Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction

Françoise Daucé, Francesca Musiani

f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction

by Françoise Daucé and Francesca Musiani

Abstract

Pursuing the autonomisation and "sovereignisation" of their national Internet (RuNet) since the early 2010s, authorities in the Russian Federation are establishing increasingly stricter regulations on Internet innovation and practices. Since 2018, the team of the *ResisTIC (Criticism and circumvention of digital borders in Russia)* project explores how different actors of the RuNet resist and adapt to the recent wave of authoritarian and centralizing regulations. 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. This special issue provides a detailed overview of the different strands of research undertaken by the ResisTIC project team at the crossroads of digital sovereignty, data and infrastructure. Articles by the project team are entwined with contributions by specialists based in Russia and worldwide.

Contents

Introduction

In the first decade of the twenty-first century, characterized by relatively high levels of freedom in the management of digital technologies and related user practices, the technical constraints on the construction of the Russian Internet (RuNet) have remained mostly invisible to its users (Deibert and Rohozinski, 2010). However, since the early

2010s, the increasingly strict regulations imposed by the government have made these aspects more evident (Oates, 2013; Soldatov and Borogan, 2015). In particular, Roskomnadzor (RKN), the federal government communications control body, has seen its jurisdiction and reach rapidly extended to domains as varied as the control of online content, the right to block Web sites, and the registering of blocked Web sites on blacklists, with a substantially increased possibility of censorship. RKN's control relies on its important nexus of relations and collaborations with state security institutions at federal and regional levels (*e.g.*, the Ministry of Internal Affairs — Министерство внутренних дел СССР [МВД, MVD], Federal Service of Security — Федеральная служба безопасности Российской Федерации [ФСБ, FSB], and judicial institutions) as well as with actors that maintain and keep the Internet operational, and propose connectivity solutions to users (access providers, owners of digital businesses ...). Russian authorities actively move towards an autonomisation and "sovereignisation" 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 (FIDH, 2018; Musiani, *et al.*, 2019).

Since 2018, the team of the *ResisTIC (Criticism and circumvention of digital borders in Russia)* [1] project endeavors to analyze how different actors of the RuNet resist and adapt to the recent wave of authoritarian and centralizing regulations. The project has a particular focus on online resistance and the lesser-known social practices and techniques deployed for circumventing online constraints. Beyond the Russian case, 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 they cross paths with innovation trajectories of digital technologies in the modern world.

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 is to shed light on the complex relationship between technical devices and algorithms (Brousseau, *et al.*, 2012; Musiani, 2013) in the Russian digital sphere, and the politics and markets taking shape in the country. This special issue provides a detailed overview of the different strands of research undertaken by the ResisTIC project team at the crossroads of digital sovereignty, data and infrastructure — both its development and its uses, oftentimes very creative and subversive when it comes to the RuNet. In this special issue, articles by the project team are entwined with contributions by specialists based in Russia and worldwide, with whom we have closely interacted in the frame of our monthly research seminar at the School of Advanced Studies in the Social Sciences (École des hautes études en sciences sociales, EHESS, Paris) or during visiting researcher tenures, and whose work inspires us.

Russia and its Internet infrastructure, between centralizing authority and distributed resistance

Since the late twentieth century, the development of networked information and communication technologies has elicited questions about their deconstructing effects on national sovereignty. The Internet itself, originally developed primarily in the United States (*e.g.*, Castells, 2001), has spread throughout the world, overcoming national borders, and has become one of the symbols and catalysts of globalization.

