A market of black boxes: The political economy of Internet surveillance and censorship in Russia

Ksenia Ermoshina, Benjamin Loveluck, Francesca Musiani

A market of black boxes: The political economy of Internet surveillance and censorship in Russia

Ksenia Ermoshina, Benjamin Loveluck, Francesca Musiani

Abstract

In recent years, the Russian Internet has developed according to strong centralizing and State-controlling tendencies, both in terms of legal instruments and technical infrastructure. This strategy implies a strong push to develop Russian-made technical solutions for censorship and traffic interception. Thus, a promising market has opened for Russian vendors of software and hardware solutions for traffic surveillance and filtering. Drawing from a mixed-methods approach and perspectives grounded primarily in Science and Technology Studies (STS), infrastructure studies and the political economy of information networks, this paper aims at exploring the flourishing sector of Russian industry of censorship and surveillance. We focus on two kinds of "black boxes" and examine their influence on the market of Internet Service Providers: surveillance systems known as SORM (System for Operative Investigative Activities), and traffic filtering solutions used to block access to websites that have been blacklisted by Roskomnadzor, the Russian federal watchdog for media and telecommunications. This research sheds light on the vivid debates around controversial technologies which Internet actors must adopt in order to avoid government fines, but which are expensive and complex to implement and raise a number of ethical and political concerns.

Keywords

Russian Internet; Internet governance; surveillance; censorship; Internet market; Internet service providers; middleboxes; SORM ; Roskomnadzor

Introduction

The Russian Internet has recently seen a swift increase in both juridical control and centralization of technical infrastructure. Its golden age as a space of "half-freedom of speech" (Gelman, 2010), with little regulation and censorship, seems to be over (Konradova & Schmidt, 2014; Oates, 2013): laws adopted in recent years, regarding the blocking of websites and surveillance of the traffic, are shaping the Russian web according to the "sovereign Internet" (Nocetti, 2015) project promoted by the government. This strategy implies a strong push for infrastructures and equipment used to control the network to be "made in Russia": in a context of international embargo and a policy of privileging domestic actors, a promising market has opened for Russian vendors of hardware and software solutions for traffic surveillance and filtering.

Based on a two-year fieldwork conducted in 2017–2019 and using a mixed-methods approach, this article aims at exploring the flourishing Russian industry of censorship and surveillance. Our research draws primarily on in-depth interviews with Internet Service Providers (ISPs), as well as on a web-ethnography of ISP internet forums and chats and a content analysis of professional documentation. It unveils vivid debates around the controversial technologies which these actors are required by law to install on their infrastructures in Russia, which are expensive and complex to implement as well as raising a number of ethical and political concerns.

In the first part of the article, we present our methods and approach, which combine the vantage points of Science and Technology Studies (STS) and more specifically internet infrastructure studies (DeNardis, 2012; Edwards, Bowker, Jackson, & Williams, 2009) with the political economy of information and communication networks (Mosco, 2009). We highlight the originality and richness of the insights that can be drawn by looking at surveillance and censorship from this dual perspective. We also provide elements of context to understand how the policies carried out by Russian authorities in order to shape technical infrastructures through legal constraints generate economic incentives as well as loopholes, friction and resistance among the actors involved.

The article focuses on two kinds of "black boxes", which are presented in detail in the second and third parts, in order to compare their role and influence on the market of ISPs. One type, known under the acronym SORM (System for Operative Investigative Activities), is used for surveillance to collect metadata and Internet traffic. The other type concerns traffic filtering, used to block websites that have been blacklisted by Roskomnadzor (RKN – the Russian federal executive body responsible for media and telecommunications, particularly censorship, content moderation and personal data protection in the field of communications). We discuss the effects of these technical objects on the market of Internet services, and the economic rationality that prevails in a context of strong technical, political and legal constraints, as well as the uncertainties and opportunities linked to their interpretation.

Market configurations or *agencements* (Callon, 2013; Muniesa, Millo, & Callon, 2007) associated with these boxes involve translating political and legal requirements into technical solutions and commercial innovations. Indeed, in the absence of standardization ISPs must interpret what is expected of them at a technical level, and with no financial support from the State most often they are expected to bear the cost of these installations alone. However, they also develop responses which can take different forms: economic (by forming alliances and

associations in order to share costs), politico-legal (by mobilizing antitrust bodies, and other legal entities), or technical (developing strategies and tricks to find a way around constraints). We thus look at the articulation between techno-legal requirements, products designed to execute them, and negotiation strategies of ISPs to mitigate economic and technical implications of filtering and surveillance, and show how this industry participates in creating "concerned groups and publics and opens new spaces for political controversies" (Geiger, Harrison, Kjellberg, & Mallard, 2014) in the governance of the Russian IT market.

We conclude by questioning the ability of governmental agencies to enforce wide-ranging surveillance and censorship policies without generating technical complications and inefficiency, closed and potentially corrupt markets, and forms of technical, legal, economic and political resistance by private intermediaries. We also alert to the potential transformation of the overall network topology as a consequence of Russia's political determination to establish greater Internet control.

Dealing with regulation: the Russian market for Internet surveillance and censorship

With 6326 licensed ISPs in 2020 and between 3461 and 3940 of them active,[1] some of which developed from local networks (*domovaya set*), the Russian Internet service provider industry is vibrant. Until recently, this market was characterized by strong competition, low prices, a good quality of networking material and connections, as well as a specific topography based on peering agreements with international partners. Lately, however, it has been affected by a gradual yet relentless centralization at the juridical and infrastructural levels. Between 2017 and today, the number of licenses delivered for "Telematic services" and "Services for data transfer" has decreased (respectively from 9395 to 8000 and from 7035 to 6326).[2] Moreover, among the latest governmental initiatives aimed at an "Autonomous Russian Internet", is the introduction of a legally-established "central point of control" for all Russian networks. This involves a mandatory registry of all Internet Exchange Points and transnational cables, which have never been properly documented in any of the government-owned lists.[3]

This centralized control over the Russian Internet is being executed via two major means, that, besides being inscribed within the same narrative of a "sovereign Russian Internet", produce, and are based on, very different technical and legal environments; and therefore create two distinct markets. These two main methods of information control are online surveillance (or "lawful interception") and online censorship (or "traffic filtering").

Surveillance, understood as "the collection and analysis of information about populations in order to govern their activities", is a "feature of modernity" intricately associated with the rise of the nation-state (Haggerty & Ericson, 2006). In the past two decades, it has largely been framed as a necessary institutional response to terrorism and to new security requirements, which have encouraged a proliferation of surveillance in various dimensions of social life and across the world. It is also associated with the accelerating digitization of social activities, enabling the monitoring of individual and collective behaviors through data collection and analysis (Lyon, 2001, 2015; Marx, 2016). Today, the growing global deployment of the "surveillance-industrial complex" is a central dimension at the junction of both state power and market dynamics, which involves a multiplicity of actors, interests and agendas (Ball & Snider, 2013). The operation and regulation of communication networks is increasingly

characterized by public-private security assemblages, but also counter-cultural and oppositional forces (Tréguer, 2019).

Censorship, i.e. preventing certain types of information from circulating in the public sphere, has become a growing issue as the promise of "free flows of information" in fact offers novel means to set barriers and check-points (Deibert, Palfrey, Rohozinski, & Zittrain, 2010). The aims of censorship range from enforcing copyright to limiting free speech, though boundaries may vary according to national political contexts: "Filtering practices closely follow the political contours of the respective governments. Repressive states are more likely to block political content, (…) most often [to] target political views that are critical of the government." (Clark et al., 2017, p. 3).

Approaching surveillance from the perspective of its political economy sheds light on its inherent logics and functioning, and on the specificities of particular regimes of control. In the Russian case, where these aspects of state power have recently been explicitly reasserted, we show how "black boxes" imposed on private actors at the Internet infrastructure level through regulatory measures are embedded in (and contribute to) a nexus of social, economic and political relations – thus de-constructing the overly simplified image of a State-led direct control via technology. By doing so, we aim at understanding a key aspect of the "global war for Internet governance" (DeNardis, 2014), and how the Internet infrastructure itself may be leveraged to assert power relations. This "turn to infrastructure" in Internet governance (Musiani, Cogburn, DeNardis, & Levinson, 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.

