12-1-2021

Varieties of digital authoritarianism analyzing Russia's approach to internet governance

Laura Howells
Bowdoin College

Laura A. Henry
Bowdoin College

LAURA HOWELLS
Bowdoin College, Brunswick, Maine, USA
LAURA A. HENRY
Bowdoin College, Brunswick, Maine, USA

Varieties of Digital Authoritarianism

Analyzing Russia's Approach to Internet Governance

ABSTRACT Digital authoritarianism threatens the privacy and rights of Internet users worldwide, yet scholarship on this topic remains limited in analytical power and case selection. In this article, we introduce a comprehensive analytical framework to the field of Internet governance and apply it first, briefly, to the well-known case of China and then, in more depth, to the still-understudied Russian case. We identify the extent and relative centralization of Internet governance as well as proactive versus reactive approaches to governance as notable differences between the cases, highlighting variation among digital authoritarians' governance strategies. We conclude that Russia's Internet governance model is less comprehensive and consistent than China's, but its components may be more easily exported to other political systems. We then consider whether recent changes to Russia's Internet governance suggest that it could converge with the Chinese model over time.

KEYWORDS Internet governance, digital authoritarianism, Russia, China, surveillance

Policymakers and scholars frequently refer to states like China and Russia as "digital authoritarians," a term that implies "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations" (Polyakova & Meserole, 2019, p. 2). Although the term is relatively new, the mechanisms of information control it encapsulates—surveillance, censorship, and manipulation of public opinion—have been widely studied (Polyakova & Meserole, 2019; Weber, 2019; Roberts, 2018; Deibert & Crete-Nishihata, 2012). The increasingly influential role of the Internet as a platform for information sharing and citizen activism presents both a potential challenge to authoritarian governments worldwide and an opportunity for them. Authoritarian regimes like China and Russia seek to monitor and restrict the free flow of information that may threaten their legitimacy. In recent years, China and Russia have sought to follow Chinese President Xi Jinping's goal to "occupy the [online] public opinion battlefield," in alarming new ways (China Digital Times, 2013, as quoted in Creemers, 2016, p. 44).

The Chinese and Russian regimes' goal of long-term survival may be similar, but their strategies for managing the digital sphere differ. What varieties of Internet governance do we see across these digital authoritarian regimes? How are the mechanisms of governing the Internet similar or different in China and Russia? Because digital authoritarianism

Communist and Post-Communist Studies, Vol. 54, Number 4, pp. 1–27, ISSN: 0967-067X, e-ISSN: 1873-6920 DOI: https://doi.org/10.1525/j.postcomstud.2021.54.4.1

encompasses a wide range of control measures, we focus more specifically on Internet governance—the policies, rules, and practices that a regime employs which shape the public's online experiences and behavior. Internet governance is an arena in which digital authoritarians can exercise censorship, surveillance, and manipulation in relation to the Internet infrastructure[1] and stakeholders who rely on it. In order to facilitate comparison across regimes, we disaggregate Internet governance by introducing a new analytical framework that can be applied to any case or context. The analytical framework identifies "targets" of governance from the Internet's infrastructure to the individual user, and specifies the mechanisms of governance for each target. We apply this framework to two cases, Russia and China. Whereas there is significant scholarship on digital authoritarianism in China, there is less comparable material regarding Russia. We focus on the latter case to address this paucity. Employing comprehensive data collection techniques for the Russian case and utilizing the new framework for comparison across cases, this article identifies the extent and relative centralization of Internet governance and a proactive versus reactive approach as the most notable differences between the cases.

Ultimately, we find that although Russia and China govern the Internet through mechanisms aimed at the same targets, the Russian Internet governance model is more decentralized, flexible, and less costly than its Chinese counterpart, and has developed in a more reactive and ad hoc way over time. As a result, Russia's model serves as a blueprint for countries around the world that want to pursue decentralized and affordable digital governance. We then consider whether these differences in models of digital authoritarianism are likely to persist or if we should expect eventual convergence as Russia begins to adopt more technologically-advanced, less visible Internet control mechanisms. This comprehensive analysis of Russian Internet governance offers a model for future studies of regional and global developments of digital authoritarianism.

In the first section of this article, we review the literature on varieties of authoritarianism and Internet governance. We then propose a new analytical framework for studying Internet governance. We employ the framework first to briefly analyze the Chinese case and then to examine the Russian case in greater depth. For the Russian case, we complement growing scholarship on this issue, as well as Freedom House, Human Rights Watch, and Levada Center reports on Russia's Internet governance, with a review of Russian Ministry of Justice legislation and Russian NGOs' detailed monitoring of Internet freedom, as well as an analysis of trends in individual prosecutions for online extremism. We then analyze a sample of representative cases from the Russian Federation's only public Internet blacklist, the extremism list ("Spisok Ekstremistov").

