8

Circumventing the "Sovereignization" of the Russian Internet

Toward an Infrastructure-Based Sociology of Digital Sovereignty and Its Resistances in Russia

Olga Bronnikova, Françoise Daucé, Ksenia Ermoshina, Valéry Kossov, Benjamin Loveluck, Francesca Musiani, Bella Ostromooukhova, Perrine Poupin, and Anna Zaytseva

8.1 INTRODUCTION

In the first decade of the twenty-first century, characterized by relatively high levels of freedom in digital innovation, the technical constraints on the construction of the Russian Internet (RuNet) have remained mostly invisible to its users (Deibert & Rohozinski, 2010). However, since the early 2010s, the increasingly strict regulations imposed by the government have made these aspects more evident (Oates, 2013; Soldatov & Borogan, 2015; Gritsenko, Wijermars, & Kopotev, 2021). In particular, Roskomnadzor (RKN), the federal government communications control body,[1] has seen its jurisdiction and reach rapidly extended to domains as varied as the control of online content, the right to block websites, and the registering of blocked websites, with a substantially increased possibility of censorship. RKN's control relies on its important nexus of relations and collaborations with actors that maintain and keep the internet operational and propose connectivity solutions to users including access providers and owners of digital businesses.

This scenario has led to a particular and Russia-specific instantiation of the "digital sovereignty" label, which has taken hold in the past decade, not only offering a telling example of how state-centric formations of digital sovereignty may be structured, but also highlighting the limits of such model, showing how it might be challenged by grassroot initiatives. In this regard, the Russian context illustrates the tension between two types of digital sovereignty as outlined in the introduction to this book: state-centered digital sovereignty and "personal" digital sovereignty struggles as a response to the increasing constraints on digital and civil liberties imposed by the State. Indeed, Russian

[1] RKN is also the data protection regulator in the country; it is not an independent authority, but a governmental agency (federal service) established under the Ministry of ICTs and Media.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

authorities are actively pursuing a digital sovereignty strategy that focuses on an autonomization and "sovereignization" of the RuNet through the adoption of new laws to counter foreign influences and agents, as well as their devices and applications. Exemplars of this tendency are what have become known as the *Sovereign Internet Law*, adopted in 2019 with the official aim of protecting the country from cyberattacks, and the *law against Apple*, passed in 2020 with the objective of having all smartphone devices in Russia to preload a host of "Russian-made" applications (Musiani et al., 2019).

In this context, since 2018, the *ResisTIC (Criticism and circumvention of digital borders in Russia)*[2] project team endeavors to analyze how different actors of the RuNet resist and adapt to the recent wave of the so-called authoritarian and centralizing regulations, with a particular focus on online resistance that reveals so far lesser-known social practices and techniques for circumventing online constraints. These circumventions expose the limits of what the introductory chapter to this volume considers as state digital sovereignty and the underlying tensions that this type of digital sovereignty inevitably unleashes against competing forms of individual digital sovereignty, echoing a long history of social inventiveness in the last decades of the Soviet period when many Soviet citizens routinely transgressed and reinterpreted the norms and rules of the socialist state (Yurchak, 2013). These "arts de faire" were notably visible in their use of communication infrastructures (Zakharova, 2020).[3] They are also in line with the protests that emerged after the demise of the USSR. Since the 1990s, Russian society has been neither apathetic nor resigned, as shown by the local mobilizations contributing to the development of citizen activism (Kleman, et al., 2010) or the large demonstrations against electoral fraud in 2011 and 2012 (Gabowitsch, 2016).

One of the project's primary objectives is to explore the extent to which control and circumvention strategies are embedded in and conducted by means of the infrastructure of the RuNet; our aim has been to shed light on the complex relationship between technical devices and algorithms (Brousseau, Marzouki, & Méadel, 2012; Musiani, 2013) in the Russian digital sphere, and the politics and markets taking shape in the country. As the project moves toward its conclusion (June 2022), this chapter proposes to take stock of the project's different fieldworks and insights concerning the theme of this book, at the crossroads of digital sovereignty, data, and infrastructure – both its development and its uses, oftentimes very creative and subversive. Beyond the Russian case,

[2] Our project website is www.resistic.fr.

[3] Zakharova (2020) recalls that postal mail in the USSR was the dominant mode of communication in Soviet society until the late 1970s. However, letters were heavily monitored and censorship agents enforced random checking of mail as well as the control of foreign correspondence. The population adapted by moderating its speech, but also by developing parallel distribution channels, through railway employees for example, or by using diplomatic mail from foreign states to contact relatives outside the Soviet borders.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

understood as a "laboratory" of broader tendencies in internet governance worldwide, the project seeks to contribute to a conceptualization of the changing patterns in politics as it is exposed to information and communication technology (ICT) in the modern world.

The chapter undertakes an infrastructure-based sociology of the RuNet, focusing on the technical devices and assets involved in surveillance and censorship, and on the strategies of resistance and circumvention "by infrastructure" that follow. In the tradition of Science and Technology Studies (STS), we understand the "infrastructural" quality of the network of networks, and its multitude of physical and logical apparatuses, as relational and conditional; infrastructures can be more usefully understood in terms of function than form. Thus, beyond objects whose infrastructural aspect is immediately obvious, such as bridges or pipes, a number of artifacts and entities that populate and shape the network of networks could be described as infrastructure because they have an infrastructural *function* – because they help to structure, shape, enable, or constrain our "being-together" on and with the internet. In this sense, internet infrastructures include physical objects, for example, submarine cables that carry global telecommunications or data centers that host our digital content, and objects that are a priori much less concrete, such as internet protocols, applications, and software (see, e.g., Musiani, 2018 for further discussion of this point).

The analyses presented in the chapter are based on original data, both quantitative and qualitative (interviews and observations on the field). In addition to the presentation of the case studies, a recurring point of interest is a reflexive assessment of our methods, in particular those related to field survey, which can be problematic and sensitive in Russia because of the constraints on researchers and the protection of interviewees, but is extremely useful as it allows to question the preconceptions attached to the RuNet and renew our understanding of the role of infrastructure in digital control and circumvention.

The empirical core of the chapter will provide an overview of a number of studies undertaken by the ResisTIC project team in the past few years. While the presentation of the case studies will, by necessity, be relatively brief, presenting them together will allow to draw some general conclusions about the state of infrastructure-based digital sovereignization in Russia; interested readers will be able to delve deeper into the case studies by means of a special issue of the open access First Monday journal (Daucé & Musiani, 2021).