Since the early 2010s, national concerns have emerged about the Internet's threats to government sovereignty, which has led to a tightening of national Internet legislation (Loendorf and Garson, 2008), and other restrictions. These restrictions may combine elements of security (fight against terrorism and extremism), economics (copyright; industrial espionage, opposition to Web multinationals) and explicitly political choices (as in China and Iran). The Internet has arguably entered an age of new domination (Fuchs, *et al.*, 2012) and surveillance (Marx, 2016), at a time of growing authoritarianism, raising the question of the repressive uses of the Web in the modern world (Morozov, 2011; Deibert, *et al.*, 2008). With massive quantities of content and data being produced on a daily basis, and constantly evolving technology, any hierarchical, state-centered concept of regulation would, however, appear to be inadequate, which has prompted numerous calls for a rethinking of Internet governance (Brousseau, *et al.*, 2012). New instantiations of control are more fleeting, invisible, changing and multi-faceted; the exercise of authority is a discreet activity, weaving many webs, playing with countless relationships that are hard to visualize. Control is exercised in the long term, exploiting the blind spots of the public arena (Chateauraynaud, 2015).

In Russia, the issue of developing communication infrastructure on a territorial scale has been a political, social and technical challenge since the Soviet period (Zakharova, 2020). Despite the authorities' interest in cybernetics and automation (Gerovitch, 2002), the USSR failed to network the country's infrastructure in the last years of socialism (Peters, 2016). After the demise of the USSR in 1991, the brutal political and economic transformations of the 1990s led to a decentralised and complex development of computational and digital infrastructures (Kolozaridi and Muravyov, 2020). The first decade of the century, after the election of Vladimir Putin to the Russian presidency in 2000, was marked by a political-digital paradox of "half-freedom of speech" (Gelman, 2010), with both rapid development of a free Internet and the strengthening of vertical, unitary political governance. By 2016, nearly 75 percent of the Russian population was connected to the Internet within the country. Outside, the RuNet (to be understood, this time, as "Russian-language" Internet) is read and consulted by those citizens of the independent, formerly Soviet, republics who know the language. In the "far abroad", the RuNet connects Russian emigrant communities throughout the world, especially in the United States, Israel and Europe (Fialkova and Yelenevskaya, 2005; Morgunova, 2012). In the early 2000s, this development of the Russian Web and its openness to the world raised hopes of democratization in the home country and more off-line mobilization (Lonkila, 2012; Etling, *et al.*, 2010). Since the early 2010s, these hopes of a Russian-style "Internet democracy" (Cardon, 2010) have been dashed, as political tensions have risen at home (the significant protest movement of winter 2011/2012) and abroad (Ukraine in 2014). Russian Internet legislation has been considerably tightened, illustrating the government's desire to establish national control within a digital arena that had hitherto

escaped it. These national Web regulation measures demonstrate the coercive responses the authorities have chosen to the challenges the Internet poses to sovereignty. This policy of refocusing the RuNet nationally has been clearly documented by researchers in this area (Nocetti, 2015; Freiberg, 2014).

However, this control policy must not necessarily be seen as following a vertical, coherent and hierarchical model. The laws applying to online activity are numerous, varied, constantly adapting (laws against terrorism, extremism, pornography, etc.). Their enforcement is often random or arbitrary. Close examination of the legislation and its enforcement shows not a centralized domination of the Russian Web and Internet, but rather a multiplicity of types of control that are partial, fluctuating and sometimes contradictory. Legal controls may apply, in various ways, to the technical constraints (algorithms) or economic features (profiling) of online activity. Understanding the diversity of constraints applying to the Russian Web and Internet is essential for understanding the many forms of resistance, escapism and circumvention that have developed in reaction to them. Since the 2000s, Russian society has been neither apathetic nor resigned, as shown by the local mobilisations contributing to the development of citizen activism (Kleman, *et al.*, 2010) or the large demonstrations against electoral fraud in 2011 and 2012 (Gabowitsch, 2017). In the digital space, activist initiatives and skills are also developing, contributing to the diffusion of critical digital knowledge in society. These practices contribute to making digital life possible, and are sometimes reminiscent of the arrangements of the late Soviet period that combined both criticism and loyalty to institutions (Yurchak, 2005).