AUTHORITARIAN STABILITY AND INFORMATION CONTROL

Scholars have long debated the inherent fragility or stability of authoritarian regimes. Authoritarian regimes share the desire to survive and perpetuate their political system in the future;

1. For the purposes of this article, we define Internet infrastructure as the transmission media (wired and wireless) and physical hardware (such as routers and IXPs) required to facilitate Internet access.

however, their governance strategies to achieve these goals vary. "Authoritarian" is a broad umbrella for regimes ranging from personalistic (Chang & Golden, 2010), theocratic, and ideologically-based one-party regimes (Huntington, 2009), to regimes characterized as hybrid (Diamond, 2002), electoral authoritarian (Schedler, 2002), or competitive authoritarian (Levitsky & Way, 2002). Naturally, strategies to cultivate stable governance depend in part on the variety of authoritarianism and the regime's legitimation strategy (Gerschewski, 2013, p. 18). Whereas some regimes employ "strategic repression and co-optation" (Brancati, 2014; Gandhi & Przeworski, 2007; Geddes, 1999; Gerschewski, 2013, p. 18; Nathan, 2003; Slater & Fenner, 2011), others focus on "infrastructural mechanisms (Slater & Fenner, 2011, p. 15) or nominally adopt democratic institutions for the sake of mitigating internal and external threats (Brancati, 2014, p. 314). We would expect that broad differences across varieties of authoritarian regimes manifest in the strategies regimes use to address particular governance challenges.

Potential threats to an undemocratic regime exist not only in traditional political spaces but also in the digital realm, a space that many authoritarian regimes, notably Russia and China, see as an extension of sovereign territory. An important component of authoritarian governance involves shaping public discourse, controlling the spread of threatening information, and surveilling public discontent (Brancati, 2014; Gerschewski, 2013; Nathan, 2003; Slater & Fenner, 2011)—much of which now occurs online. To guard against digital threats and use the Internet as a tool for repression, authoritarian governments have become more proactive in their effort to govern the Internet in the past decade. However, regimes that excessively control online content and communications risk falling victim to the "dictator's dilemma" as they lose a reliable understanding of public opinion and possible sources of opposition to the regime (Kedzie, 1997, p. 1). Thus, all digital authoritarians face a balancing act as they devise their strategies of Internet governance.

Internet Governance Conceptualized: Targets and Mechanisms

While scholars recognize the importance of digital control to maintaining authoritarian regimes, specific strategies and mechanisms of authoritarian Internet governance are poorly understood.[2] Catchphrases like the "Great Firewall" substitute for more nuanced analysis of Internet governance strategies. Some approaches to Internet governance use overly simplistic dichotomies, such as "complete" or "partial control" (Müller, 2018) or "pure unenforced self-organization" versus "direct regulation by government-imposed regulatory bodies" (Marsden, 2011; Müller, 2018, p. 41). These dichotomies neither identify specific control mechanisms nor account for countries' varied technological capacities. Other tools for analyzing Internet governance capabilities specify numerous types of "content controls," but they do not facilitate easy comparison because they do not encapsulate the variety of targets and actors that can be governed (Deibert & Rohozinski, 2010). Moreover, some non-academic approaches to measuring or

2. The literature on Internet controls remains divided on use of the term "governance" or "regulation" (Mueller, 2010, p. 9; Münkler, 2018, p. 141; Black, 2005, as cited in Müller, 2018, p. 34). For the sake of clarity and consistency, we will exclusively use the term "governance."

Targets of Internet Governance	Control Mechanisms
Internet infrastructure 	Infrastructural isolation (Ex.: Firewall) Internet service blackouts
Internet service providers (ISPs) 	License restrictions Market control Content moderation mandates Prosecution
Online platforms and websites 	Prosecution Blocking/denial of service Content filtration Blacklisting
Internet users 	Prosecution Blocking Blacklisting Denial of anonymity

FIGURE 1. Internet governance framework.

differentiating among forms of Internet governance are overly assimilative, such as the one created by Freedom House that portrays Russia and China as highly similar by highlighting the fact that they both leverage all—or, in Russia's case, all but one—of a list of "key internet controls" (FH, 2019a, p. 28), overlooking numerous differences in their Internet governance strategies.

We propose a new analytical framework that enables direct, thorough, and generalizable comparisons of Internet governance and that can be applied to any case or regime type. We build upon Howard et al.'s Internet governance model (Howard et al., 2011, p. 5), which identifies four network elements. We expand our conceptualization of Internet governance by delineating *targets of governance* more precisely and identifying a wide array of control mechanisms that governments can leverage to influence each of these targets. This comparative Internet governance framework (see Figure 1) illustrates how regimes target different actors or elements of the network, including the Internet infrastructure, Internet service providers, online platforms and webpages (such as social media companies and websites), and individual users. It also specifies a non-exhaustive yet wide-ranging list of mechanisms of control used to govern targets. Several of the mechanisms that we identify are applicable to multiple targets, underscoring the fact that although targets can be loosely disaggregated for the sake of comparison, in practice they are interrelated within the network. Our discussion of control mechanisms throughout this article is intended to highlight the capabilities necessary for regimes to shape online behavior, both for less controversial aims, such as to limit children's exposure to inappropriate online content, and for more controversial political objectives.

This framework illustrates the numerous ways states can govern different targets of Internet governance. Regimes may not choose to govern every target, instead emphasizing

control over certain targets and not others. For example, there are significant differences in the resources or centralized control needed to isolate a network's infrastructure or create centralized firewall systems as compared to manually blocking websites, encouraging Internet service providers' (ISPs) dependence on the state, or prosecuting users based on the content they create, share, or consume on the Internet.

