), the Russian ISP industry showed distinctly strong competition, low prices, and good connectivity quality until the late 2010s, as well as a relatively decentralized topography and a large number of transnational peering agreements. Many Russian ISPs started as "local networks" (*domovaya set'*) and formed active professional communities, resulting in a large number of professional associations, conferences, and forums. Since the mid-2010s, however, the ISP market has undergone increasing legal and infrastructural centralization. From 2017 to 2020,[2] the number of licenses issued for "telematics services" and "data transfer services" decreased (from

9,395 to 8,000 and from 7,035 to 6,326, respectively[3]). Additionally, government initiatives to create a "self-sustaining Russian internet" included the introduction of a "central control point." This involves, among other things, a mandatory register of all transnational cables and peering points that, until then, had not been properly documented by the various government bodies concerned.

In this chapter we discuss surveillance and censorship of the Russian internet from the perspective of their political economy, which sheds light on their inherent logics and workings. In the case of Russia, these aspects of state power have recently been asserted increasingly and in very explicit terms. We show how the "black boxes" imposed on private actors at the level of internet infrastructure through regulatory measures are embedded in (and contribute to) a set of social, economic, and political relations. In doing so, we deconstruct the oversimplified image of direct state control through technology. This affords an understanding of a key aspect of the "global struggle for internet governance" (DeNardis 2014) and of how internet infrastructures themselves can be leveraged to support power relations.

This "turn to infrastructure" in internet governance (Musiani et al. 2016) also presents a more complex picture of the articulation between law and code (Lessig 2006) and between political regimes and their translation into socio-technical and economic practices. The relationship between legal procedures and their technical implementation is a central aspect of internet governance: the behavior of internet users is regulated by the inscription of norms, affordances, and constraints in both technical infrastructures and laws, and policymakers increasingly exploit them to achieve (geo-)political goals (Winseck 2017). This is particularly true in Russia, where law and code interact in a very specific way. Technical solutions often lag behind regulation, as the law seeks to gain control over the infrastructure (see, for example, Ermoshina and Musiani 2017). Moreover, this constant increase of regulations has led to criticism from the ISP community, where some have called it a "security theatre" (Schneier 2003), in which political rhetoric primarily serves underlying commercial opportunities. With import substitution (the preference for domestic companies, put in place long before the full-scale war with Ukraine) as a rule, information control solutions must

be "made in Russia." In this context, Russian internet regulation has created a fully fledged market for censorship and surveillance, shaping competition between different domestic suppliers of infrastructure components and affecting the operations and strategies of ISPs.

Studying these markets allows us to closely analyze the relationship between standardization and competition. Although Russian internet governance is increasingly presented as a matter of national sovereignty, the Russian state remains slow to produce and certify technical surveillance and censorship solutions. Moreover, the context of Russia's invasion of Ukraine in 2022 and the international sanctions adopted in retaliation shed light on the Russian surveillance and censorship industry's reliance on foreign components, infrastructure, and know-how. The results are techno-legal loopholes and gray areas that create both uncertainties and opportunities. Our study of the middlebox market also highlights resistance practices that often develop in response to specific filtering and surveillance techniques and allows us to track and understand the politicization of web professionals.

Our ethnographic methods allow for a detailed examination of the "plugs, settings, sizes and other profoundly mundane aspects of cyberspace" (Star 1999, 379) regarding the three technical solutions discussed in this chapter. These technologies can be seen as "black boxes" (Callon, 2013) in several respects. They are presumed to be technically opaque and serve filtering and surveillance purposes, which places them in the realm of state and commercial secrecy. They do not always resemble clearly identifiable physical boxes (although they sometimes do) but consist, rather, of a multitude of software solutions, distributed technical objects, and techno-legal adjustments that complement existing physical infrastructures. Lastly, they are a focus of controversies related to surveillance and censorship in Russia, generating ambiguities, interpretations, disputes, resistance, and negotiations.

Our study of these activities, which are both specialized and sometimes shrouded in secrecy, presented a number of challenges. These were partly mitigated by adopting a "mixed methods" approach and collecting three main types of material from 2017 to 2019 and again in 2022. First, we conducted fifteen interviews with ISP staff (mainly from small and medium-sized companies with portfolios of five thousand to a hundred thousand

clients), IT experts, internet lawyers, vendors of filtering and DPI equipment, anticensorship and antisurveillance activists, and engineers working at the internet exchange point (IXP) in St. Petersburg. We then conducted five interviews in the summer and autumn of 2022 to update our survey. The interviewees all asked to remain anonymous.

The study was complemented by a web-ethnography and analysis of ISP forums and chatrooms, which were selected and observed throughout the study period. We also conducted an analysis of technical documentation and communication materials produced by vendors of surveillance and censorship solutions: websites, commercial presentations, and materials from specialized professional conferences. Finally, we measured the extent of censorship in 2018 (in partnership with Citizen Lab; see also Valentovich and Ermoshina 2019), to analyze the technical implementation of censorship on the Runet. An analysis using the OONI Explorer tool,[4] as well as analysis of Border Gateway Protocol (BGP) routing data and other traffic metrics, was conducted more recently, in 2022, to assess the impacts of Russia's invasion of Ukraine on Runet connectivity and the accessibility of digital resources.