Indeed, the relationship between legal procedures and technical implementation is a central dimension of Internet governance: the behavior of Internet users is regulated by inscribing norms, affordances and constraints in both the technical infrastructures and the law, and decision-makers increasingly leverage them together to achieve (geo-)political aims (Winseck, 2017). This is particularly true in Russia, where law and code interact in very specific ways. However, technical solutions often lag behind regulation as the law seeks to gain the upper hand on technology (see for details Ermoshina & Musiani, 2017). The "Yarovaya law" of 2016, which we discuss below, is a case in point, as it vastly expanded the requirements for providers to collect and store communications data and metadata for surveillance purposes. Legal initiatives have generally failed to provide frameworks for the production and certification of concrete technical solutions, which has led to long periods of techno-legal vacuums, where ISPs have been actively experimenting and tinkering in order to cope with (technically) imprecise yet (legally) stringent new requirements.

This feature of Russian Internet regulation has given way to critiques from the ISP community describing it as a "theater of security" (Schneier, 2003), where political rhetoric obscures underlying business opportunities. As we will develop later in this paper, the ISPs understand Russian Internet regulation as driven mainly by *economic* rather than political or technical motivations, benefiting the vendors of technological solutions needed to implement the new laws: given the "substitution of import" imperative (the privileging of domestic businesses), these solutions have to be "made in Russia" – by Russian actors.

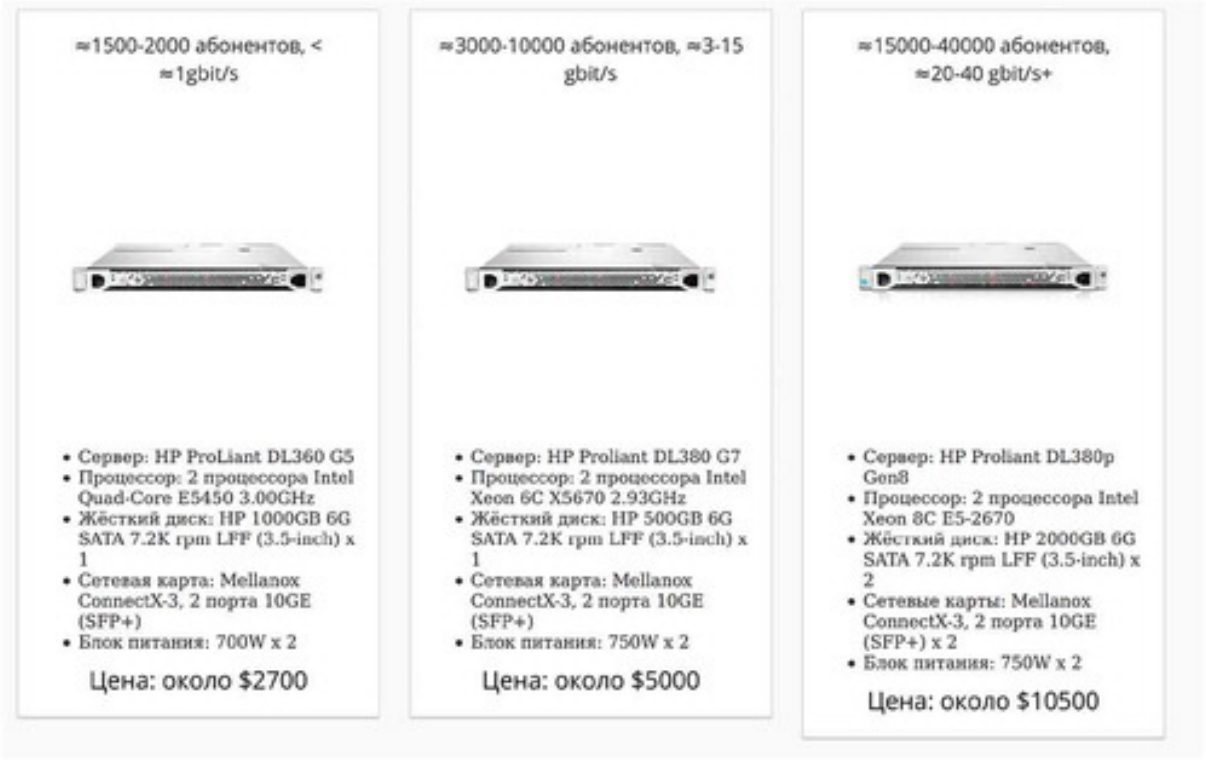
In this context, the regulation of the Russian Internet produces a full-fledged market of censorship and surveillance alongside the ISP market, shaping competition between the various vendors of infrastructure components and affecting the operations and strategies of ISPs – but also generating friction and resistance. Investigating these markets together allows to closely

analyze the relationship between normalization and competition: even if governance of the Russian Internet is increasingly presented as an issue of national sovereignty, the Russian State remains slow in producing and certifying technical solutions for surveillance and censorship. This leads to techno-legal loopholes and gray zones which create both uncertainties and opportunities. Studying the business of intermediary "boxes" (or "middleboxes") also allows us to shed light on resistance practices that are often developing as a response to specific filtering and surveillance techniques, and to follow and understand the politicization of Web professionals.

This research investigates two main types of technical solutions used for information control: the first one is known as SORM (for "System for Operative Investigative Activities") and its purpose is the *storage and analysis* of internet traffic for lawful interception; the second one is referred to as "RKN-compliant" and must be deployed to ensure the *filtering and blocking* of websites which have been blacklisted by Roskomnadzor.

This involved drawing on ethnographic methods and looking in some detail at the "standards, wires and settings" (Star, 1999, p. 379) of these technologies. They can be considered as "*black boxes*", in the sense derived from Actor-Network Theory (see e.g. Callon, 2013), at several levels: first because of their supposed technical opaqueness, but also due to their functions as filtering and surveillance devices, which place them within the realm of state and trade secrets. We approached them, from an STS perspective, as composite objects and heterogeneous networks (Akrich, 1992): though often called "middleboxes" within specialized communities, these technical objects do not always look like clearly identifiable physical "boxes" (although this may be the case – see Figure 1), but rather consist in a multitude of software solutions, distributed technical objects and techno-legal adjustments that complement existing material infrastructures. Moreover, they are a key locus of surveillance and censorship-related controversies in Russia, generating ambiguities, interpretations, disputes, resistance and negotiations.

Figure 1. Example of "actual" boxes: options of filtering equipment. Source: https://www.carbonsoft.ru/products/carbon-reductor/carbon-reductor-app/



Investigating such activities, which are both specialized and sometimes shrouded in secrecy, raised several hurdles. These were addressed by adopting a mixed methods approach, and the collection of three main types of material over the period 2017–2019. First of all, we conducted 15 interviews with ISPs, IT experts, Internet lawyers, vendors of filtering equipment, as well as anti-censorship and anti-surveillance activists. These respondents were recruited in several steps. First, we contacted publicly known experts in the field of telecommunication, Internet censorship and surveillance and digital rights, previously met at a variety of professional gatherings we regularly attended and observed (e.g. RightsCon, Internet Freedom Festival, Privacy Day, Chaos Communication Congress and so on). After this first round of interviews, we requested help from these experts in recommending us to ISPs possibly interested in taking part in the study. This recommendation process was important in itself, as the ISP community is relatively closed. The ISPs we talked to are mainly small and medium-size (between 5000 to 100 000 clients) and are active participants of professional forums and Telegram-chats (such as Nag.ru and other communities that we have identified during web-ethnography). We also talked to representatives of vendors of DPI and filtering solutions, and to engineers working at the Saint-Petersburg Internet Exchange Point. The respondents requested to stay anonymous.

The study was completed with a web-ethnography and analysis of dedicated ISP forums and chats, which were selected and monitored over the whole period (see Appendix for details). Finally, we carried out a content analysis of the communication material produced by vendors of surveillance and censorship solutions: websites, commercial presentations, and material drawn from specialized professional conferences.