Thus, this special issue seeks to examine the link between Internet governance and digital sovereignty strategies on the one hand, and dynamics of critique, resistance, and circumvention on the other hand, in the Russian context. Academic work on "disobedience" and "resistance" to domination is prolific, in history, political science and sociology, and has demonstrated that institutional order cannot be imposed without some tempering and arrangement in the distribution of prescribed roles (Hmed and Laurens, 2011). Framed in this way, resistance and protest provide a particularly useful key for analyzing social organizations. While it often proves difficult to identify a coherent, organized "resistance", researchers have shown how resistance takes the shape of skills and *arts de faire* (de Certeau, 1990), avoidance, circumvention, hacking (Keucheyan and Tessier, 2008), arrangements in the style of "dwarfs without giants" (Musiani, 2013) so as to escape the need to go through compulsory points of passage and control. On the Internet, new forms of online protest are developing against government Web surveillance policies (Best and Krueger, 2008; MacKinnon, 2012). Some may involve visible public voices (see Cardon and Granjon's 2013 work on *mediactivism*), others anonymity and obfuscation. Models derived from off-line movements and new models shaped upon networked technologies co-exist; at times, resistance takes the form of "piracy", in the sense of repurposing technology (Keucheyan and Tessier, 2008). It is important, therefore, to understand net resistance by focusing on the technical components of hardware and software, the continuously evolving infrastructure that populates the Internet, holds it together or fragments it, and is at times a "test-bed" for Internet governance battles (Bowker and Star, 1999; Lessig, 1999; Abbate, 1999; DeNardis, 2014).

Towards an infrastructure-based sociology of the RuNet

Taking into account all of the above, this special issue 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. Indeed, in response to the Russian government's increasingly authoritarian grip, direct political confrontation is difficult and risky; thus, 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 resisters" adapt to new laws and invent new techno-legal tweaks that challenge the Russian lawmaker. However, digital and civic activists act in a context of uncertainty and their strategies must not necessarily be interpreted as following a coherent and sustainable model. Thus, several articles in the special issue will 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; however, they will also examine the uncertainty surrounding the enforcement of new regulations concerning digital infrastructures.

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 (*e.g.*, Musiani, 2018, for a discussion of this point).

The analyses presented in the special issue are based on original data, both quantitative and qualitative (interviews, observations on the field). In addition to the presentation of the case studies, a recurring point of interest will be a reflexive assessment of 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 Russian Internet and renew our understanding of the role of infrastructure in digital control and circumvention.

Articles in the special issue

The articles collected in this special issue explore infrastructure-embedded sovereignty, control and circumvention in the Russian Internet according to three complementary perspectives that make it possible to deconstruct the usual opposition between vertical control and civil freedom, and to shed light on unexpected and exploratory reflections, practices and uses of digital infrastructures by multiple players.

I. Sovereignty and control by infrastructure in the RuNet: Theoretical perspectives and arenas of contention

The debates around the Russian Internet offer, first of all, new opportunities to conceptualize the public stakes related to digital sovereignty and control by infrastructure, and to explore the national and international arenas where digital sovereignty is constructed, promised, imposed, co-opted, resisted in practice.

In their article, Polina Kolozaridi and Dmitry Muravyov recall that in reference to Russia, the concept of "Internet sovereignty" is used to evoke the state's efforts to tighten its control over the Internet in order to consolidate a non-democratic political regime. However, according to them, the precise meaning of both "sovereign" and "Internet" has largely been overlooked. They discuss the structural asymmetries of power in "global" Internet governance, suggesting that Russia's Internet sovereignty claims can be seen as an expression of counter-hegemonic tendencies. Their work invites us to escape the commonplaces of dominant political thinking and to reflect further on the concepts we mobilise to grasp and understand contemporary debates on the Internet.

Indeed, abstract framings of digital sovereignty, as a legal concept and a set of political discourses, are sometimes out of step with the concrete provisions and the mundane, day-to-day functioning of digital infrastructures. As Ilona Stadnik points out in her article, since 2014, Russia invested a lot of efforts in the development and adoption of new laws and regulations that deal with Internet sovereignty through infrastructure. However, the control-by-infrastructure endeavor is not devoid of pitfalls and complications. She demonstrates this through four emblematic cases (the "Revizor" system; the battle to block Telegram messenger; the law "on Sovereign RuNet" and the project of free access to "socially significant websites"). These cases show that content filtering and blocking of access to Web resources do not work as the government would wish and can even harm other sensitive sectors of a country's digital economy.