SORM AND THE SURVEILLANCE MARKET: CONSTRAINTS AND BRICOLAGE

SORM is a system for the lawful interception of telecommunications. It is a distributed object consisting of switches, servers, data storage volumes, extractors, remote control terminals and software. While it must be installed at the operator's expense, it is directly controlled by the Federal Security Service (FSB) and accessed on request by other agencies and police services (tax, customs, border police, etc.). SORM-1 was set up in 1995 for phone tapping and surveillance. It has since evolved into the internet-ready SORM-2 in 1998, and SORM-3 in 2014, which included specifications for the collection of metadata (such as time and date, location, sender, and recipients of messages) and multimedia files.

The latest iteration was defined by the "Yarovaya" laws 374-FZ 4 and 375-FZ passed in 2016, raising a wave of criticism from digital rights and freedoms organizations[5]. After almost two years of discussions due to the

technical complexity of the law, and due to abundant criticism from the ISP community, the regulation was relaxed to some extent. According to the amendment of April 12, 2018, telecom providers must now store metadata for three years and the content of all voice calls, data, images, and text messages for thirty days (instead of the original ninety days), with a 15 percent increase in storage time each year. However, this 15 percent increase requirement has already been postponed twice—first in 2020 in the context of the pandemic and then in March 2022, following international sanctions, revealing both the difficulty of implementing this measure and the inability of the Russian market to propose technological solutions that would allow it to meet the regulators' demands by its own means.[6]

Data stored under the provisions of the Yarovaya Law must be made available to the authorities on request and can be obtained without a warrant or court order. Moreover, online services using encrypted data for messaging, email, or social media must allow the FSB uncoded access to these communications. The new regulation has been strongly criticized, not only because of the extension of the scope of surveillance but also because of the high costs of storing the data.[7] To comply with these regulations, ISPs have long preferred to tinker with existing equipment, as a representative of NORSI-TRANS, a market leader in SORM solutions, plainly stated at the KROS 8 vendor conference in May 2017: "Storing all Internet traffic for six months is not compatible with the economic realities of our country. The only practical solution for SORM is to use the existing equipment, with minimal extensions and a clear technical solution, with no cheating."[8]

Moreover, the SORM certification process is long and complex, as it involves a multitude of institutional actors, each in charge of certifying one or several of the system's components. These have to be tested according to a methodology that must first be validated by the FSB and the Ministry of Communications. The FSB then tests the installation using a simulator, and only then can the three-month certification process begin. In the absence of standardized, state-certified solutions, ISPs simply use existing infrastructures in anticipation of having to invest substantially again when the solutions are released.[9] Furthermore, legal responsibilities for data leakage or

misconfigurations are not clearly defined, and in fact, misconfigurations of SORM boxes are frequent, putting users' personal data at risk. The situation is particularly problematic because of the sensitive nature of the data, the variety of parties involved, and the lack of transparency in the process.

The requirements are tailored to ISPs' size and budget. Large ISPs are required to have SORMs, but smaller ones do not always install SORM boxes and instead respond to FSB requests on an ad hoc basis: "When necessary, the FSB calls or emails us and asks us to tcpdump the traffic for an IP address and share it via ftp."[10] Another long-used strategy, called "outSORMing," involves larger operators renting part of their SORM facilities. This strategy was standardized in 2022 and is now officially recommended by regulators.[11]

The period of relative flexibility allowing ISPs to avoid installing SORMs ended in January 2022, when the new bill, 333–34, on the Russian Tax Code[12] was proposed, introducing stricter penalties for noncompliance with SORM obligations and significantly increasing the cost of a license (which was multiplied by 183!). The package of documents that came with this bill included a study that not only revealed the figures of noncompliance with SORM obligations but also showed that the regulator was very aware of the tricks and circumvention techniques ISPs had used until then, as documented in our previous study (including closing down the company and reopening it with a new license [see Ermoshina et al. 2021]).

Table 2.1
Number of violations and fines per year, 2020–2022

Year	Number of violations	Fine
2020	954	243 fines (3 to 40,000 roubles, total sum 4,000,000 roubles)
2021	1,096	400 fines (3 to 100,000 roubles, total sum of 15,000,000 roubles)
2022 (1st half)	404	95 fines (3 to 100,000 roubles, total sum 3,000,000 roubles)

Source: https://sozd.duma.gov.ru/bill/254008-8 (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our Note on the Availability of Sources.")

CENSORSHIP PRACTICES AND TECHNOLOGIES

With regard to censorship, laws introducing the blocking of web content have been in place since 2012, when the RKN introduced a blacklist of banned web pages, and ISPs were co-opted under Russian jurisdiction to implement blocking (Sivetc 2020). The regulation was introduced in the wake of the 2011–2012 protests against election irregularities, which led to a reshaping of the digital media landscape. Its full implications became apparent, however, during the 2014 war in Ukraine, which became a testing ground for the Russian authorities' tightening of information control, including on annexed territories.

Our interviews show that as early as 2008–2009, ISPs received ad hoc instructions to block access to specific websites (gambling, pornography, drug dealing). The introduction of a centralized blacklist made it more difficult for ISPs to ignore such instructions and defend themselves in court. However, the precise requirements for blocking methods were not published until March 2018, with Law 149-FZ, Article 10, which defined the technical parameters of standardized "blocking pages" and a detailed set of technical recommendations for content filtering.

Freedom of expression advocates have severely criticized the blacklisting principle, as the "illegal" categories of content are vaguely defined, which leads to arbitrary decisions. In addition, the lack of judicial oversight facilitates the blacklisting of opposition websites on political grounds. These measures initially triggered a series of inventive initiatives that exploited the mechanism of the domain name system as a tool of protest, a famous example of which is the controversy surrounding Maksim Moshkow's online library, which was blocked in 2012. Moshkow, a Russian internet pioneer, had spearheaded major internet media projects (such as Gazeta.ru). Lib.ru, also known as the Maksim Moshkow Library, began operating in November 1994 and had become the largest and most comprehensive Russian-language electronic library.