The goal of this framework is to facilitate a more precise understanding of variations in Internet governance strategies. To illustrate the framework's utility in comparative analysis, we apply it to two case studies—China, briefly, and Russia, more expansively—to consider the extent, style, and timing of Internet governance in two regimes that have been characterized as digital authoritarians. The Chinese Internet governance model, in keeping with the regime's centralized approach, emphasizes the governance of its Internet infrastructure, thereby eliminating content associated with blacklisted themes (Tiananmen Square protests, for example) nationwide, and universally blocking certain digital platforms, like Google, Facebook, and Twitter (except to VPN users). In contrast, Russia's Internet governance approach hinges on ISP controls and reliance on ISPs' execution of controls over other network targets, a strategy that offsets the costs of governance while relinquishing some degree of control and centralized authority. In the sections that follow, we apply this framework to a brief review of the abundant scholarship on China's Internet governance model followed by a more detailed examination of the less-studied Russian Internet governance as our primary case.

CHINA'S INTERNET GOVERNANCE IN BRIEF

With an impressive 829 million Internet users, representing 59.6% of its total population, China has the ability to shape the digital experiences of almost 20% of the world's population through its Internet governance and control measures (FH, 2019a, p. 4). Freedom House's 2019 "Freedom on the Net" report indicates that "China was the world's worst abuser of Internet freedom for the fourth consecutive year" (FH, 2019a, p. 2). China's Internet governance system is notoriously ambitious and multifaceted (Chi, 2012; King et al., 2013; Laskai, 2017; Lu & Zhao, 2018; MacKinnon, 2011; Roberts, 2018; Tkacheva et al., 2013; Yang & Mueller, 2019). Applying the new analytical framework to the Chinese case confirms the comprehensive nature of the Chinese Internet governance model, which actively governs all targets. Delving deeper into analysis of China's Internet governance, we observe that governance is highly centralized around the Chinese Communist Party (CCP), is aimed at all targets, and prioritizes governance of Internet infrastructure in particular (Roberts, 2018, p. 110).

China has taken a proactive approach to Internet governance, with oversight capacity developing as the Internet became more accessible and central to daily life. China's Internet governance system—known informally as the Great Firewall—was created in 1996 by State Council Order No. 195 and epitomizes an extreme version of centralized Internet control (Polyakova & Meserole, 2019, p. 3). From 1994 to 2015, China's Internet governance model was gradually constructed by approximately 50 governing bodies responsible for enacting more than 200 policies (Miao et al., 2018, p. 3).

However, in 2014 President Xi Jinping concentrated responsibility for Internet governance in the hands of the Cyberspace Administration of China (CAC), which answers directly to the Central People's Government (State Council) and which Xi himself chairs (Creemers, 2016; Lu & Zhao, 2018, p. 3297).

The Chinese Firewall, or system of centralized Internet traffic "choke points," is perhaps the most technologically advanced example of Internet infrastructure isolation in the world and enables the state to systematically block servers and sites nationwide (Ramesh et al., 2020, p. 1). The network infrastructure is also isolated from international Internet traffic, allowing the state to control Internet access on a national and regional level. The "one button" Internet kill switch has been successfully employed on numerous occasions, illustrating China's centralized capacity to govern its digital environment.[3]

Moreover, as early as 1996, ISPs were required to register with and be approved by the state in order to provide Internet services. In 2000, State Council Order No. 292 required ISPs to adhere to censorship standards. Partially or wholly state-owned corporations now operate as the gatekeepers for China's domestic Internet traffic as it interacts with the global web, under the guidance of the CAC (FH, 2019a, p. 6). A 2015 "anti-terror" law, an amendment to the Chinese Criminal Law, and the infamous 2017 Cybersecurity Law also stipulate criminal liability for ISPs who fail to store data locally, remove content, or cut off individual users according to the state's wishes (FH, 2019a, pp. 6–7; Iasiello, 2017, p. 11; Xuan, 2018, p. 72).

The government's control of the Internet, which has tightened over time, also extends to domestic and foreign online platforms and websites. China's vibrant information and communications technology (ICT) industry has produced various cutting-edge technologies, such as search engines and platforms including Tencent and Baidu, e-commerce companies like Alibaba, and social media giants such as WeChat, Weibo, and Renren. WeChat, a multi-use platform modeled after Facebook, had approximately 1 billion monthly users in 2019 (Kharpal, 2019). The large size and domestic origins of these companies make them easier for the Chinese state to govern, surveil, and even co-opt given their localized operations (Creemers, 2016, pp. 86, 95; King et al., 2013, p. 2). China's cyber laws target corporations to foster private-sector dependence on the state. The Firewall also blocks foreign websites and platforms like Twitter, Google, Facebook and YouTube as well as virtual private networks (VPNs), which allow users to connect to ordinarily-filtered content by disguising the location of their IP addresses (Kolton, 2017, p. 120). Government-issued blacklists are not publicly accessible (FH, 2019a, p. 15).

Although China's centralized model is constructed to prioritize infrastructural governance, a number of mechanisms targeted at users also exist. China's Internet governance model surveils public opinion to monitor discontent and preempt collective action (Creemers, 2016, p. 90). There is a thriving industry for public opinion monitoring, led by the People's Daily Online Public Sentiment Monitoring Office, which was established in 2008 and is highly cooperative with the state (Creemers, 2016, p. 90). Information

3. The most notable instance of full network level control occurred in 2009 when, for 10 months, the state cut Internet access in the region of Xinjiang to punish and neutralize ethnically-motivated riots (Griffiths, 2019, p. 156).

about certain political issues, like Falun Gong and Tiananmen Square, is prohibited. Internet users who write about these topics are subject to legal and social penalties (Griffiths, 2019, p. 46; King et al., 2013; Laskai 2017; Polyakova & Meserole, 2019; Williams, 2013). In recent years, the state has cracked down on digital anonymity to more easily prosecute individuals. For example, in 2012, Chinese "micro-bloggers" were forced to register with the government (King et al., 2013). Since 2013, Article 246 of the criminal law in China has been extended to any citizen who "publicly humiliates" or "invents stories" online (Human Rights Watch, 2013). The pressure from these laws and the prosecution of some individuals encourages citizens' self-censorship online (Laskai, 2017, p. 5; Lu & Zhao, 2018).