SORM and the surveillance market: strong constraints and a lot of tinkering

SORM is a legally-defined system for lawful interception of telecommunications. It is a distributed object made up of commutators, switches, servers and software installed at operator and service provider expenses, but directly controlled by the FSB (the Russian Federal Security Service, whose responsibilities include counter-intelligence, counter-terrorism and surveillance) via a terminal and can be accessed on demand by other agencies and police departments (tax, customs, border police etc.). SORM-1 was set up in 1995 for wiretapping and phone surveillance. Since then, it has evolved into SORM-2, adapted to the internet in 1998, and SORM-3 in 2014, which included specifications for metadata (such as time and date, location, and sender and recipients of messages) and multimedia files collection. The latest iteration was defined by the "Yarovaya" 374-FZ[4] and 375-FZ laws passed in 2016, raising a wave of criticism from digital rights and freedoms advocacy organizations.[5]

After almost two years of discussions due to the technical complexity of the law, and due to abundant criticism coming from the ISP community, the regulation was somewhat loosened. The 12 April 2018 amendment to the Yarovaya law introduced new requirements for data collection: telecom providers should now store metadata for 3 years and the content of all voice calls, data, images and text messages for 30 days (instead of the original 90 days), increasing the duration of storage by 15% every year. These must be made available to authorities upon request and may be obtained without a warrant or court order; moreover, online services using encrypted data for messaging, e-mail or social media should allow the FSB unencrypted access to these communications (although in April 2020, in the Covid-19 pandemic context, it was suggested that the obligation for ISPs to increase storage duration should be postponed by one year).

The new regulation has drawn intense criticism not only because of the extended scope of the surveillance, but also due to the high costs of data storage. Indeed, an analysis[6] of its implementation and maintenance costs found that these could reach a minimum of 105k rubles or 1400 USD (according to the public university RGGU[7]) and a maximum of 91 383 000 rubles or 1.24 million USD (for a big telecommunication company, Rostelecom). At the providers conference KROS[8] in May 2017, this was reasserted by a representative of NORSI-TRANS, one of the leaders of the SORM solutions market:

"*The storage of 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 existing equipment, with minimal extensions and a clear technical solution, without shenanigans*."[9]

Moreover, the certification process is long and complex, involving a multitude of institutional actors each responsible for certification of a component or several components of the system. They must be tested according to a clearly-defined methodology which should first be certified by the FSB and the Ministry of Communications. Afterward, FSB tests the installation using a simulator, and only after that can the 3-month certification process begin. According to the director of OrderCom, a legal consultancy agency for ISPs, certifications for SORM-3 Yarovaya will not be published until 2021.

In previous rounds, ISPs have taken advantage of this techno-legal vacuum: "The legalization of SORM-2 took 10 years, the ISPs managed to defend themselves in courts because the equipment was not certified".[10] ISPs are aware of this gray zone and try not to be overzealous in order to minimize costs. In the absence of standardized and State-certified solutions, they limit themselves to tinker with and adapt existing infrastructures, "*because when they finally publish the certs, we will have to spend lots of money again, and we will have to do so, because it's the law*"(an ISP, Nag.ru forum, 4 November 2015).

Thus, legal responsibilities are not clearly defined. Misconfigurations of SORM boxes are frequent, which puts users' personal data at risk. The system is also prone to corruption. The situation is particularly problematic due to the data's sensitive nature, the different parties involved and the secrecy of the process:

"*Everything is distributed. Every ISP has its own equipment. The ISP buys it from a vendor, but there's also the person who will install this equipment, and the end-user, the FSB agent. So. (…) Who will be responsible in case of a leak? Who will appear in court?*" (SORM conference, November 2017).

However, the requirements seem to be adapted to the ISPs' size and budget. Large ISPs have to fulfill the requirements, but small ISPs do not always install SORM boxes and instead answer FSB demands on an *ad hoc* basis: "*When it's needed, the FSB calls us or contacts us over e-mail and asks to make a tcpdump of traffic for a specific IP, and share it over ftp or something like that*"[11]; "*Sometimes they [the FSB] come in person, plug into the network and listen*"(interview with Aleks Lomakin, Director, Association of Alternative ISPs, August 28, 2018). Other options include a collaboration between ISPs, who can decide to share the costs of a SORM solution – according to the OrderCom director, this may represent a 20–25% cost reduction. Another solution, called "outSORMing", involves an agreement whereby smaller actors may buy traffic which is already "SORMed" by big ISPs. Occasionally, a "SORM race" may take place, whereby ephemeral ISPs are set up and new legal entities are created in case of SORM-related problems.

Our analysis of professional ISP forums (e.g. Nag.ru), shows a critical and somewhat ironic attitude of small and middle-sized ISPs vis-à-vis SORM: the satirical drawing below (Figure 2) was published on Nag.ru and Order.com and shared widely in the ISP community. The female-looking "robot" embodies Iryna Yarovaya, the representative responsible for the "Yarovaya law"; the man in a suit stands for a vendor advertising the most expensive solution (20 million rubles, 270 000 USD) to a group of men (representing providers). Scared by the price of SORM solutions, they run away in the "shadowy forest" – a gray zone where they hope to find refuge from regulation by deploying semi-legal schemes.

Figure 2. A satirical drawing about Yarovaya law and its consequences for ISPs. Source: https://www.ordercom.ru/sorm-vvod-otchetnost/copm.html

At the moment, the actual efficiency of SORM is questioned; SORM could be either absent or badly configured for 70% of ISPs.[12] In 2017, 451 cases for violation of SORM regulation were filed, according to our analysis of open data on court hearings: 196 operators were fined, and 192 warned. Our interviews show that operators are reluctant to install SORM for four main reasons. The first one is economic: for small and medium-sized ISPs it is often easier and less costly to pay fines (around 30k-50k rubles, 400 to 660 USD) than to buy SORM solutions. The second reason is infrastructural – according to Klimarev, Director of the Society for Protection of the Internet, a nonprofit non-governmental organization: "*Preexisting infrastructures are sometimes incompatible with new equipment that 'very competent institutions' would like to make ISPs implement. In order to install this equipment, the ISP has to fundamentally change network architectures"*. The third reason is technical: recording and storing encrypted traffic is inefficient for lawful interception goals, because most of it is impossible to read. The final reason is operational, since in most investigations, FSB agents will rather visit the ISP directly

and ask for client-specific information, or use other means (e.g. manual tapping, device seizure or hacking into accounts).

SORM requirements are thus contested by operators, primarily because of the financial costs and the technical complications which ISPs have to bear, and the perceived inefficiency of top-down, bureaucratic demands. They are also considered by many interviewed actors as a potential source of corruption, because of the very architecture of SORM systems. In fact, SORM consists of two main elements: one is the terminal installed at the office of a regional FSB "curator" which enables direct, remote access to the traffic of all ISPs in his territorial jurisdiction. The other element is the traffic storage system installed on the ISPs' premises. For a long time, the remote terminal was not interoperable and could connect only to storage systems of the same vendor:

"*The ISP is caught in the crossfire. To store information about the client, the storage system installed by the provider has to understand commands from the terminal which is located at the FSB. In the early years every territorial office of FSB had a terminal from a very specific vendor, purchased through Defense Procurement and Acquisition. Norsi-Trans in Nizhny Novgorod, Spectech in Saint-Petersburg and so on. Only after the certification of SORM-2, have the terminals become universal and interoperable*."[13]

This lack of interoperability between terminals and the rest of the system has led to a quasi-monopoly of a specific vendor on given territories. Moreover, the link between SORM vendors and the Defense sector leads to the "*opacity and relative inaccessibility of the SORM market*", as described by one of our respondents, a vendor of DPI (deep packet inspection) solutions.