Moshkow's response to the blocking of his library was to exploit a vulnerability in the web censorship mechanism, which made it possible to block the Ministry of Justice's main website. Since many ISPs automatically blocked all IP addresses from the "A-Record"[13] of a blacklisted Domain Name System

(DNS), Moshkow simply modified his website's A-Record to include the Ministry of Justice's IP address.[14] Following the same principle, in 2017, a number of DNS-based guerrilla attacks took place, blocking government bank and service sites and several DNS root servers. Activists used the RKN blacklist as a starting point: they bought some orphan domain names whose subscription had expired but were still listed and proceeded to modify their A-Records. Exploiting the same vulnerability, on May 6, 2018, developer and hacker Leonid Evdokimov wrote "Digital Resistance" in Morse code on the graphics of blocked ISPs (figure 2.1).

These actions have had consequences on the regulation and implementation of censorship and on the way blacklists are maintained. Before Evdokimov's action, in April 2018, the blacklist had 5,136 orphaned domain names that could be used to replicate a DNS attack, whereas by May 13, 2018 it had only 204 such domain names. Some of our respondents were critical of this side effect, arguing that these activists had ultimately helped RKN improve its management of internet censorship.

Despite the criticism of censorship by civil society actors and by some ISPs, Russian operators still have to implement these regulatory measures, which affect their business and, to some extent, challenge the values of openness that they might defend. Like SORM, solutions for blocking sites are hybrid objects and can take different forms: ISP homemade scripts, hardware solutions, cloud-based solutions, and DPI-type software. For a long time, ISPs had a choice of blocking options and methods. As the director of

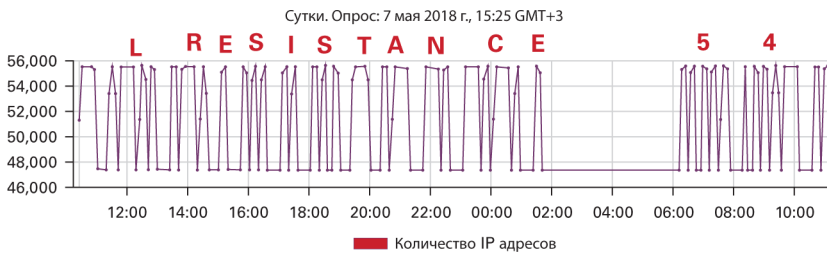


Figure 2.1

L. Evdokimov's Morse code message. *Source:* Independent host, expert, and activist for the free RuNet Phil Kulin's website (https://usher2.club/articles/msg-digitalresistance/).[15] The image is licensed under CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/).

SkyDNS, a provider of traffic filtering solutions, pointed out, "There was a kind of technology vacuum—it was 'block as you like'. RKN couldn't advise ISPs on solutions for fear of falling foul of antitrust laws. But very soon there were several complaints from administrators of websites that had been blocked by mistake. . . . So they started to impose URL blocking. ISPs used to write their scripts themselves, but that's not very common anymore, because they risk being penalized."[16] Manual blocking became too difficult as the blacklist grew longer. In addition, ISPs often criticized this blocking list for its multiple inaccuracies and messy and misleading structure. An informal survey on an ISP forum[17] shows that the most-used methods were IP blocking and DPI.

Some ISPs sought to avoid large investments in filtering solutions. As a result, they did not block blacklisted sites consistently across different networks. In December 2016, to better control the blacklist's uniform application, RKN introduced another technical solution: the automatic system Revizor (AS Revizor).[18] Since the addition of Revizor, and due to its numerous malfunctions, the distribution of accountability for blocking errors has often proved controversial and problematic. As the president of the Internet Protection Society (OZI), Mikhail Klimarev, explains, "Suppose I'm a small ISP and I buy pre-filtered traffic from Rostelecom. I install Revizor, but something is not blocked. Who should pay the fine? Rostelecom or me? Rostelecom will say that I have configured the equipment incorrectly at the local level."[19] In this context of legal uncertainty and lack of specifications, a market for website-blocking solutions has cropped up. Unlike SORM manufacturers, which are mainly state contractors, most filtering equipment manufacturers (such as SkyDNS, Ruspromsoft, and Carbonsoft) previously offered commercial solutions for billing or parental control, although some companies (such as CyberFilter) were created specifically to meet RKN's requirements.

Our interviews with ISP staff and our analysis of forums allowed us to identify at least fourteen filtering solutions. For a long time, ISPs were confused by the market, which had two clear leaders, Carbon Reductor and SKAT. However, with the aim of stabilizing and standardizing blocking procedures, and supposedly as requested by ISPs, RKN conducted a massive trial of thirteen solutions (August 2017–March 2018), in which they benchmarked a series of parameters—for example, the proportion of "extremist"

and "other content" that had not been blocked. RKN then produced a ranking, the results of which were published on its website.[20]

Overall, the Russian censorship market shows a variety of trends and strategies to deal with regulators' requirements. Providers of filtering solutions compete fiercely to offer cheaper or more effective products, while large ISPs sometimes avoid blocking everything to attract more customers. Noncompliance can thus be presented as a commercial argument: manufacturers integrate features to simultaneously avoid being fined for having failed to block websites and minimize the impact of censorship on service quality. For example, when Telegram was blocked in 2018, collateral effects included blocks on Amazon, Google, and other popular websites. Carbon Reductor then offered ISPs a package that allowed them to provide their customers with access to platforms such as YouTube or Gmail without being detected by Revizor and fined by RKN.