Despite abundant scholarship, China's Internet governance model is rarely comprehensively analyzed in terms of its component parts. Fascination with the Great Firewall often distracts observers from a detailed understanding of China's Internet governance mechanisms beyond the infrastructural realm, and rarely are all targets of Internet governance discussed as components of a larger governance strategy. Using the new analytical framework, we find that the Chinese model of Internet governance is indeed advanced, centralized, and complex. In addition to its control over network infrastructure, from the early stages of global Internet infrastructure development the Chinese regime has been able to execute a top-down and systematic preemptive approach to Internet governance, relying less on retroactive prosecution of individual users. Such extensive and centralized Internet governance can be achieved only with significant budgetary expenditures (Soldatov & Borogan, 2017, p. 56).[4]

RUSSIA'S INTERNET GOVERNANCE MODEL: VARIETIES OF DIGITAL AUTHORITARIANISM

Whereas China's Internet governance model is widely studied by political scientists and policymakers, less is written about Russia's digital information controls, despite the fact that elements of Russia's model have been reproduced in other countries (Barme & Ye, 1997; Griffiths, 2019; Krönke et al., 2018; Lam, 2013; MacKinnon, 2011, p. 44; Polyakova & Meserole, 2019). According to the 2019 Freedom House International's Freedom on the Net report, Russia's Freedom on the Net score of 31 (0 = not free, 100 = free) is still significantly freer than China's score of 10 (Shahbaz & Funk, 2019). In addition, whereas China was seen as the world's worst abuser of Internet freedoms in 2019, Russia ranks at number 11 (Shahbaz & Funk, 2019). In comparison to China, Russia's total number of Internet users is smaller, at 116.8 million, but Internet penetration is higher, reaching approximately 76% of the population by the end of 2018 (Shahbaz & Funk, 2019, p. 29) and representing about one-sixth of all Internet users in Europe (Ramesh et al., 2020, p. 2).

4. Although total figures are not publicly available, China's country-wide cybersecurity spending in 2019 was estimated at $7.35 billion, with the government accounting for about 60% of total expenditures (Xinhua, 2019). A figure that includes the operating budgets of institutions like the CAC, network infrastructure maintenance, and emerging technology expenditures by the state would be even larger.

Although attempts have been made to control and monitor digital communications since the Soviet era, Russia's post-Soviet Internet governance model initially evolved slowly as compared to China's (Kolozaridi & Muravyov, 2021). Then, in 2011, the Bolotnaia protesters' use of US-based social media platforms to mobilize against election fraud marked a critical juncture and prompted the Putin regime's search for a more aggressive Internet governance strategy (Deibert & Rohozinski, 2010; Faulconbridge, 2014; Human Rights Watch, 2017; Lonkila et al., 2019, p. 19; Soldatov & Borogan, 2017, p. 56). In 2014, Putin characterized the Internet as a "CIA project," underscoring the fear that the digital information environment could undermine the regime, just as social media had enabled Arab Spring protests (Nocetti, 2015, p. 112). Thus commenced the "occupation of Runet"[5] (Lonkila et al., 2019 p. 22).

In this section, a systematic analysis of Internet governance in Russia highlights mechanisms of governance that often have been obscured by broad and imprecise comparisons to China's model. Like China, Russia governs all four targets in our analytical framework in some manner. Yet, upon closer examination, in comparison to China, the Russian Internet governance model is more decentralized, less comprehensive, and more reactive. However, recently passed infrastructural laws in Russia raise the question of whether these differences in Internet governance will persist or whether the models will converge over time.

Internet Infrastructure Governance

Russia's Internet governance institutions are significantly less centralized than China's, with authority shared among many autonomous entities (Nocetti, 2015, p. 118). The presidential administration, Security Council, Ministry of Communications, Ministry of Internal Affairs (MVD), and a variety of federal law enforcement agencies—as well as "vigilantes" loosely tied to the state—each bear some responsibility for Internet governance. Within the MVD, the Anti-Extremism Center (Center "E") patrols the web and refers legal violations to the courts. More than 11 agencies are authorized to blacklist webpages and platforms (see Figure 2 in the "Online Platform and Website Governance" section below). Given the plethora of institutions responsible for monitoring and regulating the Internet and the limitations of infrastructural control mechanisms, Internet governance in Russia is more fragmented and the boundaries of acceptable digital behavior are less clearly demarcated than in China (Nocetti, 2015).

In recent years, Russia has introduced a number of legal and technological innovations to its infrastructural governance strategy, such as Federal Law No. 90-FZ in 2019, which legally authorizes the government to isolate the Russian Internet from foreign information flow, among other ambitious infrastructural implementations (Gazeta.ru, 2019). External threats to the network's "confidentiality, integrity, and accessibility" could trigger the complete isolation of Russian Internet traffic by Roskomnadzor, the Federal

5. The term "Runet" is often used to denote the Russian-language subset of the cyber realm, but the term has been adopted by various stakeholders who use the term to signify different phenomena (Kolozaridi & Muravyov, 2021).