Entities such as the Association of Alternative ISPs are attempting to carry out an antitrust investigation. Its director says:

"*We try to show that the price of this equipment is too heavy, we will file a collective complaint to contest the price of SORM, so that the FAS (the Federal Antitrust Service) accurately counts market shares, their revenue, their expenses … verify the cost of different elements. Some ISP colleagues have de-constructed these boxes. They have worked out a gross margin of about 90% ... Yarovaya has allowed a small group of firms to really profit*." (interview, 28 August 2018).

Thus, "new resistant" figures are born as well: those of small entrepreneurs who were deeply, and negatively, affected by the profit of few which the Yarovaya law engendered.

RKN middleboxes and the censorship market

The laws introducing web content blocking exist since 2012, when a blacklist of web content and pages held by RKN was introduced, along with the coopting of ISPs under Russian jurisdiction to implement the blocking (Sivetc, 2020). The regulation was set up in the wake of the 2011–2012 protests against electoral irregularities, which resulted in a reshuffling of the digital media landscape (Denisova, 2017), but its full implications appeared during the Ukrainian crisis in 2014, which became a testbed for Russian authorities' tightening of information control. Filtering practices expanded to areas way beyond protecting children from harmful content and by March 2014, Russia had four official blacklists of banned websites (so-

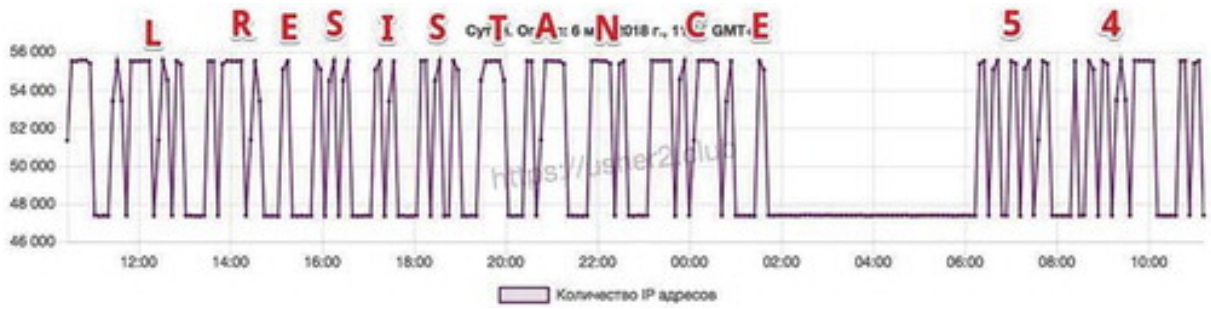
called “extremist”; child pornography, suicide, and drugs-related; copyright-infringing; and calling for “unapproved” public rallies and demonstrations) as well as an unofficial fifth blacklist aimed not at websites, but at hosting companies based abroad deemed uncooperative by RKN (Soldatov & Borogan, 2015).

However, our interviews with ISPs show that already in 2008–2009, providers received requests to block access to specific websites on a case-by-case basis, for issues related to gambling and pornography. The introduction of a centralized blacklist made it harder for ISPs to ignore requests and defend themselves in court. Precise requirements were only published in March 2018 with law 149-FZ, article 10, which defines technical parameters for standardized “block pages” and a detailed set of technical recommendations for filtering content and blocking websites.

Strictly speaking, there is no “law on censorship”; existing laws are modified to add an administrative or penal responsibility for the publication, diffusion or hosting of content considered “illegal”. At least eight different organizations can decide on this “illegal” status: the Federal Service of Taxes, tribunals of particular cities, the General Attorney, RKN, the Ministry of Internal Affairs, the Tribunal of the City of Moscow, the Federal Service of Drug Control, and RosPotrebNadzor (an agency responsible for protecting “consumer rights and human wellbeing”).

The blacklisting system has been harshly criticized by free speech advocates, because the categories of “illegal” content are vaguely defined, leading to arbitrary decisions. Moreover, the absence of court oversight facilitates the blacklisting of opposition websites for political motives. The measures initially triggered a series of inventive initiatives that leveraged the Domain Name System mechanism as a tool of contention, exemplified by the controversy surrounding the online library of Maksim Moshkow, blocked in 2012. Moshkow, a Russian Internet pioneer, had spearheaded major media Internet projects (e.g. Gazeta.ru); Lib.ru, also known as *Maksim Moshkow’s Library*, started to operate in November 1994 and became the largest and most comprehensive Russian electronic library. Moshkow’s response to the blocking of his library was to leverage the vulnerability in the very mechanism of web censorship to block the Ministry of Justice’s main website. Because many ISPs were automatically blocking all IP addresses from the “A-Record”[14] of a blacklisted DNS, Moshkow simply had to modify the A-record of his own website by adding the IP address of the Ministry of Justice.[15] Following the same principle, in 2017, a number of DNS-based “guerillas” took place, including the blocking of AS Revizor, a number of platforms and social media, and several DNS root servers. Activists used the RKN blocklist as their starting point: they bought a few “orphan” domain names whose subscription had expired but which were still in the list, and proceeded to modify their respective A-records. On May 6, 2018, Leonid Evdokimov wrote “digital resistance” in Morse code on the graphics of blocked ISPs (Figure 3) exploiting the same vulnerability.

Figure 3. Evdokimov’s Morse message (https://usher2.club/)