Another illustration of this discrepancy is provided by Liudmila Sivetc, who shows the limits of the infrastructure control system that the Russian government has been gradually implementing. She examines the building of the Yarovaya-Law infrastructure, aimed at storing content data collected by information disseminators in Russia and conclude that, by the summer of 2020, it had faltered due to cost and implementation obstacles and may have hindered the continuation of the RuNet sovereignization strategy. Her study invites us to seriously consider the successes, but also the possible failures, of the Russian state's regulatory ambitions.

II. Internet infrastructure as a battleground, from protocols to services

Phenomena such as the circulation of data, the development of social networks and communication tools, and the control of algorithms and protocols offer an exceptional

observatory for understanding the "governance" by digital infrastructures and its limits, and the extent to which Internet infrastructure becomes a "battleground" of modern times.

At the margins of Russia, in the disputed territories of Ukraine, the research carried out by Kevin Limonier, Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian and Kave Salamatian shows that data routing is of geopolitical significance. They study the new forms of power rivalries and imbalances that occur within the lower layers of cyberspace, through the analysis of Eastern Ukraine. They show how Donbass cyberspace progressively migrated from Ukraine towards Russia, but has been relegated to the periphery of both networks. Less visible than the circulation of civil and military forces, the control exercised over the circulation of data illustrates the geopolitical reconfigurations at Europe's borders.

In Russia itself, the control of data circulating on social networks has become a political issue in 2018. In their contribution, Ksenia Ermoshina and Francesca Musiani analyze the emblematic "Telegram ban" and its ramifications, understanding it as a socio-technical controversy that unveils the tensions between the governmental narrative of a "sovereign Internet" and multiple infrastructure-based battles of resistance, critique and circumvention. They show how a number of infrastructure-based digital resistances emerge and thrive despite the centralised management that the Russian government seeks to present to the world as its own.

In addition to social networks, search engines and news aggregators are also at the heart of this battle, as shown by Françoise Daucé and Benjamin Loveluck from the example of Yandex.News aggregator — the Russian equivalent to Google News. Suspected of political bias in the context of protests against electoral fraud followed by the Ukrainian crisis, the aggregator has been at the core of several controversies, which the authors analyse to show the discrepancy between the diversity of the Russian online mediasphere and the narrowness of the Yandex.News media sample. The aggregator is a key asset in the Russian government's effort to assert "digital sovereignty", but its control is drawing increasing criticism from media and digital specialists in Russia itself.

III. Activist mobilizations and understandings of Internet infrastructure

At the forefront of social and civil protest, activists are confronted with the new political challenges of digital infrastructures and look for new uses and practices to circumvent them.

In their research, Olga Bronnikova and Anna Zaytseva analyse the paradox related to the use of Google services in Russia: several NGOs based in the country consider the Internet giant as a protector of civil liberties. In a context where their risk model is focused on the threat emanating from the State rather than from global private companies, these activists prefer "big tech" solutions than open source software, leading to both Google and the Russian state, as well as the Russian NGO ecosystem, to implement complex strategies of protection and publicity.

Unlike urban political opposition that uses United States-based social media platforms and services, grassroots movements mainly use VKontakte, the Russia-developed

dominant social network in the country. In her article, Perrine Poupin describes the digital technologies-embedded repression practices developed against a local grassroot environmental protest in Far Northern Russia. Activists use VKontakte despite the potential privacy and security risks this platform has posed to users since 2014. They develop counter-practices to circumvent the government limitations to online protest activities.

Finally, Bella Ostromooukhova offers a story of shadow mass-literature online libraries in Russia. In 2013, the "anti-piracy" legislation made these libraries illegal. To survive, they had to develop inventive circumvention techniques which reinforce their particular vision of "freedom", anchored in the mastery of technical tools and in uncensored cultural practices. The "shadow libraries" case shows how a number of "invisible" technical constraints become visible for the RuNet users following the implementation of a new repressive law and the attempts, to paraphrase David Clark, to "route around it".