Service for Supervision of Communications, Information Technology and Mass Media (Russian Federation, 2019; Gazeta.ru 2019). Costs may be prohibitive, however. The hardware and software required to fully isolate Russia's network infrastructure is estimated at 134 billion rubles (approx. US$2.1 billion) per year (*Moscow Times*, 2019). Only 30.8 billion rubles (approx. US$530 million at avg. 2017 exchange rate) is known to be allocated to the budget as part of the 2017 "Digital Economy" project (Stadnik, 2019, p. 12), casting doubt on the realization of such an ambitious plan in practice. As Stadnik (2021) puts it, some of the "ambitious goals manifested by FZ-90 are gradually disappearing from drafts" because of various limitations, including "the current level of available hardware solutions and topology of RuNet."

Given that Russia's Internet did not develop with these centralized controls in place, some observers also question the technological feasibility of this project, pointing to the need to entirely overhaul the network infrastructure in order to achieve true full-network isolation. Internet isolation in Russia will be possible only through continued ISP cooperation (or co-optation) as a result of the current ISP market structure and proximity to network infrastructure. ISPs will continue to be required to install equipment that allows authorities to circumvent providers and thereby automatically block content and reroute Internet traffic according to the government's orders. In March 2021, Roskomnadzor began "throttling" or slowing traffic to or originating from Twitter, highlighting the state's ability to interfere with Internet service provision via co-optation of ISPs (Reuters Internet News, 2021). This marks a continuation of the trend of the Russian government's simultaneous reliance on and co-optation of ISPs in the execution of its Internet governance agenda, a theme that will be explored in greater depth below.

While full network control remains under construction, Russia has cut off regional service during periods of increased political unrest. The first instances of state-mandated regional Internet outages in Russia, legally authorized by Article 64 of the Law on Communications, occurred in 2018–19 when cellular data service was blocked in Ingushetia in response to regional unrest and calls for separatism (Kolomychenko, 2018). In June, October, and November 2018, during mass protests over a border agreement with the Republic of Chechnya, three mobile service providers staged a network blackout in response to a request from state security agencies (FH, 2018). It is suspected that similar measures were taken during protests in Moscow and in Arkhangelsk in summer 2019 (Shahbaz & Funk, 2019).

Internet Service Provider (ISP) Governance

The Russian government focuses significant attention on ISP governance through legal mandates. However, there exists a tension between the government's control of ISPs and its reliance on their cooperation. On the one hand, the state is, to a certain extent, beholden to on ISPs for executing governance of *other* network targets, given ISP proximity to the network infrastructure. For example, the state depends on ISPs' ability to cut service, filter content, and apply other Internet controls ordered by the government. On the other hand, by leveraging a significant level of control over ISPs, Russia offsets many operating costs of digital governance by requiring ISPs and other proxies to purchase and install surveillance

technologies that comply with data storage and censorship laws, and to regularly consult and execute federal blacklists (Ermoshina & Musiani, 2017, p. 44; Sivetc, 2019a, p. 44). All Internet service or telecommunications providers in Russia are licensed by Roskomnadzor.[6] Of the four main private Internet service providers (MTS, MegaFon, VEON, and Tele2), two have been taken over by Rostelecom (now the primary stakeholder), a state-owned giant in the broadband market (FH, 2019b). Due to limited competition in the ISP sector, the Russian state is able to exercise significant control over ISPs. ISPs are required to pay for and install the "System for Operative Investigative Activities" (SORM) black box, which intercepts communications traffic, allowing the FSB to present a warrant to the Ministry of Justice to seize a private citizen's data without providing any information (or a warrant) to the ISP itself (Soldatov & Borogan, 2017, p. 55). Most recently, Roskomnadzor asked ISPs "to provide information about physical Internet exchange points that they and network operators use to exchange Internet traffic," suggesting a move toward greater centralization in infrastructural governance *through* ISPs (FH, 2019b).

Roskomnadzor also requires ISPs to refer to federally-maintained blacklists or its "Unified Register" of prohibited information to block new websites and content, under penalty of fines and denial of operation.[7] Although the onus for blocking or filtering digital resources and content falls on the ISP, there is no standard approach for doing so. For instance, ISPs can utilize TCP-layer blocking, application-layer blocking facilitated by deep packet inspection (DPI), or DN manipulation to filter content. Because ISPs employ different blocking tools, a level of inconsistency and randomness is introduced that creates coverage area disparities on the one hand and on the other prevents citizens or entities from systematically circumventing these blocks (Ramesh et al., 2020, p. 2). Although the implementation of blacklisting in Russia is inconsistent, it is effective in reducing the accessibility of content overall. It is estimated that blacklisted content or sites are inaccessible to approximately 90% of Runet users (Sivetc, 2019a, p. 40).

Online Platform and Website Governance

The Russian government does not, and cannot, comprehensively govern international social media and communications platforms. Whereas China blocks most of its domestic users from accessing international sites like Google, Facebook, and Twitter through its Firewall, Russian users can and do access all but a few foreign platforms and websites. A myriad of domestic Internet platforms and products exist, including Yandex (originally a search engine that has expanded to digital media streaming, among other services), social media sites VK and Odnoklassniki, and several other media conglomerates and search engines such as Mail.ru, Rambler, and Sputnik (which closed in 2019 after five years of operation). Generally speaking, Russian citizens use a combination of domestic and foreign Internet services; for example, some Russians have both Facebook and VK

6. For a complete list of laws governing ISPs, issued by Roskomnadzor, see the Roskomnadzor page: https://rkn.gov.ru/p582/p850/p865/ (accessed 15 September 2021).