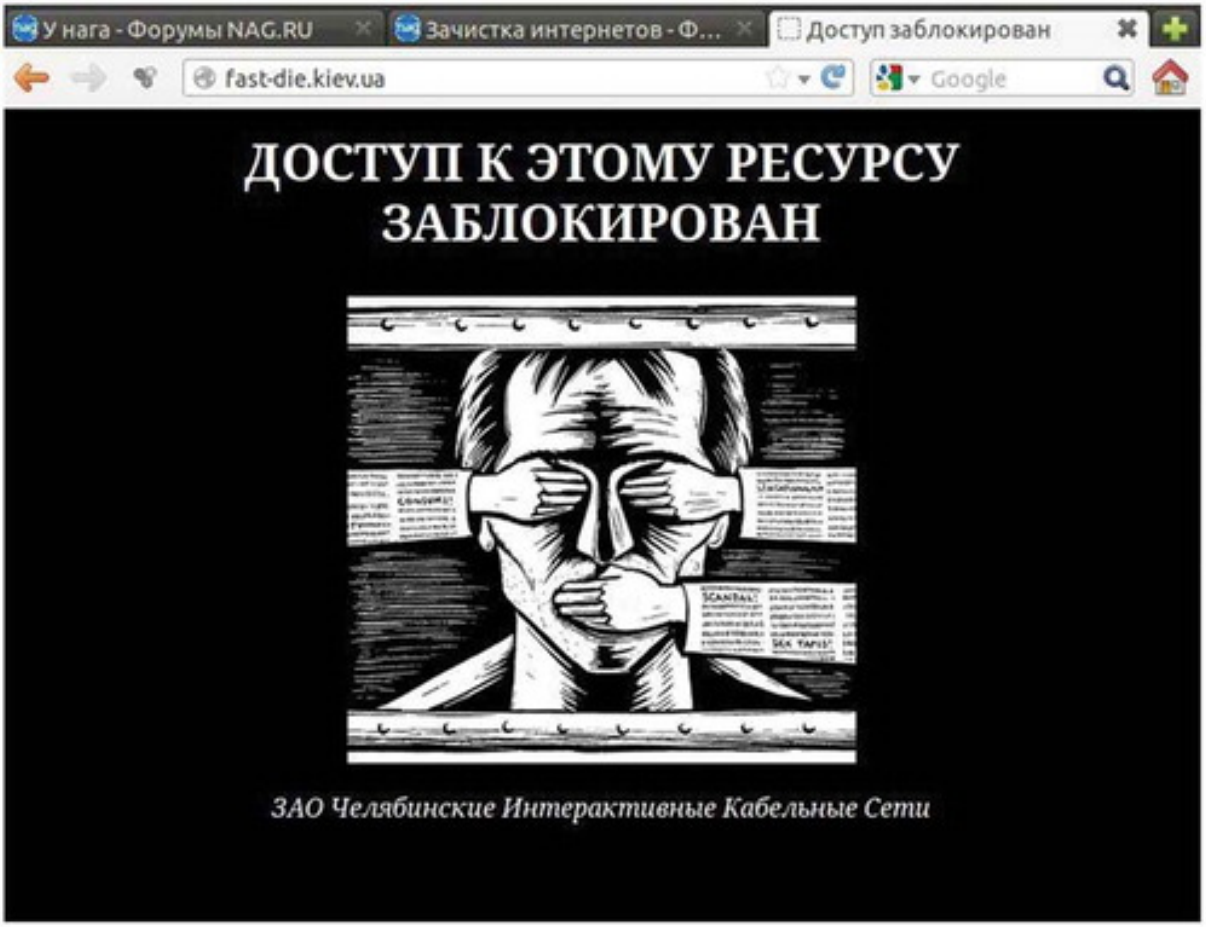


These cases had consequences for the regulation and implementation of censorship, and the way blocklists are maintained. Before Evdokimov's action, in April 2018 the blacklist counted 5136 orphan domain names that could have been used to reproduce a DNS attack, while on 13 May 2018 it counted only 204 such domain names. This "side-effect" was criticized by some of our respondents, who said that activists ultimately helped RKN to improve its management of Internet censorship.

Other forms of resistance involve blockpages, placed by ISPs in order to denounce censorship when a particular address redirects to a blocked site (Figure 4). Blockpages were also used to inform users about reasons of blocking and means of circumvention, and to express criticism of Internet censorship and RKN (Ermoshina & Musiani, 2017). For example, some ISPs would add a link to RFC 7725,[16] an IETF standard for the "Error 451", which is a peculiar text in itself: its name refers to Ray Bradbury's landmark work, while the second paragraph of the standard explicitly recommends using Tor and VPNs to circumvent blocking. Other ISPs expressed criticism on the blockpages:

"*When users try to access a blocked page, we show them the error message that starts with a phrase: 'The struggle against evil is almost never a struggle for good'*"

Figure 4. Example of a blockpage featuring an illustration from George Orwell's 1984 (screen capture; the URL belongs to a Ukrainian website focusing on suicide)



(interview, representative of an ISP from Penza, 27 September 2016). However, amendments to the article 15.3 of the 149FZ law introduced a standardized text for blockpages, which considerably reduced the popularity of this form of contention among ISPs.

Activists have made the censorship issue more visible by revealing some of the limits and vulnerabilities of the blocking mechanisms (e.g. DNS guerilla). Russian web operators and professionals, however, must implement these regulatory measures, which affect their business and, to some extent, question the values of openness they might uphold. Thus, they have often adopted different strategies to resist and adapt to them.

Just like SORM, the "boxes" to be implemented are in fact hybrid objects and can take different forms, such as homemade scripts which ISPs put together, hardware solutions, cloud-based solutions, or software for DPI blocking. ISPs can therefore choose between different options, and can rely on either DNS, proxy, IP or DPI for filtering and blocking traffic.[17] The director of SkyDNS, a vendor proposing traffic filtering solutions, points out:

"*There was a technological vacuum of sorts – block as you wish. RKN could not advise ISPs on solutions, lest they fall under antitrust laws. But very soon, there were several complaints from administrators of mistakenly blocked websites … So they started to mandate blocking via URL. ISPs used to write their scripts in a DIY fashion, but this is no longer very frequent, as they risk being penalized*" (interview, 22 November 2018).

According to an ISP in the Moscow region (40 000 customers), manual blocking became too hard as the blocklist grew longer. Moreover, this blocklist is often criticized by ISPs for multiple

mistypes and a messy structure that results in errors. An informal survey on an ISP forum[18] shows that the most popular methods are IP blocking and DPI.

Several ISPs looked for ways to avoid substantial investment in the most expensive blocking/filtering solutions, and blocking among ISPs was not homogeneous. In order to better control the even application of the blacklist, RKN introduced another technical solution for Web content blocking in December 2016: the Revizor Automatic System (AS Revizor). ISPs quickly identified the label's ironic connotation, comparing it to Nikolay Gogol's play of the same name (translated into English as *The Inspector General*), satirizing imperial Russia's extensive political corruption. The tender to develop Revizor was allegedly won by MFI-Soft, a company also involved in the production of SORM systems. AS Revizor's production costs were estimated to be 84 million rubles (close to 1.14 million USD),[19] however the State provides the devices to ISPs.

Revizor ensures the automatization of ISP controls, including those of smaller ISPs. It comes as a box (a router containing an embedded operating system and pre-installed software), as a virtual machine or as software for Windows and Linux. As its code is not open, its functioning and features remain obscure for the involved actors. An engineer conducted an independent investigation to describe Revizor's actual work, demonstrate its vulnerabilities, and compare the actual costs of its components compared to Revizor's market price. Beyond these security issues, a few outages of Revizor were experienced due to the overloaded blacklist.[20]

With the addition of Revizor and because of its numerous failures, responsibility attribution in the censorship market is often controversial and problem-generating. Klimarev explains:

"*Let's suppose I am a small ISP, and I buy Rostelecom's pre-filtered traffic. I install Revizor, but something is not blocked. Who pays the fine? Rostelecom or I? Rostelecom will say I have badly configured and implemented the equipment at the local level…* "

In this context of legal uncertainty and absence of specifications, a market of website-blocking solutions has developed. Unlike SORM vendors, mostly specialized in developing solutions for lawful interception and connected to the defense and state security sectors, the majority of filtering equipment vendors (e.g. SkyDNS, Ruspromsoft or CarbonSoft) previously made a living by offering solutions for billing or parental control; eventually, filtering solutions were introduced as one of their services. Some companies (e.g. the small CyberFilter) were created specifically to respond to RKN's requirements. ISPs mentioned at least fourteen different filtering solutions during our interviews or on specialized forums. For a long time, a confusion persisted among ISPs at the moment of choosing a particular vendor, the leaders of the market being Carbon Reductor and SKAT.

In an attempt to stabilize and standardize blocking procedures, and supposedly due to requests by ISPs, RKN conducted a massive testing of thirteen solutions (August 2017-March 2018). Vendors were asked to install their blocking solutions among a number of ISPs (between 10 and 30 depending on the equipment), and a certified laboratory observed their functioning for a month. The test compared different solutions according to a number of parameters, including the proportion of "extremist" non-blocked content and of "other" non-blocked content, and established a ranking of the solutions according to the "quality" definition established by these criteria. The results were published on RKN's website.[21]

Overall, several trends and strategies can be identified within the Russian censorship market to deal with the requirements. Middlebox vendors compete fiercely to provide either the cheapest

or the most efficient solutions, while bigger ISPs sometimes avoid blocking everything to attract more clients. This can result in a "non-compliance as a feature" arrangement: vendors start advertising built-in ways to avoid charges for non-blocking and minimize impacts from state regulators. For instance, after massive blockages of Amazon and Google servers and popular websites, as a side-effect of the "Telegram ban",[22] Carbon Reductor proposed a pack that guaranteed ISPs' ability to provide access to popular platforms for their clients without being detected by Revizor and fined by RKN. ISPs actively seek ways to avoid compliance with censorship, especially if it involves substantial investment on their part, and this becomes part of their market positioning.

Some ISPs engage in practices of selective censorship or attempt to fool Revizor. According to the director of SkyDNS: "*Some operators apply censorship only to a separate sub-network, where they install Revizor. And for their final users, they fashion another network where there is no or little censorship*". On their end, network administrators or hosting services engage in technical ruses of their own; e.g., when IP addresses of Revizor are identified, a blockpage is sent as a response.