Conclusions

Overall, this special issue sheds light on four yet understudied dynamics. First, it explores the obstacles that the Russian government raises against foreign techniques and alternative infrastructures, considered as "subversive". Second, it highlights the "collateral damage" resulting from the technical implementation of these infrastructure-based coercive measures. Third, it shows how the current RuNet context leads to the creation and development of new "digital champions" under an increasingly close government supervision, such as the pressures and manipulations exerted by the State on particular platforms and their algorithms. Finally, it demonstrates the emergence of strong critiques of "governance by infrastructure" dynamics among Internet users, which contributes to the emergence of new forms of "resistance by infrastructures".

This special issue provides a non-linear, nuanced and complex understanding of the specificities of Russian Internet governance, often described as a strictly vertical, centralized, efficient information control system. By focusing on techniques of circumvention at different levels, we show how the discourse on Internet sovereignty (and the subsequent demand for all information control technologies to be "made in Russia") paradoxically open up technical and legal opportunities for mundane resistances and the existence of "parallel" RuNets, where particular instantiations of informational freedom are still possible.

About the authors

Françoise Daucé is Professor at the School for Advanced Studies in the Social Sciences (EHESS) and director of the Center for Russian, Caucasian and East-European Studies

(CERCEC).
E-mail: dauce [at] ehess [dot] fr

Francesca Musiani is Associate Research Professor at the French National Centre for Scientific Research (CNRS) and Deputy Director of its Centre for Internet and Society.
E-mail: francesca [dot] musiani [at] cnrs [dot] fr

Acknowledgments

This work has received funding from the French National Agency for Research (Agence Nationale de la Recherche, ANR) in the frame of the project ResisTIC (Les résistants du net. Critique et évasion face à la coercition numérique en Russie, ANR-17-CE26-0020).

We are deeply indebted to the work of the 18 colleagues who, across disciplines and geographical boundaries, have graciously accepted to review the articles in this special issue: Balázs Bodó, Stanislas Budnitsky, Philip Di Salvo, Rashid Gabdulhakov, Olessia Kirtchik, Valery Kossov, Sophie Lambroschini, Kenneth Merrill, Stefania Milan, Julien Nocetti, Benjamin Peters, Elena Sherstoboeva, Daniel Taninecz Miller, Félix Tréguer, Daniel Trielli, Mariëlle Wijermars, Liliia Zemnukhova and Vera Zvereva.

Thank you to Guillaume Lavezzari of OKB-Buro (https://okb-buro.com) for the cover image.

Note

1. The project is supported by the French National Research Agency (Agence Nationale de la Recherche, ANR) and will conclude in June 2022. Its consortium includes five research units: Centre d'études des mondes russe, caucasien et centre-européen (CERCEC, EHESS/CNRS); Centre Internet et Société (CIS, CNRS); Cultures et sociétés d'Europe orientale, balkanique et médiane (Eur'Orbem, Sorbonne Université/CNRS); Institut des langues et cultures d'Europe, Amérique, Afrique, Asie et Australie (ILCEA4, Université Grenoble Alpes); Institut interdisciplinaire de l'innovation, Télécom Paris. The project Web site can be found at https://www.resistic.fr.

References

Janet Abbate, 1999. *Inventing the Internet*. Cambridge, Mass.: MIT Press.

Samuel J. Best and Brian S. Krueger, 2008. "Political conflict and public perceptions of government surveillance on the Internet: An experiment of online search terms," *Journal of Information Technology & Politics*, volume 5, number 2, pp. 191–212.
doi: https://doi.org/10.1080/19331680802294479, accessed 7 April 2021.

Geoffrey C. Bowker and Susan Leigh Star, 1999. *Sorting things out: Classification and its consequences*. Cambridge, Mass.: MIT Press.