Before we delve into the case studies, however, we seek to outline the particular relationship that exists in Russia between law and infrastructure as means of control, as it has taken shape in the past few years. In response to the Russian government's increasingly coercive grip, direct political confrontation is difficult and risky; thus, we argue that the use of infrastructure is a way to indirectly bypass constraints and coercion. A number of dynamic behaviors, which can be qualified as infrastructure-based ruse and resistance, have emerged in close response to legislation. Russian "digital

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

resisters" adapt to new laws and invent new techno-legal tweaks that challenge the Russian lawmaker. Understanding this dialectic is of vital importance to understand the context in which the initiatives described below, between promotion of and resistance to digital sovereignty by means of infrastructure, take place.

8.2 THE RELATIONSHIP BETWEEN LAW AND INFRASTRUCTURE IN RUSSIAN DIGITAL SOVEREIGNTY STRATEGIES

The regulation of internet infrastructure began in a firm manner since 2012 with new laws such as 139 FZ,[4] which establishes a legal framework for the system of filtering websites included in the "blacklist" of digital resources, whose illicit nature may be defined by various state institutions. This law introduces a new relationship between the infrastructure providers and the state. Indeed, the law obliges internet service providers (ISPs) to inform site owners of the need to remove pages with illegal information or to block access to sites listed in the register prepared by RKN. Initially, the law prohibits content relating to child pornography, suicide, or drug use. However, the new Law 398 FZ extends blocking practices to the sites calling for unauthorized public protest actions considered "acts of extremism"[5]; for example, media such as Grani.org were banned on Russian territory for their publications dedicated to actions in support of the people prosecuted for participating in political protests on Bolotnaya Square in 2012. The prosecutor's office also deemed Kasparov.ru's website as "extremist," in an article related to the annexation of Crimea. Since March 2014, "nonsystem" political opposition sites[6] have been blocked under the law.

These blocking attempts, as well as RKN's "manual" control of ISPs – that is, the case-by-case verification of the blocking of prohibited sites – have proven to be ineffective. From 2015, RKN is therefore imposing Revizor boxes on operators, which automatically check whether prohibited resources have been blocked by ISPs. The new monitoring system entails additional costs for ISPs due to installation of hardware and software components and the high fines for noncompliance to the law (Stadnik, 2021). The web community is responding to blocking practices with the increasingly common use of virtual private networks (VPNs) or Tor software, dynamic IP addresses, and mirror sites.

[4] Federal Law 139-FZ of July 28, 2012 "On Amendments to the Federal Law on the Protection of Children from Information Harmful to Their Health and Development and to Certain Legislative Acts of the Russian Federation."

[5] Federal Law 398-FZ of December 28, 2013 "On Amendments to the Federal Law on Information, Information Technology and Information Protection."

[6] A variety of political groups dissatisfied with the actual regime, and not represented in official bodies at the federal and regional levels.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

In parallel with these information control practices, the Russian authorities are attempting to regulate the RuNet by law, targeting its infrastructure more directly. On July 21, 2014, the President signed Law 242 FZ,[7] which requires private internet players to store the personal data of Russian users on servers physically located on Russian territory. The Law 531 FZ[8] prescribes the hosting on Russian territory of all sites of Russian public authorities. These measures are justified by the need for data security for the population and the State in a tense international context linked, *inter alia*, to the conflict with Ukraine, and to a broader context in which cyberattacks from Russia to US, and vice-versa, happen on a regular basis (Sanger & Perlroth, 2019) and, to some extent, the need for a RuNet is seen by the Russian government as a cybersecurity strategy. Ultimately, the application of the law 242 FZ has been postponed until October 30, 2022.

The trend of repatriation of digital resources and data continues with the so-called Yarovaya Law 374 FZ.[9] This time the legislator modifies the nature and quantity of data that would be controlled by the state in the context of the fight against terrorism. Indeed, the law obliges operators to store telephone conversations, SMS, videos, and emails of users for a period ranging from 30 days to 6 months. The encryption keys must be made available to security services upon request. Given the significant cost to operators, it was expected that their storage capacity would increase by 15% annually. However, the application of this rule was temporarily suspended in 2020 because of the pandemic, which caused an explosion in the number of video and other content exchanges, making it impossible to store such a large volume of data (Peškova, 2020).

All this legislation aimed at territorializing infrastructure of the RuNet finds a general framework in the Doctrine of Information Security (Presidency of the Russian Federation, 2016). This document provides definitions of critical infrastructures, emphasizing the territorial anchoring of information systems and communication networks.

The Doctrine gave rise to the Law 90 FZ called "on the Sovereign Internet," which came into force on November 1, 2019. Indeed, it takes up the notion of sovereignty of the Russian digital space and tasks the government with ensuring the stable functioning of its critical infrastructure by taking control

[7] Federal Law Concerning the Introduction of Amendments to Certain Legislative Acts of the Russian Federation to Clarify the Procedure for Processing Personal Data in Information and Telecommunication Networks.

[8] Federal Law 531-FZ of December 31, 2014 "On Amendments to Articles 13 and 14 of the Federal Law on Information, Information Technologies and Information Protection and to the Code of Administrative Offences of the Russian Federation."

[9] Federal Law 374-FZ of July 6, 2016 "On Amendments to the Federal Law 'On Combating Terrorism' and to Certain Legislative Acts of the Russian Federation with Regard to Establishing Additional Measures to Counter Terrorism and Ensure Public Safety." The law borrows the name of its sponsor, Russian MP Irina Yarovaya.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

of the traffic exchange points, all autonomous systems and the system of national domains ru. and рф. The law also provides for the establishment of state control over cross-border traffic by the infrastructure that will ensure network routing in case of the impossibility of connection to foreign servers. In addition, it requires ISPs to install Deep Packet Inspection (DPI) filtering equipment. RKN has been given the power to set routing policy for ISPs and to ensure centralized network management. To this end, tests were planned to simulate the situation where RuNet would be disconnected from the external network. However, after a first test in December 2019, others were canceled in 2020, officially due to the pandemic. In January 2021, the Ministry of Digital Development announced that the final plan for the exercises would be decided after the end of the pandemic (Pâtin, 2021). In contrast, COVID-19 did not become an obstacle for Twitter throttling in 2021,[10] which was done with the use of DPI equipment. Furthermore, the pandemic did not prevent the passage of Law 19 FZ, which holds operators accountable for not installing DPI equipment.[11]

The process of RuNet sovereignization continues to develop according to the guidelines of the Information Security Doctrine, with Law 425 FZ mandating foreign hardware manufacturers to preinstall Russian software on electronic devices sold in Russia from April 1, 2021 (Presidency of the Russian Federation, 2016, art. IV, sect. 23, par. 3). The so-called "anti-Apple" law has been met with an unfavorable response from other major computer brands including Microsoft and Intel. However, even the most resistant, such as Apple, have found a compromise with the government: Russian applications are proposed as opt-in mechanism for the device buyer, without the device manufacturer preinstalling them (Kodačigov, 2021).