Generally speaking, between 2012 and the end of 2018, censorship in Russia was not homogeneous, and ISPs developed ways to avoid complying with it, for both economic and technical reasons. Our interviews and analysis of the forums show that ISPs share a form of care for their networks and despise external interventions in their facilities, especially when they are imposed by the regulators, whom they consider incompetent. As a result, they have developed numerous circumvention strategies and "network tricks," which we have explored in more detail elsewhere (Ermoshina and Musiani 2021). One of these is the practice of selective censorship, which aims to deceive Revizor. The director of SkyDNS explained in an interview with us: "Some operators only apply censorship on a separate subnet they call a 'sandbox', where they install Revizor. And for their end-users, they fashion another network where there is little censorship, if any at all. For their part, network administrators or hosting services engage in technical tricks; for example, when Revizor IP addresses are identified, a blocking page is sent in response." Other strategies involve legal resistance. The OrderCom organization supports ISPs that oppose RKN-mandated decisions and fines, with some success: in 2016, 15 percent of decisions were overturned. ISPs also challenge what they consider to be errors resulting from the use of Revizor, providing certified true copies of blocked pages. However, out of

33,533 court decisions issued from 2012 to 2017, only forty-six cases were successfully overturned[21].

TSPUS AND THE CENTRALIZATION OF CONTROL

After a period of semifreedom for ISPs and Runet users, a new legal and technical apparatus was introduced in 2019 with the Runet Stability law (known to the general public as the Sovereign Runet law). ISPs and civil society actors were initially very skeptical of this law, as they doubted the government's technological ability to implement it effectively, and its opacity and complexity made it tricky to interpret. The law itself comprises around thirty regulatory acts that define "threats to the stability of the internet" or assign new responsibilities to Roskomnadzor, such as monitoring traffic exchange points (IXPs) or establishing an exhaustive list of cross-border cables (which had still not been completed at the end of 2022).

Analyzing the press reports and specialized Telegram channels, we found that experts involved in the "Free Runet" struggle perceived this law as a "regulator's dream" and saw a discrepancy between technological reality and legislative imagination: "The regulator sees Net regulation as some kind of central control point, a big screen in a bunker and a lot of people with headphones. They really think that's what it looks like. Its like watching a demiurge drawing their childhood dreams."[22] Other experts have linked the Sovereignty Law to the ineffective attempts to block Telegram in 2018 or to the 2016 Yarovaya Law, which was amended and largely watered down due to the lack of technical means to implement it. The principle of sovereignty "through infrastructure," according to which any information control instrument should be made in Russia came back to bite its promoters, as Russia did not produce technological solutions capable of complying with its own injunctions.

Despite its critics and sceptics, the 2019 law has nevertheless truly changed the ways in which the Runet is controlled, on several levels. First, RKN's perimeter of control over communication infrastructure has been radically expanded. In particular, the obligation to provide client information (including traffic volume, autonomous system numbers, owner contact

details, etc.) has been extended to internet exchange points (IXPs), which were still excluded from these provisions in November 2019 when we spoke to a representative of Piter IX, the St. Petersburg IXP. Since 2020, RKN has started to list operators with cross-border infrastructure.

As mentioned above, about fifteen companies offered traffic censorship and filtering solutions, seven of which had been tested and certified by RKN. ISPs were able to circumvent their obligations, as they were responsible for choosing, implementing, and maintaining their filtering and monitoring solutions. A range of technical and legal tricks allowed them to minimize control over networks and thus to defend a certain vision of the "free" Runet. Traffic measurements carried out in February to April 2018 using the OONI Probe software (developed by the Open Observatory of Network Interference) confirmed that ISPs enjoyed this relative freedom. With more than 200,000 measurements conducted using local testers, we provided evidence of inconsistencies in the blocking of websites on the official RKN blacklist (Valentovich and Ermoshina 2019).

However, the 2019 law recommends installing a single solution called TSPU (technical means for countering threats), which combines hardware with DPI-type software. While the DPI solutions are manufactured in Russia (mainly by RDP.ru, owned by Rostelecom, or by Carbonsoft), the hardware part of the TSPU is not entirely Russian. Commonly used solutions are produced by Intel, Huawei, or Supermicro, and network cards are manufactured by Mellanox or Intel. The TSPU is not a single box; it is an assemblage of devices and software solutions recommended by RKN (figure 2.2). An example of a TSPU assemblage could be an EcoDPI filter manufactured by RDP, a Huawei server, an Eltex commutator switch, a Silicom switch, a Fiber Trade optical module, and "Kontinent" encryption software. To this day, there is no certification for the assembly work.