Eric Brousseau, Meryem Marzouki and Cécile Méadel (editors), 2012. *Governance, regulations and powers on the Internet*. Cambridge: Cambridge University Press.

Manuel Castells, 2001. "Internet y la Sociedad Red," *La factora*, volume 14, number 15, pp. 1–13, and at https://red.pucp.edu.pe/wp-content/uploads/biblioteca/Castells_internet.pdf, accessed 7 April 2021.

Dominique Cardon, 2010. *La démocratie Internet: Promesses et limites*. Paris: Éditions du Seuil.

Dominique Cardon and Fabien Granjon, 2013. *Médiactivistes*. Seconde édition augmenteée et mise à jour. Paris: Sciences po, les presses.

Francis Chateauraynaud, 2015. "L'emprise comme expérience. Enquêtes pragmatiques et théories du pouvoir," *SociologieS*, at https://journals.openedition.org/sociologies/4931, accessed 7 April 2021.

Michel de Certeau, 1990. *L'Invention du quotidien. 1, Arts de faire*. Paris: Gallimard.

Ronald Deibert and Rafal Rohozinski, 2010. "Control and subversion in Russian cyberspace," In: Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (editors). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, Mass.: MIT Press, pp. 15–34.

Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (editors), 2008. *Access denied: The practice and policy of global Internet filtering*. Cambridge, Mass.: MIT Press.

Laura DeNardis, 2014. *The global war for Internet governance*. New Haven, Conn.: Yale University Press.

Bruce Etling, Rob Faris, John Palfrey, John Palfrey, John Kelly and Karina Alexanyan, 2010. "Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization," *Berkman Center, Research Publication*, 2010-11, at https://cyber.harvard.edu/publications/2010/Public_Discourse_Russian_Blogosphere, accessed 7 April 2021.

Larisa Fialkova and Maria N. Yelenevskaya, 2005. "Incipient Soviet diaspora: Encounters in the cyberspace," *Narodna umjetnost: hrvatski časopis za etnologiju i folkloristiku*, volume 42, number 1, at https://hrcak.srce.hr/2920, accessed 7 April 2021.

FIDH (Fédération internationale des ligues des droits de l'homme, International Federation for Human Rights), 2018. "2012–2018: 50 new laws to ban freedom of expression in Russia," at https://www.fidh.org/en/region/europe-central-asia/russia/russia-2012-2018-50-anti-democracy-laws-entered-into-force-within, accessed 25 March 2021.

Phillip Freiberg, 2014. “Putin’s Russia — On a path to cyber sovereignty?” *SSRN* (24 January).
doi: https://doi.org/10.2139/ssrn.3108579, accessed 7 April 2021.

Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (editors), 2012. *Internet and surveillance: The challenges of Web 2.0 and social media*. London: Routledge.
doi: https://doi.org/10.4324/9780203806432, accessed 7 April 2021.

Mischa Gabowitsch, 2017. *Protest in Putin’s Russia*. Cambridge: Polity Press.

Vladimir Gelman, 2010. “Ловушка полусвободы (Lovushka polusvobody: The trap of a half-freedom),” *Slon.ru*, at http://slon.ru/russia/lovushka_polusvobody-310531.xhtml, accessed 7 April 2021.

Slava Gerovitch, 2002. *From newspeak to cyberspeak: A history of Soviet cybernetics*. Cambridge, Mass.: MIT Press.

Choukri Hmed and Sylvain Laurens, 2011. “Les résistances à l’institutionnalisation,” In: Jacques Lagroye and Michel Offerlé. *Sociologie de l’institution*. Paris: Belin, pp. 131–146.

Razmig Keucheyan and Laurent Tessier, 2008. “Présentation. De la piraterie au piratage,” *Critique*, numbers 733–734, pp. 451–457.

Karin Kleman, Ol’ga A. Mirjasova and Andrej N. Demidov, 2010. *От обывателей к активистам: зарождающиеся социальные движения в современной России (Ot obyvatelej k aktivistam: Zaroždajuščiesja social’nye dviženija v sovremennoj Rossii)*. Moskva: Tri kvadrata.