The adoption of new laws regulating the internet infrastructure reduces opportunities of circumvention for digital companies, the media, NGOs, and simple users. However, the digital ecosystem is organizing itself to cope with the constraints of the legislation. First, there are legal means such as appeals against court decisions or even legal recourse against RKN decisions. Second, the RuNet community continues to seek for technical solutions to adapt to restrictive rules. Finally, the proliferation of punitive laws and the high rate of their adoption are turning against the state, which is failing to enforce them in a regular and systematic manner throughout the Russian territory. This diminishes the effectiveness of the law and leads to the slowing down of the sovereignization process.

[10] RKN started throttling Twitter in Russia on March 10, 2021. The agency explained it by the fact that the social network does not respond to requests to remove "illegal content": appeals to suicide, extremist materials, child pornography, information about drugs. On May 17, RKN decided to remove access restrictions on desktop terminals, keeping Twitter traffic slowed down on mobile devices. See Roskomnadzor (2021).

[11] Federal Law 19-FZ of February 24, 2021 "On Amendments to the Code of Administrative Offences of the Russian Federation."

8.3 SOVEREIGNIZATION AND RESISTANCE "BY INFRASTRUCTURE" IN THE RUNET: INSIGHTS FROM THE FIELD

We now turn to the empirical core of the chapter, which provides an overview of a number of studies undertaken by the ResisTIC project team in the past few years. We focus on both the technical devices and assets involved in sovereignization processes, and the strategies of resistance and circumvention "by infrastructure" that follow.

8.3.1 "Black Boxes" and Strategies of Internet Service Providers

One of the key levers of control over the RuNet is the legal framework targeting ISPs. These private technical intermediaries ensure the routing of internet traffic toward end users, and in Russia, they represent a vibrant and diverse market with many actors of different sizes, providing an overall good quality of service. Digital sovereignty policies regarding ISPs seek to achieve two main objectives: enabling surveillance of the traffic and ensuring compliance with censorship regulation. Moreover, the technical solutions to cater for these regulations need to be "made in Russia." A domestic industry of surveillance and censorship has thus flourished, which affects the ISP market in different ways.

We explored this industry through a two-year fieldwork in 2017–2019, including in-depth interviews with ISP representatives, a web-ethnography of ISP forums and chats, and a content analysis of professional documentation (Ermoshina, Loveluck, & Musiani, 2022). Our research focused on the vendors of surveillance and censorship solutions and on the "black boxes" known as "middleboxes," which ISPs must implement on their infrastructures: actual physical boxes that are plugged on the network, but also software solutions and distributed technical devices and equipment. By drawing on both STS and the political economy of information and communication networks, we sought to understand their functioning and the ambiguities and controversies they generate, as well as assessing the liabilities, technical impediments, and economic costs that weigh on ISPs, and the strategies they devise in order to circumvent them or negotiate compromises.

We focused on two types of "black boxes" that ISPs need to embed within their infrastructure. The first one is known as SORM (System for Operative Investigative Activities), and it is used to collect and store metadata and internet traffic, which must be made available to the authorities upon request as lawful interception. Though SORM must be installed at the ISP's expense, it is controlled by the FSB (the Russian Federal Security Service) via a terminal and can be accessed by other agencies and police departments (tax, customs, border police, etc.). SORM-1 was set up in 1995 for wiretapping and phone surveillance, before adapting to the internet in 1998 as SORM-2, and it has evolved

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

several times since then. The latest iteration was defined by the "Yarovaya" 374-FZ4 and 375-FZ laws passed in 2016 (and somewhat loosened in 2018): the law now requires all telecom providers to store metadata for 3 years and content such as data, voice calls, images, and text messages for 30 days. The hefty costs of this system and the long delays in specifying the certifications have drawn criticism on the part of ISPs – who must choose between various expensive solutions, are never completely sure they are complying with the regulation, and may also face legal responsibilities in the case of data breaches. Indeed, not only are there different ways of conforming to the regulation, but misconfigurations of SORM are also common. Moreover, requirements are different according to ISP size and to mitigate these different risks, various strategies are adopted such as sharing solutions between ISPs or even buying already "SORMed" traffic from bigger actors. Finally, SORM is contested not only because it is costly but also because it involves cumbersome compatibility issues with existing ISP infrastructures, because most of the stored traffic is encrypted and therefore unusable, and because the FSB often uses other ways to access specific information. It is said to mainly benefit a small number of firms who have gained quasi-monopolistic positions on the market, and who benefit from existing ties with the Defense sector.

The second type of "black box" we focused on is the solution needed to filter the traffic and make it "RKN-compliant" – blocking any website that RKN (Roskomnadzor, the Russian federal executive body responsible for media and telecommunications) has added to its "black list" of banned websites. Although ISPs previously received blocking requests on a case-by-case basis, a centralized list was set up in 2012 after the protests against electoral fraud, and was further expanded especially after the Ukrainian crisis in 2014. There is no unique "law on censorship" however, but many existing laws that have been amended to include responsibility for publishing "illegal" content. This category is only vaguely defined and decisions to ban content are made with no oversight, paving the way for politically motivated suppressions.[12] Moreover, precise requirements such as standardized "blockpages" and guidelines for traffic filtering were only issued in 2018. Prior to that, vulnerabilities in the mechanism meant that activists could leverage DNS-based "guerilla" tactics to block other websites – including at one point the Ministry of Justice main website – as a sign of protest. With no standardized blockpages, these could also be used by ISPs to criticize censorship and promote circumvention tools such as VPNs. Today, there are still different available methods for blocking websites, which range from homemade scripts to hardware devices, cloud-based solutions, and DPI-blocking software, but attempts have been made to standardize the blocking procedures. And with an increasingly voluminous

[12] In June 2020, the European Court of Human Rights has delivered multiple judgments stressing the incompatibility of the Russia take-down system with the ECHR. See, for example, Grover and Thomas (2021).

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

blocklist, cobbled-up solutions have gradually become increasingly difficult to maintain. Nevertheless, ISPs still actively seek to avoid complying completely with censorship – in order to reduce their costs but also to remain attractive to their clients. Some even engage in selective censorship or try to fool the system in various ways, such as blockpages or the so-called "DNS guerillas" (see Ermoshina, Loveluck, & Musiani, 2022).

Both SORM and RKN-compliance must be implemented if ISPs want to avoid being fined. However, none of them are standardized and the certification processes are lengthy. ISPs therefore often find themselves in uncharted waters, where they must *interpret* these requirements and often experiment in order to find a balance among imprecise (yet strict) rules, technical feasibility, and economic costs. These gray areas present strong uncertainties for ISPs but also opportunities. Our research shows that along with ethical and political concerns, Russian surveillance and censorship policies generate inefficiency and potential corruption of the market and affect the overall topology of the RuNet. However, we also highlight that ISPs develop different forms of technical, legal, economic, and sometimes political resistance. Far from a vertical, centralized, and all-powerful model of State control, the regulation of surveillance and censorship shows that control – though burdensome – is only partial, often inefficient and fraught with contradictions, opening up spaces for resistance and evasion.