Other strategies involve legal resistance. The OrderCom organization provides support to ISPs opposing RKN-mandated decisions and fines, with some success: in 2016, 15% of the decisions were canceled. ISPs also contest what in their views are mistakes derived from the use of Revizor, by providing certified conform copies of the blocked pages. However, out of 33,533 court decisions, only 46 cases were successfully contested between 2012 and 2017, according to a study by the digital law and policy researcher Serguey Hovyadinov.[23]

The Russian regime of Internet surveillance and censorship: economic and political implications

One of the main consequences of surveillance and censorship requirements for ISPs has been a rise in their overall expenses. According to the director of the Association for Alternative ISPs, "*Yarovaya has had a substantial impact … [Equipment costs] are at least equivalent to an ISP's annual income, even without the additional certification costs*". Indeed, costs for the entire sector are estimated by the FSB and the Ministry of Communications to be around 4,5 trillion rubles (60 billion USD), and by the Union of Russian Industrials and Entrepreneurs to reach as far as 17,5 trillion rubles (235 billion USD). [24] It has also resulted in price increases for Internet services.

However, the fundamental differences between SORM equipment and the solutions for traffic filtering and website blocking are not only technical, but extend to their economic and legal consequences, and ISPs' perception of them. The SORM industry is directly connected to national security and defense sectors, and relatively closed to external players. It is considered to be intrinsically "corrupt", and its technical soundness is heavily criticized: storage of encrypted traffic is considered useless for investigations, and all the interviewed ISPs said they doubt SORM can help prevent terrorism. Finally, because of their very high costs, solutions for SORM and Yarovaya law are deemed destructive for the Internet services industry. Conversely, filtering solutions were developed from a preexisting market of billing, parental control and traffic optimization solutions, also intended to improve the quality of Internet services (especially for B2B ISPs, as a vendor of DPI solutions explained in an interview). Vendors of

filtering solutions are not directly associated with security services, and are perceived as a "necessary evil". Although the ISPs we interviewed generally do not appreciate website blocking and criticize "*very long and often dirty blacklists*", they think that "*everybody knows how to use VPNs and users eventually will find their way out*".[25]

Moreover, differences in the technical architecture of these two systems shapes the market dynamics and their relation with the state. SORM requires a remote-control terminal installed at the FSB, therefore the production of SORM solutions involves a collaboration with the state special services. This was especially true in the early years of SORM-2 systems, when the remote control was not interoperable and bound ISPs to the equipment produced by specific vendors. Conversely, website filtering and blocking solutions offer more flexibility in terms of technical design (of both software and hardware), and can be developed rather autonomously from state control. As mentioned above, tests were conducted to evaluate the efficiency of certain solutions, but using one of the tested devices is not mandatory. Two interviewed ISPs said they still use hand-made solutions for filtering and have almost no problems.

However, the "turn to infrastructure" in Russian internet governance and stricter control of the ISP industry have led to important reconfigurations within the market for Internet services: especially a growing consolidation and centralization of commercial ISPs. According to the director of SkyDNS:

"*We have twenty ISP clients using [our solution] Zapret ISP, and around three hundred using our solutions for cloud filtering. We see a trend: the big ones, especially Dom.Ru, are absorbing small ones. If you have two or three thousand subscribers, you are a sure candidate for acquisition*".

Almost all interviewed ISPs agree with the general trend toward monopolization of Internet services by a few big companies, involving increasing infrastructural dependence of smaller ISPs on bigger players, such as the obligation to rent conduit systems from them (through which fiber-optic cables can be pulled) or to pay extra fees to have the right to connect new buildings.

On the other hand, some of our interviewed ISPs say that the Yarovaya law had only limited impact on price increases, and attribute them to the overall economic and political crisis:

"*The rise of pricing is due to the crisis of the ruble: we buy equipment from abroad and depend on the currency exchange rates. We increased the price by 200% during the last 5 years, but in the end it's only about 500 rubles (6.7 USD) per month for a basic plan*".[26]

Indeed, not all interviewed ISPs agree that "black boxes" have a direct effect on prices and quality of Internet connections for Russian users; according to them, other legal initiatives also contribute to substantially reconfigure the market. For instance, the Ministry of Communications' Order #148[27]forces ISPs to provide "free access to socially important resources" since 1 April 2020, which includes 400 Russian websites.[28] Besides the law's controversial impact on net neutrality due to the discrimination in website access it entails – presented in a positive light, but discrimination nonetheless – the resulting loss for the ISP market is estimated at around 200 billion rubles (2.7 billion USD).[29]

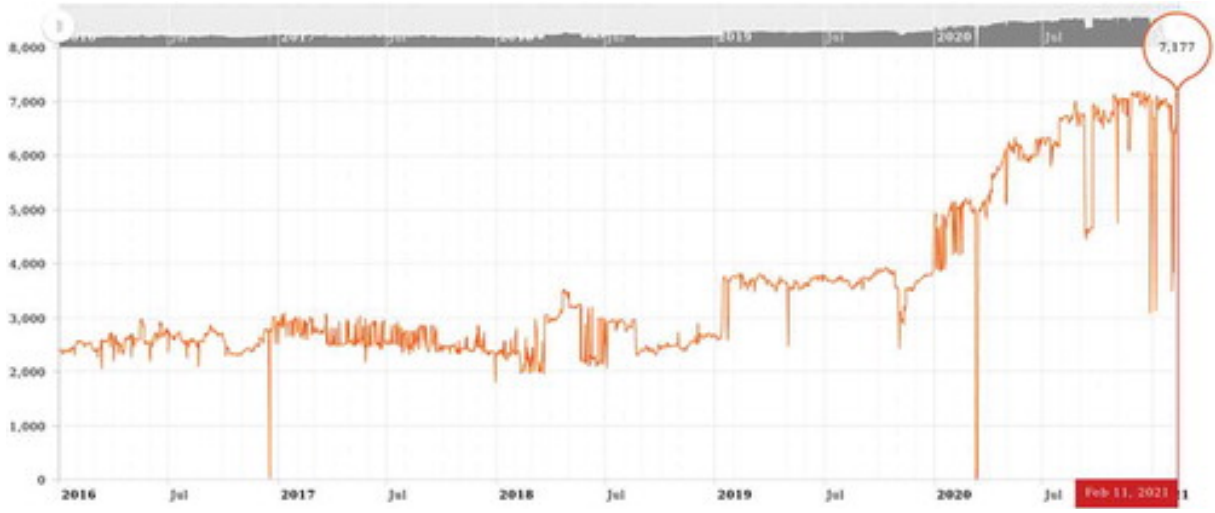
Finally, ISPs argue that prices of Internet services rise also because of the market saturation and the fact that it is hard for ISPs to grow. The point of saturation is located somewhere between 2008 and 2010, depending on the interviewees. Thus, state regulation is perceived by

ISPs not always as the key factor, but as an additional obstacle for successful development of their businesses.

Another likely long-term indirect effect is the threat that the Russian network could be "cut off" from the wider Internet. With the law "On the isolation of the Russian segment of the Internet" in February 2019, a possible "kill switch" was legitimated by external danger, namely, by the "aggressive nature of the United States National Cybersecurity Strategy". According to the law, Russia intends to create its own version of the DNS, to operate if links to servers located abroad are broken, and ISPs will direct information flows exclusively to government-controlled routing points. Internet Exchange Points (IXPs) which were relatively free from regulation, will now forcibly become part of the official registry.

ISPs are concerned by the centralization of routing paths, described as harmful for the overall Internet "health" as it enables easier control over ISPs and makes it possible to shut down parts of the network. Even before the law on digital sovereignty, Internet shutdowns were orchestrated in several regions of Russia, e.g. Ingushetia in 2018[30] or Moscow in 2019,[31] during mass protests. However, the law has not (yet) had any tangible consequences for the connectedness of the Russian networks with the rest of the world, at least according to the Connectivity Index – developed by the Society for Protection of the Internet[32] to monitor connectivity between Russian and foreign Autonomous Systems – which shows that the overall connectivity is growing (Figure 5).