Polina Kolozaridi and Dmitry Muravyov, 2020. “The narratives we inherit: The local and global in Tomsk’s Internet history,” *Internet Histories*, volume 4, number 1, pp. 49–65.
doi: https://doi.org/10.1080/24701475.2020.1723980, accessed 7 April 2021.

Lawrence Lessig, 1999. “The law of the horse: What cyberlaw might teach,” *Harvard Law Review*, volume 113, number 2, pp. 501–549.

Todd Loendorf and G. David Garson (editors), 2008. *Patriotic information systems*. Hershey, Pa.: IGI Publishing.
doi: https://doi.org/10.4018/978-1-59904-594-8, accessed 7 April 2021.

Rebecca MacKinnon, 2012. “The netizen,” *Development*, volume 55, number 2, pp. 201–204.
doi: https://doi.org/10.1057/dev.2012.5, accessed 7 April 2021.

Markku Lonkila, 2012. “Russian protest on- and offline: The role of social media in the Moscow opposition demonstrations in December 2011,” *Finnish Institute of International Affairs (FIIA), Briefing Paper*, number 98,
at https://www.fiia.fi/en/publication/russian-protest-on-and-offline, accessed 7 April 2021.

Gary T. Marx, 2016. *Windows into the soul: Surveillance and society in an age of high technology*. Chicago: University of Chicago Press.

Oksana Morgunova, 2012. "National living on-line? Some aspects of the Russophone e-diaspora map," *e-Diasporas Atlas*, at http://www.e-diasporas.fr/working-papers/Morgunova-Russophones-EN.pdf, accessed 7 April 2021.

Evgeny Morozov, 2011. *The net delusion: The dark side of Internet freedom*. New York: Public Affairs.

Francesca Musiani, 2018. "L'invisible qui façonne. Études d'infrastructure et gouvernance d'Internet," *Tracés. Revue de Sciences humaines*, volume 35, pp. 161–176. doi: https://doi.org/10.4000/traces.8419, accessed 7 April 2021.

Francesca Musiani, 2013. *Nains sans géants: Architecture décentralisée et services Internet*. Paris: Presses des Mines.

Francesca Musiani, Benjamin Loveluck, Françoise Daucé and Ksenia Ermoshina, 2019. "'Digital sovereignty': Can Russia cut off its Internet from the rest of the world?" *The Conversation* (28 October), at https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-internet-from-the-rest-of-the-world-125952, accessed 25 March 2021.

Julien Nocetti, 2015, "Contest and conquest: Russia and global Internet governance," *International Affairs*, volume 91, number 1, pp. 111–130. doi: https://doi.org/10.1111/1468-2346.12189, accessed 7 April 2021.

Sarah Oates, 2013. *Revolution stalled: The political limits of the Internet in the post-Soviet sphere*. Oxford: Oxford University Press. doi: https://doi.org/10.1093/acprof:oso/9780199735952.001.0001, accessed 7 April 2021.

Benjamin Peters, 2016. *How not to network a nation: The uneasy history of the Soviet Internet*. Cambridge, Mass.: MIT Press.

Andrei Soldatov and Irina Borogan, 2015. *The red Web: The struggle between Russia's digital dictators and the new online revolutionaries*. New York: PublicAffairs.

Alexei Yurchak, 2005. *Everything was forever, until it was no more: The last Soviet generation*. Princeton, N.J.:Princeton University Press.

Larissa Zakharova, 2020. *De Moscou aux terres les plus lointaines: Communications, politique et société en URSS*. Paris: Éditions de l'EHESS.

Editorial history

Received 2 April 2021; accepted 7 April 2021.

Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction
by Françoise Daucé and Francesca Musiani.
First Monday, Volume 26, Number 5 - 3 May 2021
https://firstmonday.org/ojs/index.php/fm/article/download/11685/10122
doi: https://dx.doi.org/10.5210/fm.v26i5.11685