8.3.2 The "Telegram Ban": RuNet between Infrastructural Dependency and Resistance

These resistance tactics of both technical experts and users have become especially visible through the case of the "Telegram ban," a two-year long attempt by RKN to block one of the most famous messaging applications in Russia. The "Telegram ban" should be approached as a sociotechnical controversy that unveils the close dependencies of RuNet *vis-à-vis* global internet infrastructures. Indeed, this case questions both technical and geopolitical boundaries as it opposes the strong government-originated discourse on the Russian "Sovereign Internet" (Freiberg, 2014) and the transnational character of material internet infrastructures. This "Telegram ban" favors a better understanding of both the threat of balkanization of the internet and the "turn to infrastructure" (Musiani et al., 2016) in RuNet governance, as it makes visible the ensemble of sociotechnical and legal mechanisms used to exercise control over RuNet.

Created in 2013 by the Durov brothers, Telegram fell under scrutiny of the Russian political police in the space of a few years: on July 14, 2017, the Russian FSB requested decryption keys for all messages sent and received via Telegram, in accordance with the 2016-approved Yarovaya Law. Telegram did not satisfy the FSB's request, and after a second request to provide the keys in March 2018, Telegram's lawyers explained that it was

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

cryptographically impossible because of the way in which encryption works in Telegram. In response, on April 16, 2018, Telegram was officially blocked by RKN. However, Telegram was never completely blocked on the territory of the Russian Federation. Users could access all of its services rather easily – sometimes even without any circumvention tools because small and medium ISPs did not always comply with RKN's requirements to block the app. This inability of governmental agencies to successfully block Telegram raised concerns as to the efficiency of RKN and technical expertise of its employees.

This trust in Telegram, according to our interviews (see also Maréchal, 2018), lies not so much with the technology, but with its main developer, Pavel Durov, his reputation, and his political position. Indeed, Telegram became so influential in Russia that governmental institutions kept maintaining their own official Telegram channels, probably so as to maintain some kind of influence within this platform. Interestingly, and ironically, the Russian government itself kept on using Telegram as one of its primary means for official communications during the COVID-19 pandemic, despite the fact that the tool was still officially blocked until June 2020. As the official Telegram statistics show, Telegram's Russian audience has doubled since 2018 and the ban did not impact this growth.

Telegram has attracted tech user communities that have chosen it as their primary messenger, not only for daily one-to-one communication but also for professional chats. Telegram's API has engendered a dynamic user-driven development of the bot and bridge ecosystem that made Telegram something "bigger than just a messenger, a new kind of social network" – as one of our respondents puts it. Telegram has evolved into a hybrid network with multiple functions and purposes, offering shelter to censored media using Telegram as a circumvention tool to deliver content to their audiences, allowing public group chats and proposing tools to promote cultural and political events and gatherings, organize surveys, create and distribute cultural and artistic content, generate stickers, and process payments.

There is no single history of the Telegram ban, but several ways to tell this story, competing chronologies and narratives that trace it back to different moments in the history of the RuNet – itself a rather controversial one. The defenders of Telegram do not interpret the ban as an isolated case but analyze it in a broader context of "the war on RuNet," while pro-governmental media, on their end, frame the Telegram ban as "the (legitimate) war on terrorism." The difference in framing strategies unveils how an instant messenger becomes in itself an instrument used to build and distribute concurrent political narratives about what RuNet has been and how it should function in the future. The Telegram ban crystallizes two competing paradigms: the one mourning RuNet's "Golden Age," based on free competition and cooperation between tech professionals, absence of censorship and centralized regulation, transnational circulation of tools, services, and people; and the other that affirms the necessity of stronger, infrastructure-driven control of RuNet's

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

"borders" and content production and circulation. Both paradigms include a third party: the complex network of foreign, mostly US-made, services such as Google or Amazon Web Servers that actually become crucial for the functioning and well-being of RuNet. While the Telegram ban unveils these fundamental dependencies on foreign infrastructures, it paradoxically becomes the trigger for faster "sovereignization" – the relocalization of servers, data, and services – of the Russian segment of the global network.

Indeed, the very circumvention mechanisms used by Telegram (such as IP hopping) relied on Amazon and Google Web servers to temporarily host the elusive messenger. Access restrictions to Telegram were extended to all third parties providing infrastructural support for the infamous messenger. In April 2018, eighteen million IP addresses were blocked, including hundreds of IPs of Amazon, Google, and other major web services. This method, dubbed by Telegram defenders as "carpet blocking," turned out to be quite inefficient: only 18 IP addresses out of three million blocked Amazon addresses were actually used by Telegram.

Collateral damages caused by these blockings had an important effect on the politicization of particular segments of RuNet users (e.g., small entrepreneurs whose websites were accidentally blocked). These new "concerned publics" (Geiger et al., 2014) were either involved into collective action or engaged into usage and understanding of circumvention technologies. Researchers have observed a wider adoption of privacy-enhancing technologies and circumvention tools such as VPN and Tor. A vibrant market of proxies for Telegram developed, while popular opposition media helped raise user awareness about internet censorship and circumvention.

During the first months of The Telegram ban, tech activists developed a new repertoire of contention (Tilly, 2002) ranging from disobedience (ISPs using various tricks to avoid blocking Telegram) to hacktivist actions. The Telegram ban also led to a rise of offline activism focused on internet freedom. A wave of demonstrations "For Telegram" took place across the country. The instant messenger became, at least for Spring and Summer 2018, a contextual point of unity for various anti-governmental movements.

Telegram was officially unbanned in June 2020, for two main reasons explained by the Ministry of Communication: first, the "technical impossibility" to effectively block it, and second, because Telegram has agreed to block specific channels related to drug sale or terrorism; a less-official but no less important reason was the need to share information via governmental channels during the COVID-19 pandemic. While the outcome of the battle for Telegram shows the inefficiency of the infrastructural apparatus and of the censorship methods used by RKN, there are indications that the Russian authorities, RKN in particular, may also have learned some lessons from the case, in terms of how they could adapt their "sovereignization" strategies by being more "hybrid" and acting at both the infrastructure and content governance levels (buying popular Telegram channels, sponsoring ideological content by their means).

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

8.3.3 Yandex.News, "Official" News Ratings, and Their Circumvention

Russia is one of the very few countries where search is not monopolized by Google, with Yandex owning a share of over 45% – thus making it a prized national champion of the Russian digital economy. Yandex has also developed other services such as Yandex.News, which presents a selection of topics and articles to reflect the themes most widely covered by the media at a given moment. The algorithms deployed by Yandex.News and Google.news can be perceived as an "invisible hand" deciding which topics will be singled out as relevant and which news outlets will be pushed on the forefront according to sometimes unfathomable criteria (Brake, 2017).