7. To access the "Unified Register," see http://eais.rkn.gov.ru/. For more about extremist digital content, see http://398-fz.rkn.gov.ru/ (accessed 15 September 2021).

accounts, despite the fact that VK is a close analog of Facebook (Nocetti, 2015). Although the Russian government cannot prevent users from accessing foreign social media platforms altogether, it does attempt—yet often falls short of—exerting influence over platforms by filing legal demands for content and user removal. According to Twitter's transparency reports on 6 June 2020, Russia had filed approximately 21% (roughly 30,000) of all global legal demands from 2012 to the present, but Twitter had complied with requests in only 14% of instances.[8]

The Russian government has made several recent attempts to bring these international platforms directly under its sphere of influence. Federal Law No. 242-FZ, spurred in part by Edward Snowden's revelations about the US government's use of personal data, was adopted in 2014 and compels providers to "store personal data of Russian citizens, used by internet services, on the territory of the Russian Federation" (Ermoshina & Musiani, 2017, p. 46). The July 2018 Yarovaia Laws modified Article 10.1(3) of the Federal Law on Information, Information Technologies and Data Protection of 2006 (149-FZ) to compel corporations operating in Russia to store users' data, including text and voice messages, photos, and videos, for up to six months (Maréchal, 2017). This provides the government with unrestricted access to troves of user data (FH, 2018, p. 15). Some foreign companies, like LinkedIn, Twitter, Google, and Facebook, have refused to comply with laws that could permit government access to users' and internal company data (FH, 2019b). Others, including Samsung, AliExpress, and PayPal, have upgraded to cloud data services to skirt the No. 242-FZ data localization law (Stadnik, 2019, p. 7). Telegram, a heavily encrypted messaging service developed in Russia but now based in Dubai, was banned by a Moscow court in 2018 for both refusing to store company data on domestic servers and refusing to provide encryption keys to the state for surveillance purposes (Griffiths, 2019, p. 270). Access to Telegram was partially and variably blocked, but in 2020 Roskomnadzor lifted restrictions completely after failing to curtail usage of the service (Reuters Technology News, 2020). The confluence of political and economic control over social media companies, such as the Mail.ru Group's purchase of VK in 2014, is another way in which domestic social media platforms are governed and their content monitored and filtered (Wijermars & Lehtisaari, 2019, p. 6).

In terms of governing the content *hosted on* platforms and websites, Russia maintains and operates a number of blacklists. The first blacklist was established in 2007 and was intended as a catalog of both digital and non-digital "extremist materials" (Sherstoboeva, 2020, p. 91). This list will be considered in more depth below. Following the 2012 Bolotnaia protests, the 2006 federal law No. 149-FZ "On Information, Information Technologies and Information Protection" was amended to include Article 15, providing for a national blacklist of digital and non-digital materials that reference suicide, drug use, child pornography, or other inappropriate content (Griffiths, 2019, p. 267). In 2013

8. For Twitter's transparency data, see https://transparency.twitter.com/en/reports/countries/ru.html (accessed 6 June 2021). For Roskomnadzor's news release detailing various international social media platform compliance rates in response to their requests for removal, see https://rkn.gov.ru/news/rsoc/news73688.htm (accessed 6 June 2021).

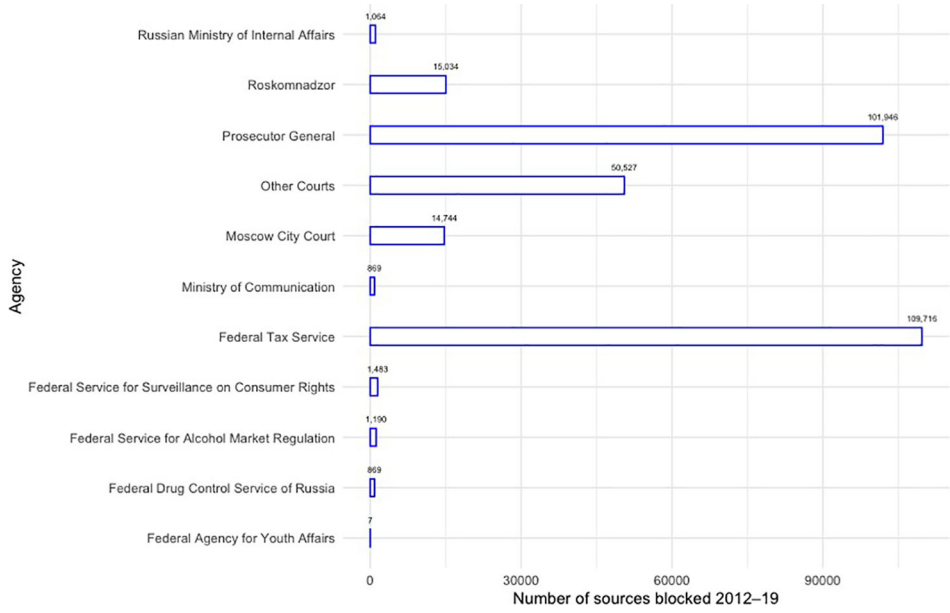

FIGURE 2. Distribution of digital blocks 2012–19 by agency. Source: AGORA Internet Freedom Report (2018).

additional federal blacklists were created under Federal Law No. 398-FZ to police piracy websites, sources promoting extremism, and those abetting unauthorized protests (Human Rights Watch, 2017; Soldatov & Borogan, 2017, p. 40). As of May 2019, approximately 4.1 million Internet resources, or 96% of blacklisted content, were blocked without any prosecution record or warrant (FH, 2019b).