TSPUs are installed by FSB- and RKN-authorized agents and are usually located in locked cages, so ISPs have limited access to them. Their purchase and installation are paid for by the state, but maintenance remains at the ISP's expense. The law provides for a fine for violations of TSPUs' installation, operation, and updating rules of up to 500,000 roubles (about 6,400 euros). In the event of a breakdown, the ISP is held responsible and

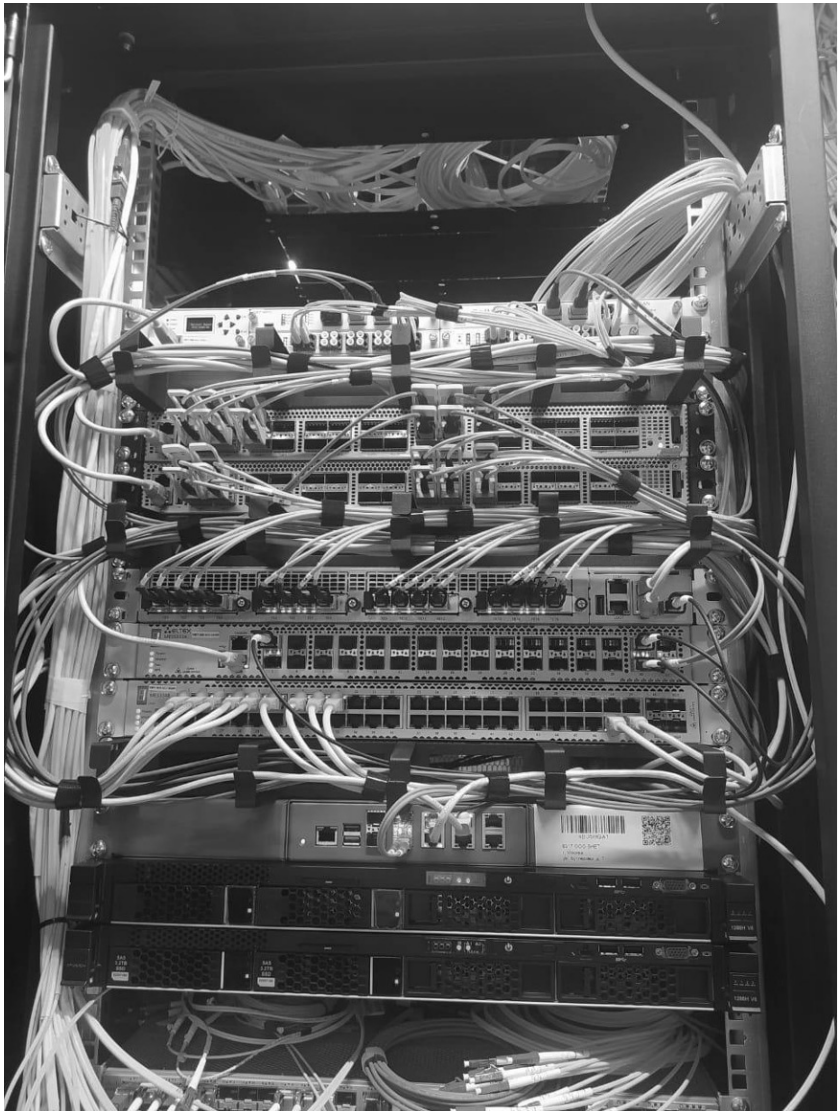


Figure 2.2
TSPU installation for 40Gb/sec. *Source:* Personal archive of Mikhail Klimarev.

penalized—even if it is due to RKN's intervention. This limits ISPs' room to maneuver and curtails their ability to avoid filtering traffic.

TSPUs can be used to block certain VPNs (ExpressVPN, RedShield, NordVPN, etc.) and to slow down certain services, which Twitter experienced in 2021. In autumn 2021, they were used for massive extrajudicial blockings, which included the online shopping service Avito.ru, the servers of the game World of Tanks, GoogleDocs, Apple Music, Recaptcha, Telegra.ph, and so on. These services were blocked by the TSPU during the parliamentary elections to stop the distribution of Aleksei Navalny's SmartVote application, which called for citizens to vote for opposition candidates. These services were not included in the register of blocked sites and were therefore blocked without a court decision. Moreover, the introduction of the TSPU has affected the transparency of censorship. While the blacklist allows for traceability and some degree of citizen monitoring of censorship and its application (especially by the NGO Roskomsvoboda), there is to date no list of sites blocked by TSPUs.[23]

According to the Main Radio Frequency Centre director, Sergey Tyomniy, small providers with speeds of up to 10 Gbit/second are not required by law to install a TSPU.[24] However, while the large number of small providers with relatively low bandwidth is a distinctive feature of the Russian ISP market, their combined traffic accounts for only 5 percent of all traffic in the country.[25] In their case, the onus falls on operators upstream from them to filter contents. Yet even some large operators, such as MTS, consider TSPUs to be a "threat to the connectivity, stability and proper functioning of the Runet."[26] ISPs are thus developing new stratagems, especially at the legal level. During RKN's forced census of ISPs in December 2021, Dmitry Galushko, a lawyer who specializes in defending ISPs, advised on his Telegram channel that bandwidth should be declared at less than 10 Gbit/second.[27] As for technological resistance, lately it has shifted to the development of traffic obfuscation protocols (Shadowsocks, OBFS4, Cloak) and new generations of "multiprotocol" VPNs that mask traffic (AmnesiaVPN and Roskomsvoboda's CensorTracker).

Another workaround proposed by ISPs is to create "internet consumer cooperatives" to avoid the need to install TSPUs and SORM.[28] This confirms

the intentions that representatives of several small ISPs in St. Petersburg had already mentioned in the interviews we conducted with them in 2019, when they spoke of their strategies in case of an actual activation of "Tcheburnet" (a word used by free RuNet advocates to describe the Sovereign Runet project, composed from the name *tcheburashka*, a character from a Soviet cartoon, a mythical animal that exists only in Russia, and "net" for "internet"): "We're going to go back to local networks, but also maybe experiment with administrative bricolage like cooperatives, associations or Internet enthusiasts' clubs, to share connectivity with very small circles of family, friends or loyal customers. But I imagine that, in general, if their Sovereign Runet plan really works, only a minority will be able to afford access to the global Internet, a minority that has the necessary technical skills and equipment."[29]