Figure 5. The SPI's connectivity index grows in 2020; the sovereign Internet law does not yet have direct consequences on BGP traffic. Source: https://ozi-ru.org/proekty/indeks-svyaznosti/



Unlike in China, Russian Internet infrastructure is very closely entwined with the global Internet. According to the director of SkyDNS: "*When it comes to cables, China can afford a balkanization, but Russia cannot. We are too dependent on the international infrastructure. This will entail a catastrophic degradation of Internet services*." The unsuccessful attempt to block the instant messenger Telegram has proven that methods used by RKN cannot guarantee an efficient isolation of parts of the RuNet without causing collateral damage, including accidental blocking of state-owned digital services, some of which turn out to be hosted on foreign servers. Hence, many of our respondents share an optimistic view of the situation,

summed up in this interview excerpt: "*Our government's laziness, corruption and lack of expertise will protect the RuNet better than any protests*".[33]

Conclusion

This paper has explored the flourishing "market of censorship and surveillance" that has opened in recent years for Russian vendors of hardware and software solutions for traffic blocking and filtering. We aimed to shed light on the debates around controversial technologies that are at the core of the Russian Internet market. These technologies are expensive, complex to implement, and problematic from ethical and political standpoints.

Surveillance and censorship have been present in Russia for a long time, with the SORM system set up in the 1990s when computer networks started to grow. However, since the early 2010s, as a consequence of the political tensions that have risen internally and abroad, Russian internet legislation has considerably tightened, illustrating the government's strategy to establish national control within a digital arena that had hitherto escaped it. These national regulatory measures demonstrate the coercive dimension chosen as a response to the challenges the internet poses to sovereignty. Our research contributes to investigate techno-political and legal measures as a testament to Russia's efforts of refocusing its internet nationally.

We show that this control policy must not necessarily be seen as following a vertical, coherent and hierarchical model. The somewhat simplistic image of a State regulation that merely needs to deploy a given technology in order to attain its political objectives needs to be questioned and de-constructed. Indeed, the analysis of the Russian internet industry and its regulation for surveillance and censorship purposes shows that the laws applied to online activity are numerous, varied, constantly adapting, and their enforcement often arbitrary. Close examination of the legislation and its consequences shows not a centralized domination of the Russian network, but a multiplicity of types of control that are partial, fluctuating and sometimes contradictory. Understanding the diversity of constraints exerted on the Russian internet is essential for understanding the many forms of resistance, escape and circumvention that have developed in reaction to them. We have also shown that the forms of resistance range from public displays of protest to underground, infrastructure-embedded circumvention strategies, including a whole range of hybrid practices, part protest, part arrangement.

In this context, marked by norm enforcement via a techno-legal apparatus on one hand, and different forms of "digital resistance" on the other, we have sought to observe how Russian Internet regulation has recently given way to a true market of censorship and surveillance, which is embedded in the wider market of Internet services, and re-models it in depth. In this market, and in a situation where clear and balanced guidelines are mostly absent for the technical actors of the Russian Internet, economic rationality is strictly tied to the interpretation of techno-legal norms, and to the capacity of actors to negotiate, or disagree with, these norms, as the numerous examples of strategies and compromises have shown throughout the article. ISPs are central actors in this process, having to deal with legal constraints, but also with the uncertainties related to the absence of certification, standardization and "proven" technology, the difficulty to establish responsibilities, and their relative political and economic weight. Our research proposes an alternative investigation of online resistance in Russia, that reveals less well-known social practices and techniques for circumventing online constraints. This endeavor, present and future, is intended, beyond Russia, to contribute novel ways to make

sense of changing patterns in politics as it is exposed to networked digital technologies in the modern world.

Acknowledgments

This work was carried out within the project ResisTIC (Les résistants du net. Critique et évasion face à la coercition numérique en Russie, ANR-17-CE26-0020) funded by the French National Agency for Research (ANR), and was also supported by CitizenLab (University of Toronto). We also wish to acknowledge the H2020 NEXTLEAP project (H2020-ICT-2015 – GA nº 688722).

About the Authors

Ksenia Ermoshina is Associate Research Professor at the Center for Internet and Society of the French National Center for Scientific Research (CNRS), Paris, France.
Benjamin Loveluck is Associate Professor in Sociology at i3-SES, Telecom Paris, IP Paris, France.
Francesca Musiani is Associate Research Professor at the Center for Internet and Society of CNRS, Paris, France, and currently serves as its deputy director.

Notes

1. Methodologies for counting the actual number of active ISPs vary. The number of licenses delivered to ISPs was equal to 5950 in 2017. According to a study conducted by ISPs themselves in December 2017, there are 3940 ISPs (https://habr.com/en/post/345258/) while according to RKN numbers, only 3461 ISPs are actively communicating with the regulator in 2018 (https://rkn.gov.ru/news/rsoc/news70316.htm).

2. According to the data provided by our informants from the Society for Protection of the Internet.

3. https://zona.media/article/2019/04/11/avtonom.

4. https://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/.

5. See for example the Electronic Frontier Foundation's reaction to the Yarovaya law: https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

6. Our analysis of procurements (2016–2018), using the "SORM" keyword, is based on the open data from "goszakupki.ru", a website that publishes tender procedures and results for government procurements.

7. RGGU stands for Russian State University of Humanities. According to Russian legislation, public universities are also required to install SORM equipment through government procurement procedure.

8. KROS (https://cros.nag.ru/), the Conference of Russian Telecommunications Operators, is the largest professional gathering of ISPs, equipment vendors, policy makers, lawyers and regulatory agencies.

9. Source: ZaTelecom, Telegram channel dedicated to analyzing Russian telecommunication industry, managed by the director of the Society for Protection of the Internet, Mikhail Klimarev. Published on 25 May 2017 at 10:04. https://t.me/zatelecom/192.

10. Source: Telegram channel OrderCom, April 19, 2018, https://t.me/ordercomru/179.

11. Sky_lord, "The scary and terrible SORM: a bit of practice", August 1, 2009, https://habr.com/post/65924/.

12. RBC, 9 November 2011, https://www.rbc.ru/technology_and_media/09/11/2017/5a03187e9a7947d88f988f53.

13. Source: OrderCom Telegram channel, 30 May 2018, https://t.me/ordercomru/111.

14. A-record maps a domain name to the IP address of the computer hosting the domain, and is used to find the IP address of a computer connected to the internet from a name.

15. https://tjournal.ru/46700-moshkov-minjust.

16. See https://tools.ietf.org/html/rfc7725.

17. In DNS blocking, if an IP address of a requested site is on a block list, instead of returning the valid IP address, the DNS replies that the domain is unknown, or directs to a different IP address and eventually a page stating that the requested domain is not permitted. In proxy filtering, a proxy server (a machine acting as an intermediary between the user and the Internet) runs every site request through a filter, looking up each address in its database of allowed or disallowed sites, and allows or blocks each request based on its internal database. In IP blocking, a network service is configured so that requests from hosts with certain IP addresses are rejected. DPI allows a third party to inspect data packets circulating on the Internet (usually looking at the IP header of each packet), a technique which can be used both for ordinary network management purposes and for censorship and surveillance.

18. Nag.ru forum, accessed 4 May 2019, https://forum.nag.ru/index.php?/topic/79886-blokirovka-saytov-provayderami/.

19. ccording to an investigation by ValdikSS, a hacker and activist connected to RosKomSvoboda who conducted a detailed analysis of and retro-engineered the AS Revizor box https://habr.com/ru/post/282087/.

20. See e.g. https://www.znak.com/2019-10-12/v_rossii_ne_rabotaet_sistema_kontrolya_za_blokirovkoy_zaprechennyh_saytov_vnedrennaya_rkn We also observed dozens of complaints on numerous bugs and outages of the Revizor system in Telegram chats of ISPs.

21. http://www.rkn.gov.ru/communication/p922.

22. In April 2018, RKN ordered to block the popular Telegram messaging service and prompted a movement for the defense of Telegram, including the rise or "creative deployment" of

obfuscation and circumvention protocols, proxies and VPNs designed by users and the Telegram team itself, to bypass governmental censorship. The ban was eventually lifted by RKN in June 2020.

23. http://telegra.ph/Kogda-sudy-otkazyvayut-v-priznanii-informacii-nezakonnoj-04-27.

24. https://www.rbc.ru/newspaper/2017/11/09/5a03187e9a7947d88f988f53.