The controversies that arose after 2012 in Russia put an end to the belief in the objectivity of the aggregator. Control over the public sphere stepped up again in 2014, during the conflict with Ukraine and the occupation of Crimea. Yandex.News was accused of partiality by the authorities for providing visibility to information that didn't align with the official narrative. This led to the adoption in 2016 of a law on news aggregators, designed to extend control to such intermediaries and specifically targeting Yandex. News. It became legally responsible for any content published in its results (and at risk of heavy fines in case of violations), unless the selected media are officially registered with RKN. As a consequence all non-registered media as well as all foreign media (such as the BBC in Russian, as well as exiled media such as Meduza) disappeared from the Top 5 results. An audit of the aggregation algorithm we conducted in 2020 (Daucé & Loveluck, 2021) strikingly shows the concentration of information on Yandex.News among 14 large media players: public press agencies, state-funded media, leading newspapers, and mainstream online publications. This is a much narrower range than the results observed by Nechushtai and Lewis (2019) in the case of Google News in the US for instance where, although a small selection of 14 outlets also dominated the aggregator, a long tail of other publications also figured in the results.

Media players and news professionals, along with the new hurdles they face, are gradually developing critical views of the role and functioning of platforms and their algorithms – uncovering the political stakes of these key infrastructures. Controversies, regulations, and concentration of information lead to a delegitimation of the algorithm in the eyes of journalists, as well as web professionals and programmers who seek ways to bypass it. Some of them consider the service to be useless. As Lev Gershenzon, the former head of Yandex.News, remarked in 2016: "Aggregators make sense (…) only when there is something to aggregate. If all independent, interesting, professional publications on a federal scale can be counted on the fingers of one hand, rocket technology for their aggregation and processing is not needed – you can simply add them to your bookmarks" (Gershenzon, 2016). The idea of closing the service seems to have been considered by Yandex

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

executives themselves. According to well-known journalist A. Plyushchev, from Ekho Moskvy:

> Well, you know, I once talked to A. Volozh, the head of Yandex, and that was before the law on aggregators was passed. And he told me that if the law was adopted, he would close the service. (…) Well, the law was softened a bit, and the service, as you can see, did not close. I still doubt if that was the right decision. Because, well, I think, unfortunately, the state did everything possible to manipulate both the media and extraction in search engines.[13]

In May 2018, in an open letter to Yandex CEO Yelena Bunina, A. Plyushchev advised her to shut down the Yandex.News service or to rename it Yandex. Propaganda.[14]

However, closing the aggregator is not the only option. Excluded from Yandex's rankings since 2016, independent media carry out dissemination actions on social networks to bypass the aggregator. They have migrated and relocated to other spaces and new types of distribution, disseminating their content on social media such as Facebook, Twitter, Instagram, or Telegram. The example of *Meduza*, a Riga-based online newspaper created by Galina Timchenko after she was fired from the news website Lenta.ru in 2014, is very enlightening here. According to its own metrics, in 2020, traffic came mostly from direct connections and social networks, which is presented as a badge of honor with its traffic being "certified organic." *Meduza* does not obtain any traffic from Yandex.News (compared with Lenta.ru, *Kommersant*, and RBK, which are more dependent on the aggregator). It has an active presence on social networks, which is consistent with the new information practices of the younger generation. Since 2016, a growing gap between how people experience news on Yandex.News and on social networks is noticeable. A media consumption study carried out by the Levada Sociological Center in Russia in February 2020 showed that people over 40 years old get their information mainly from official websites or from television, while younger people (18–39 years old) secure it mostly from social networks.[15]

Another scenario to bypass Yandex.news concerns the creation of an alternative aggregator. In 2019, from abroad, Telegram founder Pavel Durov announced his intention of developing a news aggregator on his platform: "We have a chance to create the first effective and free news aggregator in the history of the Internet," said Durov. "We can start recommending articles from the Recommended Articles block after reading each article in Telegram, gradually bringing it into service with an hourly selection and a global search on all the news in the world" (Eremenko & Brzygalova, 2019). In the context of the

[13] Interview with Aleksandr Plyushchev, Moscow, March 2019.

[14] See https://t.me/PlushevChannel/2533"\t"_blank.

[15] See the study by the Levada Center (2020). These results are coherent with the research on media consumption in Russia done by the audit company Deloitte (2020).

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

failed blocking of Telegram in Russia, P. Durov announced his aggregator will be beyond the control of the Russian security services and political censorship, unlike local operators. He invited Yandex.News developers to participate in the creation of his service and announced a competition to develop an algorithm from the Data Clustering Contest. Its first round took place in spring 2020 and was won by "Mindful Squirrel" (contestants appear on the platform under animal aliases to ensure fairness and transparency in testing). However, according to experts, "Mindful Squirrel" is actually Ilya Gusev, who works as a machine learning engineer at Yandex.News. In this way, the Telegram news aggregator is built on the skills of Yandex engineers, who themselves contribute to the circumvention of the aggregator they work for. This singular case highlights the agentivity of web engineers circulating in a plural technical world where cooperation is possible beyond the opposition displayed between the major internet actors. They thus contribute themselves to the bypassing of the infrastructures they built.

8.3.4 Online Repression of Local Environmental Movements as a "Sovereignization" Process

Processes of circumventing online constraints are also enacted by "ordinary" citizens and activists in far-off Russian regions. We analyzed one of these processes in the frame of a specific case study: citizens have been fighting since July 2018 against a waste landfill project designed to dispose of half a million tons of Moscow waste per year in a swampy area in a remote site called Shies, 1,200 km north of Moscow. A protest camp was set up and maintained to physically preserve the site, joined by people from all over Russia.

Activists do not themselves mobilize the notion of "digital sovereignty." The phenomenon of RuNet sovereignization is, however, a phenomenon whose effects on protest practices are felt on a daily basis. In other words, there are indeed practices of protection among mobilized inhabitants vis-à-vis the state's digital repression and surveillance, but no discourse on sovereignty or sovereignization as such, either to contest it or to appropriate the term, as we see in activist or indigenous movements in other countries (Couture & Toupin, 2019).

If we consider sovereignty as a discourse, a performative action of the state, sovereignty is "a speech act to (re-)establish the claimant's position as absolute authority, and to legitimise its exercise of power" (Werner & de Wilde, 2001). In the Shies case, the question of authority, power, and the rule of law was raised by habitants when they discovered that forest areas had been cut down near Shies and a building site was under construction. The project was started illegally from the point of view of Russian law, that is, without any state ecological, health, and technical expertise, public hearings, or legislative decree. In response to the Shies mobilization, the state did not question the illegal development project; instead, it repressed protest activities, including online ones.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

If the State had forced the project owner to bring the project into conformity with the law, this would have been another form of sovereignization.