THE EFFECTS OF RUSSIA'S INVASION OF UKRAINE ON THE INFORMATION CONTROL INFRASTRUCTURE

Russia's invasion of Ukraine in February 2022 led to an intensification of measures claimed to "combat external threats" (as defined by the 2019 law: threat to stability, threat to connectivity, threat to security). Our analysis of press reports and specialized Telegram channels reveals the rise of alarmist discourse about a potential disconnection of the Runet, tightening controls on it, and the acceleration of the "autonomous" Runet project. Inspections were carried out at ISP offices between February and August 2022. On June 8, 2022, a draft amendment to Law 333, Part 2 of the Tax Code, was proposed, introducing fines for the lack of a SORM installation; the amount of the fine depends on the ISP's annual profits but should in all cases be at least 1 million roubles (approximately 12,800 euros).

Tests were conducted in August 2022 to check Russian ISPs' ability to respond to attacks on routing carried out via the Border Gateway Protocol (BGP). Further trials were conducted in 2022 to test DNS servers located within the country. Several new types of satellites (e.g., Gonets M and Skif D) have recently been launched to provide satellite connectivity and defense for radio frequencies. Another measure to implement the plan for the Runet's technological autonomy and digital sovereignty is the development of Russia's own

certification authorities.[30] Although this was announced in September 2022, on November 22, 2022, Sberbank, the Russian savings bank, purchased a certificate from the Greek certification authority Harica,[31] showing that, despite the rhetoric about sovereignty and despite the international sanctions against Russia, the Russian central bank continues to use European certificates. Moreover, the country's various administrative services have not synchronized their transition to certificates that are made in Russia. In late October 2022, services such as Nalog.ru[32] (taxes), Gosuslugi,[33] and Revizor were still using certificates issued by Let's Encrypt, a Californian certification authority.

It turns out that the Sovereign Runet project is itself dependent on foreign solutions—and especially American and Chinese ones—even for tools like Revizor. While it has diminishing points of connection and infrastructural dependence, these remain embedded in its foundation. Paradoxically, the context of international sanctions calls into question the realization of the Sovereign Runet project. Our analyses of the technical documentation for "special" communications solutions (for the Russian military) developed by Protei ST (a Russian manufacturer of DPI, SORM, and other filtering, monitoring, billing, and teleconferencing devices and software solutions) show a dependency on Intel processors, which can no longer be exported to Russia.

The sanctions even affected long-term and seemingly sustainable collaborations. A noteworthy example of this is relationships with Taiwanese manufacturers involved in the production of Baikal processors—which, ironically, were presented as being made in Russia. However, despite international sanctions on dual-use electronic components (those that can be used for military purposes), "parallel" import schemes have been set up at several levels. Not only have individual ISPs taken this initiative to continue to find Cisco, Juniper, or Mikrotik solutions, mostly on eBay and via Kazakhstan, SORM manufacturers have gone about it even more systematically and openly, as they publicly announced at the KROS 2022 conference. Parallel imports, in turn, impact the costs of SORM solutions, which have risen by 20 percent, and manufacturing times, which have increased to three to four weeks.[34]

The obligation to implement SORM and filtering solutions was extended to the occupied territories of Ukraine (Zaporizhzhia and the occupied regions of Luhansk and Donetsk), but their actual implementation

was pushed back to 2026 (according to Laws 5, 6, 7, and 8 FZ, which allow for a transition period). However, despite the lack of a legal framework and a standardized technological procedure, in November 2022, ISPs in the occupied regions of Ukraine received an order from the local Ministries of Communication requiring ISPs to block, slow down or "partially degrade" services for Google, YouTube, Zoom, Facebook, Twitter, Viber, and Instagram and to send reports with evidence to RKN. Instructions were sent to explain how to set up these blocks and verify their effectiveness. The licenses of ISPs that refused to block or slow down these services may be withdrawn.

Russian manufacturers of SORM and DPI boxes are exploring new markets, especially in Asia and Africa: Uzbekistan, Tajikistan, Kazakhstan, Kyrgyzstan, Iran, and Afghanistan (where Vas Expert and Protei solutions are sold and installed). Russia is thus exporting its vision of sovereignty through infrastructure, while antiwar activists, journalists, and developers are going into exile in these same regions. However, the flight of technical experts is also a factor that impacts the SORM and DPI markets.

Finally, as we have shown above, the ISP market is undergoing rapid centralization. This is happening primarily at the infrastructure level, with "outsourcing" or "upstream filtering" schemes that render small ISPs dependent on larger ones, from whom they rent infrastructure parts or buy traffic in transit. It is also taking place at the legal level, as the decline in the number of licenses issued illustrates (figure 2.3). The cost of entering the market is now 1.5 million roubles for licenses that include SORM.

CONCLUSION

A thriving market for censorship and surveillance has opened up in recent years for Russian providers of hardware and software solutions for blocking and filtering traffic. This chapter describes some of the controversial technologies at the heart of this market and shows the ecosystem of actors and socio-technical processes at work around them. It also shows how central this market's development is to the implementation of the coercive, authoritarian, and centralizing strategy that underpins the Russian state's conception of digital sovereignty.