25. Interview, ISP from Saint-Petersburg, 19 February 2020.

26. Interview, CEO of a large regional ISP, Saint-Petersburg, 20 August 20 2019.

27. http://www.consultant.ru/document/cons_doc_LAW_349660/.

28. See the list of resources https://filearchive.cnews.ru/img/news/2020/04/07/spisok33.pdf.

29.
Source: https://www.rbc.ru/technology_and_media/08/04/2020/5e8cbae99a7947abc1b50793.

30. https://www.themoscowtimes.com/2018/11/16/russia-stifled-mobile-network-during-protests-a63523.

31. https://netblocks.org/reports/evidence-of-internet-disruptions-in-russia-during-moscow-opposition-protests-XADErzBg.

32. Russian NGO focused on research and analysis of the quality of Internet service in Russia, led mainly by technologists and lawyers.

33. Interview, ex-CTO of an Internet Exchange Point (IXP) in Saint-Petersburg, 18 November 2019.

References

1. Akrich, M. (1992). The de-scription of technical objects. In W. Bijker & J. Law (Eds.), *Shaping technology/building society. Studies in sociotechnical change* (pp. 205–224). Cambridge, MA and London: MIT Press.
2. Ball, S., & Snider, L. (Eds.). (2013). *The surveillance-industrial complex. A political economy of surveillance*. London: Routledge.
3. Callon, M. (2013). Qu'est-ce qu'un agencement marchand? In M. Callon et al. (Eds.), *Sociologie des agencements marchands. Textes choisis* (pp. 325–440). Paris, France: Presses des Mines.
4. Clark, J., Faris, R., Morrison-Westphal, R., Noman, H., Tilton, C., & Zittrain, J. (2017). *The shifting landscape of global internet censorship*. Cambridge, MA: Berkman Klein Center for Internet & Society Research Publication.
5. Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds..), (2010). *Access controlled. The shaping of power, rights, and rule in cyberspace*. Cambridge, MA and London: MIT Press.
6. DeNardis, L. (2012). Hidden levers of Internet control. An infrastructure-based theory of Internet governance. *Information, Communication & Society*, 15(5), 720–738. doi:10.1080/1369118X.2012.
7. DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press.

8. Denisova, A. (2017). Democracy, protest and public sphere in Russia after the 2011–2012 anti-government protests: Digital media at stake. *Media, Culture & Society*, 39(7), 976–994. doi:10.1177/0163443716682075

9. Edwards, P. N., Bowker, G. C., Jackson, S. J., & Williams, R. (2009). Introduction: An agenda for infrastructure studies. *Journal of the Association for Information Systems*, 10(5), 364–374. doi:10.17705/1jais.00200

10. Ermoshina, K., & Musiani, F. (2017). Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era. *Media and Communication*, 5(1), 42–53. doi:10.17645/mac.v5i1.816

11. Geiger, S., Harrison, D., Kjellberg, H., & Mallard, A. (2014). *Concerned markets. Economic ordering for multiple values*. Cheltenham: Edward Elgar.

12. Gelman, V. (2010). The Dynamics of Subnational Authoritarianism (Russia in Comparative Perspective). *Russian Politics & Law*,48(2), 7–26.

13. Haggerty, K. D., & Ericson, R. V. (2006). *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

14. Konradova, N., & Schmidt, H. (2014). From the utopia of autonomy to a political battlefield: Towards a history of the "Russian Internet". In M. S. Gorham, I. Lunde, & M. Paulsen (Eds.), *Digital Russia. The language, culture and politics of new media communication* (pp. 34–44). London: Routledge.

15. Lessig, L. (2006). *Code: Version 2.0*. New York, NY: Basic Books.

16. Lyon, D. (2001). *Surveillance society. Monitoring everyday life*. Buckingham: Open University Press.

17. Lyon, D. (2015). *Surveillance after Snowden*. Cambridge and Malden, MA: Polity Press.

18. Marx, G. T. (2016). *Windows into the soul. surveillance and society in an age of high technology*. Chicago, IL and London: University of Chicago Press.

19. Mosco, V. (2009). *The political economy of communication. rethinking and renewal* (2nd ed.). London, Thousand Oaks, CA and New Delhi: Sage.

20. Muniesa, F., Millo, Y., & Callon, M. (2007). An introduction to market devices. In M. Callon, Y. Millo, & F. Muniesa (Eds.), *Market devices* (pp. 1–12). Malden, MA and Oxford: Blackwell/The Sociological Review.

21. Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (Eds.). (2016). *The turn to infrastructure in Internet governance*. Basingstoke: Palgrave Macmillan.

22. Nocetti, J. (2015). Russia's 'dictatorship-of-the-law' approach to internet policy. *Internet Policy Review*, 4(4). doi:10.14763/2015.4.

23. Oates, S. (2013). *Revolution stalled. The political limits of the internet in the post-soviet sphere*. Oxford: Oxford University Press.

24. Schneier, B. (2003). *Beyond fear. Thinking sensibly about security in an uncertain world*. New York, NY: Copernicus Books.

25. Sivetc, L. (2020). The blacklisting mechanism: New-school regulation of online expression and its technological challenges. In M. Wijermars & K. Lehtisaari (Eds.), *Freedom of expression in Russia's new mediasphere* (pp. 39–56). Abingdon: Routledge.

26. Soldatov, A., & Borogan, I. (2015). *The red web: The Kremlin's wars on the Internet*. New York, NY: Public Affairs.

27. Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, 43(3), 377–391. doi:10.1177/00027649921955326

28. Tréguer, F. (2019). Seeing like big tech: Security assemblages, technology, and the future of state bureaucracy. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics. Worlds, subjects, rights* (pp. 145–162). London: Routledge.

29. Winseck, D. (2017). The geopolitical economy of the internet infrastructure. *Journal of Information Policy*, 7, 228–267. doi:10.5325/jinfopoli.7.2017.0228

Appendix

Non-exhaustive list of relevant forums and chats analyzed for this research:

1. IP News Forum (http://ip-news.ru/forum/) – professional news website and forum created in 2009, focused on Internet and telecommunication services mostly in Saint-Petersburg and its region. The forum has been actively used since 2009, now in decline but still alive, and counts 4723 users. Among other topics relevant for this research: sales of small ISPs, reforms of legislation, local networks and their evolution, "rumors" of telecom, agreements between providers, etc.

2. Nag.Ru (https://nag.ru/) – the oldest news website and forum focused on the Internet and telecommunication industry, created in 2001. The project is financed by Nag, Russian company producing various kinds of equipment for ISPs (from cables to switchers, commutators and servers). The forum (https://forum.nag.ru) counts 95042 users as of 25 June 2020. The Nag community is active, they organize an annual gathering of providers (KROS) and also own an online marketplace for sales and exchange of the telecommunication circuits. Nag.Ru Telegram channel and chat (https://t.me/nag_public; https://t.me/NR_Politota) where many informal discussions about SORM and filtering equipment take place, were also part of our corpus.

3. Telegram channel "ZaTelecom" (https://t.me/zatelecom) – one of the most popular dedicated blogs on Telegram that focuses on telecommunication and Internet infrastructures, regulation, market analysis.

4. Telegram channel "OrderCom" (https://t.me/ordercomru) – legal project defending ISPs in court; information on regulation, news of the industry, court hearings.

5. Telegram channel "IT and SORM" (https://t.me/itsorm) – the most popular blog covering issues of Internet regulation in Russia; critical perspective on RuNet governance, news of the telecom market, analytics and investigation including reverse engineering of government-made software and malware analysis.

6. Website (http://roskomsvoboda.org) and Telegram channel (https://t.me/roskomsvoboda) of RosKomSvoboda – Russian NGO focused on defense of Internet Freedom and digital rights; monitors blacklists (list of blocked websites) and collects data on censorship and surveillance.

7. Website (https://usher2.club) and Telegram channel (https://t.me/usher2) of Usher2 Club – a project focused on monitoring blocked IPs and analysis of the consequences of regulation on the RuNet. Usher2 has become one of the crucial resources for the so-called "DNS guerilla".