The online repressions take place in a political context where uprisings across the Middle East and North Africa (the so-called Arab Spring), Europe (the Indignados in Spain), and the US (the Occupy Wall Street protest) have received a great deal of attention from the Russian government (Nocetti, 2015). Other revolts in post-Soviet countries, such as Ukraine (2013–2014), Armenia (2018), and Belarus (2020), where social media played a prominent role, confirmed this trend. After 2012, the regime started to more closely monitor online media and social platforms. Oligarch Alisher Usmanov's Mail.ru group, with close ties to the Kremlin, bought VKontakte and since, the government has had no difficulty blocking groups or accessing personal data of site users. In this way, Russia develops a strong "data sovereignty," as it attempts to "subject data flows to national jurisdiction [...] with an emphasis on safeguarding national security" (Polatin-Reuben & Wright, 2014: 1). In 2014, with conflict rising in Ukraine, the crackdown against critical voices and opponents in Russia became even greater. Pavel Durov, the VKontakte (the Russia-developed dominant social network in the country) founder, lost control of his company and left the country because of political pressure. Like other local grassroots movements, the Shies one mainly use VKontakte. Activists use it despite the potential privacy and security risks this platform has posed to users since 2014.

The repressive practices against the Shies mobilization can be seen as attempts from the state to reassert its own sovereignty and that of its allies, the private waste sector. Repression related to VKontakte either took place offline, and meticulously documented online by activists in groups, or enacted entirely online. As for the first type, the blockade of fuel transfers and trucks by activists led to conflicts with site guards, with injuries and arrests in the ranks of activists, which in turn led to trials. Other cases of offline repressions documented online were related to the meetings organized by activists. For the second type, repressions were carried out online, or related to the internet directly. They included internet shutdowns at critical moments, seizing activists' audio, video, and computing equipment, blocking, deleting, or hacking groups and personal accounts, and carrying out legal trials based on material related to online groups.

After an initial moment of surprise derived from the first group blockings, the communities devised reaction strategies. At each blocking, a new group was created on VKontakte and activists intensively shared the link with others. Moreover, activists were making clones of VKontakte groups: the contents were copied simultaneously to Telegram and Instagram. A minority of activists exit platforms that implement stricter surveillance regimes and technologies (as VKontakte), moving, for example, to Telegram. But even so, most kept an account on VKontakte. Local activists, as the substantial majority of ordinary citizens, even those who are physically on the front line of local struggles,

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

do not use free software, servers, and encryption-based technologies, as telecommunications, digital, and internet surveillance is the norm and routine for them; further, they do not trust digital services to protect them from privacy threats. They have the belief, inherited from the Soviet times, that “the State knows everything about everyone anyway.”

Protest repression tools are continuously experimenting. Each protest case is an opportunity to test and search for effective technologies to block and filter out critical content and hold trials based on online materials. There is a continuum of the infrastructures and territories that are under the authority of the state and that are subject to a reassertion of power in critical situations: from the classic ones, such as landmass (with the landfill project), to digital content. Faced with repression, activists are learning and using new techniques of circumvention.

8.3.5 Google and US-based Tech Giants as “Recommendable” Tools in RuNet Digital Security Practices

Unlike in other so-called authoritarian regimes (e.g., China and Iran), Google remains legally accessible in Russia and is widely used, including by political leaders and pro-government media. This positions Google as a core actor in negotiations on digital freedoms between authorities and actors of civil society in Russia. Its position is further strengthened by the close dependence of the Russian economy and communication networks on internet giants. Indeed, a strong embeddedness of the Russian internet sector in the global IT ecosystem has been highlighted on several occasions, in particular during the aforementioned blocking of Telegram.

Nevertheless, Google’s relations with Russian authorities are tense. Although the company has been present on the Russian market since 2005, the Russian authorities began to take a close interest in it after the mobilizations in 2011–2012: YouTube was widely used to disseminate evidence of electoral fraud. Several other cases have subsequently set Google against the Russian state, especially following the law on blocking prohibited content in Russia and the localization of data of Russian citizens on Russian territory. But the peak of the tensions was reached in May 2021, when Google was the first of the Big Tech companies in Russia to take legal action against RKN following the latter’s request to remove the links on the demonstrations in support of Alexei Navalny.

In the polarized context of “information warfare,” Western sanctions against Russia and a growing divide between civil liberties activists and the pro-government camp, any regulation of global internet companies, often seen as desirable in liberal regimes, is discredited in the eyes of Russian activists for free internet as synonymous with the internet’s subordination to state surveillance and a threat to freedom of expression. In contrast to their Western colleagues, Google is considered mostly reliable by activists for

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

internet liberties in Russia. This trust is based on the monitoring of Google's Transparency Reports. As noted by a digital security trainer for civil society NGOs in Russia, "*while for countries (...) participating in the 'five eyes' intelligence alliance, 80 to 90% of requests for information from the authorities are met, for Russia these figures represent only a few %.*"[16] This trust is, of course, not exempt from paradox, since Google Transparency Reports are, with some naïveté, considered here as an authoritative source providing a complete picture of what foreign companies may do with the personal data of RuNet users, neglecting both possible and acknowledged biases that do exist in this kind of documents.

Our contacts rely also on their own databases and measurement tools. For example, the "Map of repression on the Internet" (a project of the Internet Protection Society) lists only a few cases related to internet giants,[17] whereas 95% of them concern posts in VKontakte.[18] As to digital security trainers, they draw on their own internal "incident database": very few incidents involving Google services have been relayed in post-Soviet countries.[19]

While not always being deeply concerned about Google's involvement in "surveillance capitalism," internet freedom defenders point out the same phenomenon for Russian technology companies: *"In Russia, there are two logics of surveillance capitalism. On the one hand, companies that want to collect the maximum amount of behavioral data. On the other hand, there are some traditions and logics of citizen surveillance that allow the authorities to perceive this data as their property. The number of actors who can use it is really unlimited."*[20] Despite pointing out that Google has fairly similar commercial strategies in a variety of countries, our respondents nevertheless underline the specificities of the Soviet context, marked by the porosity between public and private spheres and the total distrust in political institutions, which arguably still impact post-Soviet societies (Svenonius & Björklund, 2018). Thus, different experts in digital security for civil security actors understand and convey to their audiences the risks associated with the registration of technology companies in the Russian jurisdiction. Thanks to this positive "publicity" by the expert community, Google is used by multiple civil society organizations and activists in Russia in their everyday work for the usability, security, and efficiency of its various services. Indeed, several of our interlocutors pointed out the danger of "physical infiltration" by malicious people that NGOs are

[16] Interview with I.S., digital security trainer, Minsk, April 2019.