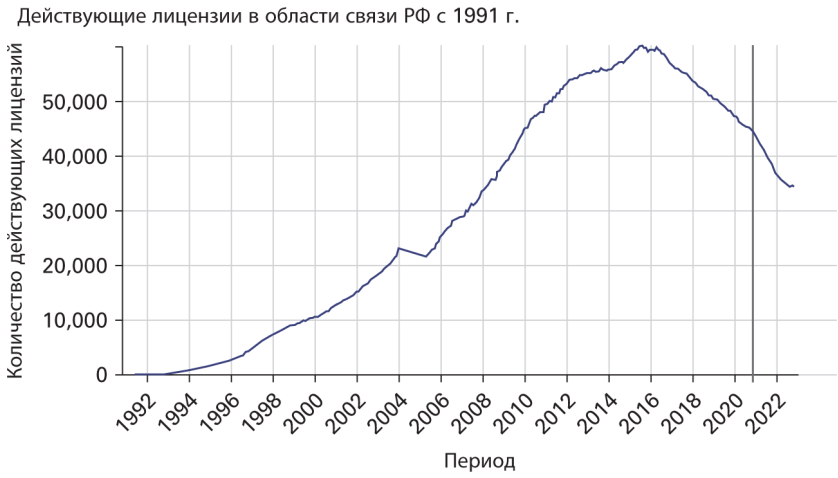


Figure 2.3

Active licenses issued in the telecommunications sector of the Russian Federation since 1991. *Source:* https://ifreedomlab.net/connectivity-rating/licenses-russia/.

A previous study of this surveillance and censorship technologies market, running from 2012 to 2019 (Ermoshina et al. 2022), showed the distributed and sometimes inconsistent nature of the Russian model of information control, which afforded ISPs some room to maneuver. Recent developments, especially relating to TSPUs, suggest that this is not as clearcut now as it was then. However, despite the considerable legal and technical adjustments that followed the introduction of TSPUs, state control over Russian networks remains incomplete. As RKN director Andrei Lipov pointed out, while 100 percent of mobile operators have installed TSPUs, only 60 percent of landline internet service providers are equipped with them. Serguey Khutortsev, director of the Centre for Observation of Communication Networks, spoke of 860 "TSPU nodes" by 2022 and promised 1,360 by 2023.[35] However, in a survey of ISPs conducted on December 22, 2021, only 19 percent of the respondents had installed a TSPU, 3 percent had signed the implementation plan, 48 percent had not yet done so, 14 percent were not going to do so, and 21 percent expressed their intention to "opt for a 'grey' strategy."[36]

As this example and many others presented throughout this chapter show, studies of this market continue to produce valid illustrations of the

diversity of constraints exerted on the Russian internet. An understanding of these constraints is in turn essential if we are to grasp the many forms of resistance, evasion, and circumvention that have developed in response to them. In this ecosystem, economic rationality is strictly linked to the interpretation of techno-legal norms and to the players' ability to navigate or oppose these norms.

NOTES

1. ISPs themselves offer different ways of analyzing the market. For instance, a study by a group of ISP employees in December 2017 found that there were 3,940 active ISPs (https://habr.com/en/post/345258/), whereas according to RKN, only 3,461 ISPs reported to the regulator in 2018 (https://rkn.gov.ru/news/rsoc/news70316.htm). (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
2. This index is no longer updated by the Internet Protection Society (OZI, a Russian digital freedom NGO).
3. According to OZI data.
4. Open Observatory of Network Interference, an open-source project monitoring internet censorship worldwide, supported by a network of volunteers (https://explorer.ooni.org/).
5. See, for example, the reaction of the Electronic Frontier Foundation to the Yarovaya law: https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.
6. On March 28, 2022, the regulators made another change to the law, allowing streaming services and online radio and television channels not to store traffic.
7. According to official government figures published on December 8, 2022, "The cost of SORM equipment depends on bandwidth and connection speed. For example, for a speed of 0–3 Gbit/second the cost of the equipment varies between 2 and 4.5 million roubles, for 3–6 Gbit/second—between 3 and 6 million rubles, for 6–10 Gbit/second—between 4 and 7.5 million roubles. In addition, these prices include implementation and configuration work, data storage for 3 years and warranty for 1 year" (https://sozd.duma.gov.ru/bill/254008-8). (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
8. Telegram channel ZaTelekom, message published on May 25, 2017 at 10:04 (https://t.me/zatelecom/192).
9. Intervention by an ISP on the Nag.ru forum, November 4, 2015.
10. Interview with Aleks Lomakin, director of the Alternative ISPs Association, August 28, 2018.
11. See the Duma's website: https://sozd.duma.gov.ru/bill/254008-8. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")