Each blacklist is compiled on the basis of opaque protocols determined by the responsible governing bodies. According to statistics collected by Roskomsvoboda, a Russian NGO that promotes digital rights, between 2012 and 2019 the Prosecutor General's Office and the Federal Tax Service were the two most active contributors to the blacklists (see Figure 2). These two government bodies are responsible for moderating content related to "the threat of mass disturbance of public order . . . information offending human dignity, public morality, expressing clear disrespect for society, the state, state symbols, the Constitution, public authorities" and the "organization and conduct of gambling and lotteries," respectively.[9] In addition, two "vigilante" NGOs, Molodezhnaia Sluzhba Bezopasnosti (Youth Security Service) and Liga Bezopasnogo Interneta (Safe Internet League), patrol the Runet to alert authorities to posts that violate the cultural, political, or social standards enshrined in Russian legislation (Daucé et al., 2020, pp. 48–49).

Once a website has been blacklisted, ISPs and technology companies are legally required to block related sites and content, according to a 2006 federal law (Maréchal,

9. For more about the roles of various government entities in moderating digital content, see Roskomnadzor's 2019 "Publichnii Doklad" (Public Report) here: https://rkn.gov.ru/docs/docP_2866.pdf (accessed 15 September 2021).

2017). In this respect, the system remains decentralized, relying on both public and private providers to carry out the government's decision. In general, content flagging is conducted both automatically by detection systems and manually by the "Center E," which was created in 2008 to serve as a federal policing institution but, after the protests in 2012, expanded to include district-level police offices (Meduza, 2019b). Internet users can also propose content that should be blacklisted through a special form on Roskomnadzor's website (Sivetc, 2019b, p. 43).

The most comprehensive information on Russian blacklisting is the publicly available data from the federal "extremism list," which has been updated regularly with entries dating back to 2005. As of February 2020, it contained 4,959 entries.[10] The blacklisted entries include materials of all kinds—physical pamphlets, books, lectures, audio and video clips, websites, digital articles, and social media posts and comments. Entries are added to the list in accordance with regional court proceedings. Of the 4,959 entries, at least 215 have been labeled "excluded" (*iskliuchen*) and do not contain any identifying information or date stamp. It is unclear if this designation is meant to signify that the entry is no longer considered extremist, the relevant material has been removed, or the material is too sensitive to publicize. Materials included on the extremism list appear to be cited for a range of characteristics, from exhibiting hatred of a religious or ethnic identity, incitement to regional separatism or religious minority empowerment, historical claims contrary to regime-sanctioned histories, to criticism of President Putin and his administration.

To shed light on the content of this blacklist, we took a random sample of entries ($N = 357$, the threshold for a 95% confidence level of a population this size) to make the following observations. We find that 81% of entries in the sample were added during or after 2011. Of entries sampled, at least 64% were digital (websites, digital articles, social media videos, audio clips, posts, and comments) and approximately 20% were non-digital (brochures, books, poems, songs, and print newspaper articles); the rest of the entries were indeterminable based on the information available. Of the blacklist entries that could be definitively categorized, 54% of digital materials were found on social media sites, most (84%) of which are Russia-based platforms, such as VK and Odnoklassniki. The notable exception was content appearing on YouTube, comprising 13% of all social media entries in our sample, and 81% of international social media entries. The remaining 46% of digital materials were websites or content therein.

Though this data analysis is limited, it is highly suggestive and underscores the utility of further research in this area. Generally speaking, the extremism list entries we sampled suggest a trend toward increased restriction of contentious digital materials in the Russian information environment. The disproportionate blacklisting of Russian social media content is another interesting phenomenon we observe; perhaps it underscores the state's desire to govern its digital space as an extension of its territorial sovereignty. The choice to focus on Russian-based platforms and Russian-language posts may alternatively be

10. For updated extremism list data, see https://minjust.gov.ru/ru/extremist-materials/ (accessed 15 September 2021).

borne of resource constraints, operational challenges in deploying content flagging of non-Russian-language pages, or the state's desire not to confront international social media companies with large-scale blacklisting.

Internet User Governance

To govern Internet users, the Russian legal system relies on a series of interconnected laws, primarily amendments to the Russian Criminal Code and the Code of Administrative Offenses, focused on the information environment broadly, not just the digital realm. Some laws specifically target the Internet, however, such as the 2014 "Bloggers' Law" (Federal Law No. 97-FZ), according to which Internet users with posts visited more than 3,000 times per day were required to register their legal surname and provide other identifying information to Roskomnadzor (Human Rights Watch, 2017). In 2017, the "Bloggers' Law" was superseded by Federal Law No. 276-FZ, which "imposes on bloggers the same responsibilities and legal constraints as on the mass media without providing the same protection," and 241-FZ, which denies user anonymity in messaging services and compels ISPs to restrict user access to messaging platforms if the content of messages is suspected of violating Russian laws (Rudnick, 2017; Lonkila et al., 2019, p. 24). Online behavior is governed primarily by Criminal Code Articles 280 ("for encouraging extremist activity"), 282 ("inciting hatred"), 205.2 ("encouraging terrorist activity or public justification of terrorism"), and 148 ("insulting the feelings of believers"). Other, newer provisions such as Article 20.1 ("insulting the government"), 354.1 ("rehabilitation of Nazism"), 20.29 ("mass distribution of 'extremist materials'"), and 20.3 ("public display of banned symbols") are invoked with less frequency but exist to deter specific Internet behavior the government sees as undesirable (Human Rights Watch, 2017; Verkhovsky, 2019).