[17] According to our interviewees, these few cases were mainly related to terrorism, hate speech, or telephone fraud. Google would cooperate with the Russian authorities only after eliminating any possibility of its use for repression.

[18] Interview with M.K., coordinator of the "Map of repression on the Internet" (project of the NGO Internet Protection Society), April 8, 2020.

[19] Interview with I.S., April 2019.

[20] A.S. (civic tech ONG), Panel on the regulation of algorithms, conference "Setevoy Sentyabr," September 3–4, 2020.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

facing. Services such as Google Workspace (formerly GSuite) allow differentiated access to data for different NGO employees. In addition, many NGOs cannot afford to hire an IT manager to maintain digital architecture. In this case, the use of open-source solutions appears too difficult to them.[21] This situation of dependency upon Google demonstrates that Russian NGOs have little choice, given the chronic lack of resources and various threats from the Russian authorities.

However, the NGOs dependency upon Google is also due to the role played by the company in the technological assistance to the nonprofit sector. Indeed, while having a reputation for being practical, Google services, such as Google Workspace, are quite expensive for NGOs. Thus, Google, with other Big Tech actors, has partnered with NGOs via its global TechSoup[22] program to provide its services and devices (cloud storage, Google "AdWords," YouTube Premium, etc.); as with similar, private-sector promoted initiatives such as Facebook's Free Basics,[23] Google's strategy via such programs likely goes beyond philanthropy and assistance, and may be connected to the well-documented history of cooperation between US tech giants and national security agencies. The example of Teplodigital program also shows the efficiency of the worldwide efforts made by the company to consolidate the hold of its "soft power" beyond conventional means of lobbying, such as a long-term work with the nonprofit sector, in particular, with NGOs defending internet freedom and digital rights, "influential in civil society and devoted to myriad missions, including shaping technology and privacy policy" (Jewler, 2015). Presenting itself internationally as a defender of free speech and a sponsor of human rights organizations and of international Human Rights events, Google is thus criticized to fund "those who might otherwise raise alarms about its practices" (Ibid., 2015).

More specifically for the Russian case, nonprofits' partnerships with Big Tech actors appear paradoxically as a fallback solution, given the particularly tense context in which NGOs function in Russia, operating in quasi-"cold war" conditions, drastically reducing the opportunities for funding by international foundations and favorable to the official hunt for foreign influences. "My state is my main enemy" seems to be a formula that sums up well the polarized quasi-war situation in which the civil activists find themselves in their daily activities as well as in their social and professional representations. This trust in Google is indeed defined by this crude arithmetic of threats and power relations: "the enemy of my enemy is my friend." Thus, the American Net giant is valued for what it is otherwise criticized for: its monopolistic position, which allows it to resist the Russian state and to comply only partially with its legislation.

[21] Ibid.

[22] TechSoup website is www.techsoup.org

[23] Its website can be found at www.facebook.com/connectivity/solutions/free-basics.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

8.3.6 "Shadow Libraries" as Knowledge Disseminators, between Conformity and Repression

Online user-generated "shadow" libraries may be seen as troublemakers that challenge the Russian sovereignization project in several ways. First, by disseminating texts without regard to their legal status, they defy the state's increasing willingness to enforce copyright on the Russian web. Second, they challenge the cultural dimension of sovereignty: by creating an autonomous, uncensored text-sharing space, they thwart the Russian government's desire to control the cultural consumption of internet users by filtering their access to cultural goods. And finally, by developing and promoting tools to circumvent website blocking, the administrators and users of shadow libraries contribute to public resistance to the sovereignization project.

Long blamed for numerous copyright infringements, especially by the US Creative industries (Kirya, 2011), Russian federation authorities gradually developed copyright legislation that not only meets global standards, but is aligned with its strictest versions (Alekseeva et al., 2013, p. 69). New internet control tools introduced in the 2010s have ensured its compliance on Russian territory. A year after the FZ-139 law adoption, in 2013, an "anti-piracy law" designed to apply the black-listing and blocking mechanism to copyright-infringing sites entered into force. Mobilizations against the "Russian SOPA" were numerous (Zasursky, 2016, pp. 62–63), and different struggles for digital freedoms converged in a common struggle for a "free RuNet." However, the "anti-piracy" legislation has been reinforced ever since, integrating more actors and amplifying penalties.

In this context, Russian "shadow" mass-literature libraries, access to which was progressively blocked on the Russian territory since 2015, developed different survival strategies. A major concern is to ensure the sustainability and growth of the collections, which depends on the vitality of the community that nurtures it. Major sites, such as Librusec and Flibusta, operate in a Wiki-like way: texts and annotations are uploaded and corrected by the users themselves, thus ensuring the exponential growth of collections. Librusec's administrator, Ilya Larin, relies on both code and text sharing – which he calls "cross-pollination" – to guarantee the survival of the ecosystem. Torrent distribution in one of the alternative dissemination channels. Torrents allow users to download the entire archives onto their computers, accompanied by a program that transforms it into a database for convenient use. Once the full database is installed on the computer, the user may download its updates. Thus, the library's collection is replicated many times and kept not only online, but also offline. Its ability to be restored anytime makes its total disappearance impossible. The server on which the main collection is stored is also of great importance for the security of the library. The legislation of the country the hosting is located in must be sufficiently tolerant of copyright infringements.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

Another important concern of these libraries is to ensure access to the collections on the Russian soil. The first way consists of multiplying "mirrors" in locations that are considered safe. For example, the .lib domain, ruled by Emercoin, is regarded as such thanks to its decentralized structure. In its current form, the Domain Name System root is under the centralized authority of Internet Corporation for Assigned Names and Numbers (ICANN, a Los Angeles–based nonprofit). In this system, every DNS record is kept by the DNS provider and can be blocked under political or commercial pressure; however, in a decentralized DNS each record is managed solely by its owner, and is readable by all users on the network[24]. Networks that guarantee anonymity, like Tor and "Invisible Internet Project" (i2p), are also suitable to escape national constraints, which leads shadow libraries to have their "representatives" there[25].

The second way focuses on instructing users. Since the beginning of site blockages, libraries and forums have displayed lists of the technical means to escape the communication barriers created by RuNet service providers at RKN's request. This dissemination of circumvention knowledge seems to be omnipresent and circulates through many channels: mailings, posts on social networks, or YouTube tutorials. The proposed solutions include the change of DNS server, browsers with turbo mode (Opera, Chrome, and Yandex),[26] or embedded VPN, special plug-ins for browsers, VPN services, Tor browser, and the use of anonymizers. Expert community members explain to nontechnical users how each method works and present its advantages and disadvantages (which are usually speed of execution versus simplicity of use). This mastering of circumvention tools today becomes a part of the know-how of every person visiting the shadow libraries.