12. "Tax Code of the Russian Federation (Part Two)" dated August 5, 2000, N 117-FZ (as amended on December 28, 2024, as amended on January 1, 2025), available (in Russian language only) at http://www.consultant.ru/document/cons_doc_LAW_28165/a3cd0bcff028f127a00fa0aa61842f4ff13ffafb/.
13. The A-Record serves to associate IP addresses with a domain name.
14. https://tjournal.ru/46700-moshkov-minjust (Tjournal was blocked in Russia in March 2022 and it deleted its website; 2023 and 2024 snapshots retrieved on the Wayback Machine report a 404 error. Please refer to our Note on the Availability of Sources.")
15. This website kept a graphical record of blocked IP addresses for a long time. It became a privileged source of data for the media and regulators and was frequently consulted, including by Roskomnadzor agents. Hence Leonid Evdokimov's choice to display his message on this graph.
16. Interview of November 22, 2018.
17. https://forum.nag.ru/index.php?/topic/79886-blokirovka-saytov-provayderami/
18. An investigation carried out by ValdikSS, a hacker and activist associated with Roskomsvoboda who conducted a detailed analysis of the Revizor AS box, showed that the tender for its development was won by MFI-Soft, a company also involved in the production of SORM systems. Production costs for Revizor have been estimated at 84 million roubles (about US$1.14 million), but the state is supplying the devices to ISPs (see https://habr.com/ru/post/282087/).
19. Interview with Mikhail Klimarev, September 14, 2018.
20. https://rkn.gov.ru/communication/p922/. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
21. See the study conducted by digital law and policy specialist Serguey Hovyadinov (https://rankingdigitalrights.org/2018/07/19/russia-telcos-fail-to-respect-users-rights/).
22. Interview with Phil Kulin on the Fontanka website, May 30, 2019 (https://www.fontanka.ru/2019/05/30/058/).
23. https://roskomsvoboda.org/ru/cards/card/tspu-blokrovki-runet/
24. Video of Sergej Tëmnij's presentation at the MUSE Operators Conference on September 22, 2022, https://t.me/ordercomru/3588.
25. According to the Interfax news agency, June 15, 2021, https://www.interfax.ru/russia/772325.
26. *Kommersant*, July 29, 2021, https://www.kommersant.ru/doc/4919761?query=%D0%B4%D0%BC%D0%B8%D1%82%D1%80%D0%B8%D0%B9%20%D0%B3%D0%B0%D0%BB%D1%83%D1%88%D0%BA%D0%BE.
27. https://t.me/ordercomru/2794
28. See discussions on the Nag.ru forum: https://forum.nag.ru/index.php?/topic/146324-uslugi-svyazi-bez-sorm-revizor-i-tp/page/3/#comment-1599314

29. Interview with D., on 14 November 2019.

30. An SSL certificate is a digital certificate that is associated with a domain name or URL. It establishes the link between a website and its owner with certainty and thus makes it possible to secure electronic exchanges. Certificates are issued by certification authorities, whose reputation and renown depend on how long they have been operational and agreements with the most popular OS and browsers. In the context of the transition to the sovereign Runet, the development of Russian certification authorities would be a major decision in terms of infrastructure.

31. https://crt.sh/?id=8043006484

32. https://t.me/zatelecom/24122

33. https://t.me/zatelecom/24122

34. SORM manufacturers' conference at KROS 2022 (https://youtu.be/nZmbsYTfCNM).

35. See Serguey Khutortsev's presentation video at the 'Spektr-Forum 2022' cybersecurity conference (https://t.me/ordercomru/3811).

36. Telegram channel of OrderCom, a legal firm specializing in defending the interests of ISPs against RKN administrative proceedings (https://t.me/ordercomru/2822).

REFERENCES

Callon, Michel. 2013. "Qu'est-ce qu'un Agencement Marchand?" In *Sociologie des agencements marchands. Textes choisis*, edited by Madeleine Akrich, Sophie Dubuisson-Quellier, Catherine Grandclément, Antoine Hennion, Bruno Latour, Alexandre Mallard, Cécile Méadel, Fabian Muniesa, Vololona Rabeharisoa, and Michel Callon. Presses des Mines.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. Yale University Press.

Ermoshina, Ksenia, Benjamin Loveluck, and Francesca Musiani. 2021. "A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia." *Journal of Information Technology and Politics* 19 (1): 18–33.

Ermoshina, Ksenia, and Francesca Musiani. 2017. "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era." *Media and Communication* 5 (1): 42–53.

Ermoshina, Ksenia, and Francesca Musiani. 2021. "Ruser sur les Réseaux: Résistances 'par l'Infrastructure' des Fournisseurs d'Accès Internet en Russie." *Quaderni* (103): 53–70.

Lessig, Lawrence. 2006. *Code. Version 2.0*. Basic Books.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. 2016. *The Turn to Infrastructure in Internet Governance*. Palgrave Macmillan.

Schneier, Bruce. 2003. *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*. Copernicus Books.

Sivetc, Liudmila. 2020. "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges." In *Freedom of Expression in Russia's New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari. Routledge.

Star, Susan Leigh. 1999. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43 (3): 377–391.

Valentovich, Igor, and Ksenia Ermoshina. 2019. "Measuring Internet Censorship in Disputed Areas: An Examination of Online Media Filtering in Russia and Crimea During the 2018 Presidential Elections." Open Technology Foundation report. https://public.opentech.fund/documents/Measuring_Internet_Censorship_in_Disputed_Areas_Crimea_Russia_ICFP.pdf.

Winseck, Dwayne. 2017. "The Geopolitical Economy of the Internet Infrastructure." *Journal of Information Policy* 7: 228–267.

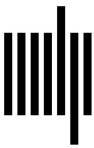
Digital Authoritarianism in the Making

Repression and Resistance on the Russian Internet

Edited by: Françoise Daucé, Benjamin Loveluck, Francesca Musiani

Citation:

Digital Authoritarianism in the Making: Repression and Resistance on the Russian Internet
Edited by: Françoise Daucé, Benjamin Loveluck, Francesca Musiani
DOI: 10.7551/mitpress/15798.001.0001
ISBN (electronic): 9780262385312
Publisher: The MIT Press
Published: 2025



The MIT Press

The MIT Press
Massachusetts Institute of Technology
77 Massachusetts Avenue, Cambridge, MA 02139
mitpress.mit.edu

Translated by Paco Libbrecht, with Elizabeth Carey-Libbrecht

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Adobe Garamond and Berthold Akzidenz Grotesk by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data is available.

ISBN: 978-0-262-55367-4

EU Authorised Representative: Easy Access System Europe, Mustamäe tee 50, 10621 Tallinn, Estonia | Email: gpsr.requests@easproject.com