In addition to the torrents mentioned earlier, library users and administrators compete in creativity to organize the distribution of new archive updates. Here again, the proliferation of means and media is the rule. For example, Librusec.ucoz, a forum common to several shadow libraries and which acts as a safe harbor in case the internal forum is inaccessible, has a section called "Our Tortuga"[27] centralizing the links to the updates of Librusek and Flibusta databases *via* free file-sharing sites.

In parallel to these friendly sites, the communities use social networks and messaging. For example, a bot on the Russian social media VKontakte allowed, for a while, to make a quick search in the shadow libraries and thus

[24] See https://roskomsvoboda.org/12118/, accessed May 20, 2024.

[25] See https://roskomsvoboda.org/28612/, accessed May 20, 2024.

[26] Invented by the developers of the Opera browser in 2009, the turbo mode was intended to increase browsing speed: data is first downloaded to the browser's server, and the user downloads it from there in compressed form. But the fact that the data transits through Opera's server allows this tool to be used for bypassing site blockades: the ISP cannot detect and therefore deny access to banned sites.

[27] See http://librusec.ucoz.de/forum/7-171-318"\l"105370"\t"_blank, accessed July 16, 2020.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

facilitate access in case of breakdown or blocking.[28] In June 2019, VKontakte and the publishing house Eksmo concluded a settlement according to which the social network has to check the legal status of all the books downloaded by users. However, this did not lead to the disappearance of the bot: in September, it was transferred to a safer storage medium.[29] After the tightening of VKontakte's attitude toward illegal content, some shadow libraries began to actively use Telegram bots to distribute books, since this messenger was known to be tolerant to illegal content, thanks to the libertarian worldview of its owner, Pavel Durov. However, by August 2020, these bots would have stopped working, supposedly as a result of an agreement between Telegram and the Russian authorities.

8.4 CONCLUSIONS

This chapter has sought to provide an analytical overview of the ongoing processes related to infrastructure-based digital sovereignization in Russia, drawing from three years of fieldwork conducted in the frame of the ResisTIC project. Our overview of case studies has highlighted four recurring dynamics in the Russian state's attempt to enforce digital sovereignty by infrastructure, as well as in strategies of circumvention and evasion enacted by different groups of actors, from civil society organizations to technical actors and "ordinary citizens."

First, we have observed how the Russian government seeks to raise a series of obstacles against foreign techniques and alternative infrastructures, considered as "subversive." Second, our research sheds light on the "collateral damage" resulting from the technical implementation of these infrastructure-based coercive measures, and the (often infrastructure-based, as well) attempts to remedy or mitigate this collateral damage; in doing so, it shows in parallel the extent to which such measures are frequently ineffective with respect to their intended purpose (on this point, see also Musiani et al., 2016). Third, we have followed the creation and development of new "digital national champions" under an increasingly close government supervision, which leads to pressures and manipulations exerted by the State on particular platforms and their algorithms, as well as to countermoves that can be surprising from the standpoint of a Europe- or United States-based scholar, such as, the trust in American "Net giants" as powerful actors able to stand up to the Russian government. Finally, we have highlighted the emergence of critique and circumvention initiatives among internet users vis-à-vis "governance by infrastructure," and we have observed how these reactions contribute to the emergence of new forms of "resistance by infrastructure." This approach by case studies provides a nonlinear, nuanced, and complex understanding of the specificities of RuNet

[28] See Flibusta's VK page: https://vk.com/wall-98093156_238, accessed September 2, 2020.

[29] See https://github.com/FlyInk13/FlibustaBot, accessed September 5, 2020.

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

governance, which mirrors the national conception of digital sovereignty, often described as a strictly centralized, top-down, and efficient information control system. Our chapter has proposed to pay attention to microtechniques of circumvention and shows how the discourse on internet sovereignty (and the subsequent demand for all information control technologies to be "made in Russia") is currently giving way to two important paradoxes in the country. On the one hand, it can lead groups of activists and users whose main priority is to escape the Russian government's surveillance, control, and sovereignization to end up spontaneously subjecting themselves to surveillance, control, and "sovereignization" originating in the United States. On the other hand, it opens up technical and legal opportunities for mundane resistances and the existence of "parallel" RuNets, where particular instantiations of informational freedom are still possible.

8.5 OVERTURE: UKRAINE, INTERNET AS A TOOL (AND BATTLEFIELD) OF WAR?

On February 24, 2022, the Russian military offensive against Ukraine is accompanied by an immediate reinforcement of censorship on the media as well as controls and blockages of the internet in Russia. The process of co-opting the internet as a tool in the warmongering policy of the Russian state is suddenly accelerating and making it possible to tighten the grip on the public space in the context of the war. This justifies the brutal tightening of the network of constraints that already weighed on both the actors and the digital infrastructures in Russia. On the one hand, the law is amended in a more restrictive sense, prohibiting any criticism of the army or any evocation of the term "war" (qualified as "special military operation"). This censorship leads many media to give up their publications. Criminal proceedings are initiated against independent journalists and opponents of the war while the repository of "foreign agents," kept by the Ministry of Justice, is considerably longer.

When it comes to internet infrastructures, the topic of this chapter, the government is blocking international social networks (Facebook, Instagram, etc.) and strengthening its control over local digital players (VKontakte, Yandex, etc.). These decisions come as, under the effect of sanctions, a number of foreign digital operators have left the country and disconnected their infrastructure from the Russian network. The invasion of Ukraine by Russia, and the retaliatory international sanctions, makes visible the manifold dependencies of the Russian surveillance and censorship industry on foreign components, infrastructure, and know-how: for example, the lack of filtering software traditionally supplied by Western firms, such as Sandvine and Nokia, is heavily impacting the monitoring and blocking activities of the Russian government. Furthermore, this results in techno-legal loopholes and gray areas that create both uncertainty and opportunity for technical actors, such as internet service

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press

providers. It also leads to paradoxical situations for the government, such as the fact that, despite the discourse on sovereignty and despite the sanctions, the Russian central bank continues to use European certificates in order to give a stamp of approval to the activity of the RuNet technical actors.

While all of these dynamics are currently evolving at a steady pace and conclusions cannot yet be drawn from the situation, one thing is clear: internet governance has never been as close to a "global war" (DeNardis, 2014) as today, and the upcoming months and years will keep on providing illustrations of this problematic trend.

ACKNOWLEDGMENTS

In addition to ResisTIC, several authors (F. Daucé, K. Ermoshina, B. Loveluck, F. Musiani) would like to acknowledge the research project that supports them at the time of this book's publication on the topic of this chapter, DIGISOV "Digital Governance and Sovereignty in a Fractured World: Competing States and Circulating Norms" (2024-2027) ANR-23-CE53-0009-02, funded by the French National Agency for Research (ANR).

https://doi.org/10.1017/9781009531085.012 Published online by Cambridge University Press