The governance of Internet users is shaped by directives from the executive branch and complex and vague legislation, and is characterized by inconsistent enforcement at the regional level. Article 282 governing hate speech, the law invoked most often in prosecutions of individuals' online behavior (represented in Figure 3 by a dotted line), reached a high of 571 invocations in 2017, but decreased to 519 in 2018 after a partial decriminalization of the law (Verkhovsky 2019). The Inter-regional Association of Human Rights Organizations "AGORA" also identifies Articles 280 "encouraging extremist activity" (solid line) and 205.2 "public justification of terrorism" (dashed line) as the next most frequent charges for online activities. Although Article 282 of the Russian Criminal Code was partially decriminalized in 2018, only a few months later more direct restrictions on freedom of speech were introduced. For instance, amendments to Article 282's "younger sister," Article 20.3.1 of the Code of Administrative Offenses ("public display of banned symbols"), have been passed, in addition to two new laws nicknamed "Klisha's Laws" targeting "fake news" and criticism of the government and Putin himself (Verkhovsky, 2019).

The sheer breadth of laws governing Internet activity provides prosecutors with a degree of autonomy in initiating and carrying out individual cases. Between 2014 and 2016, approximately 85% of convictions for "extremist expression" were made on the

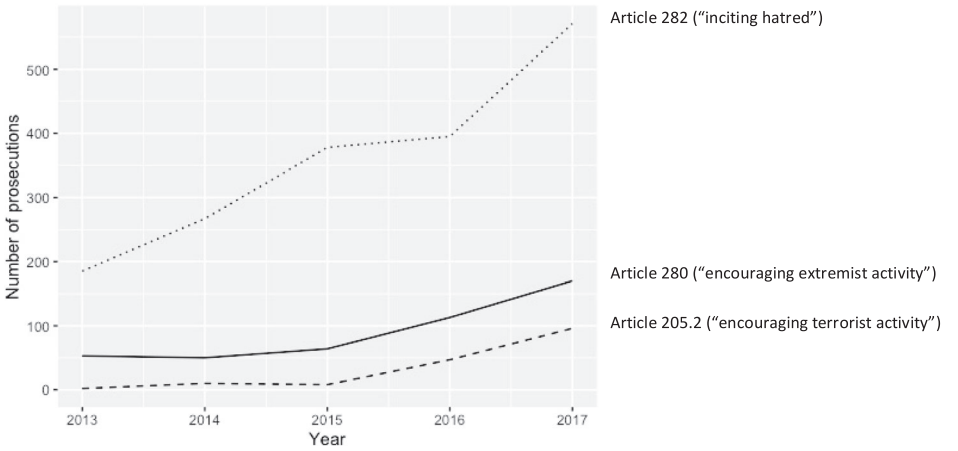

FIGURE 3. Number of prosecutions 2013–17 per article of the Russian Criminal Code. Sources: AGORA Internet Freedom Report (2018) and AGORA (2019b).

basis of online activities (Human Rights Watch, 2017). Prosecution records suggest the Russian government's Internet governance priorities and the topics it attempts to discourage on the web: most notably, criticism of President Putin,[11] his administration, the regime's policies, as well as the Russian Orthodox Church,[12] and reinterpretations of history.[13] The variation in prosecution outcomes illustrates challenges with the relative centralization and consistency of Russia's Internet governance model. AGORA and Roskomsvoboda report that in 2019, Internet users paid roughly 1 million rubles (US$15,900) in fines for insulting state officials, with Putin as the most common target (AGORA and Roskomsvoboda, 2020). These legal decisions also imply an effort to promote a uniform and state-approved interpretation of Soviet history. Moreover, they underscore that broad legal provisions are variously and inconsistently interpreted.

DIGITAL AUTHORITARIANISM COMPARED: RUSSIA AND CHINA

China's Internet governance model has come to represent digital authoritarianism writ large, even though, as we demonstrate, the strategies and implementation of Internet governance are diverse across regimes. The Internet governance framework underscores

11. The first individual charged under Article 20.1.3 of the Code of Administrative Offenses was fined 30,000 rubles (approx. US$500) for posting "Putin is an incredible f . . . wit" (Baumgartner, 2019).

12. One woman charged for posting a religious-themed meme on VK successfully counter-sued, receiving 100,000 rubles and an apology from the prosecutor's office (Robinson, 2018; AGORA, 2019).

13. According to the 2016 federal decree on Internet security, one of the "strategic goals and main directions of ensuring information security" is the "neutralization of the information-psychological impact, aimed at undermining the historical foundations and patriotic traditions associated with the defense of the Fatherland" (Russian Federation, 2016). For example, in 2016, a Russian user was convicted of "falsifying history" after reposting an article on VK suggesting the Soviet Union bore some responsibility for the start of WWII by invading Poland (AGORA, 2019; Human Rights Watch, 2017).

the variety of control mechanisms leveraged on each network target and allows us to interrogate the differences among models. We find that there are two major differences between the Russian and Chinese models: Russia's institutional oversight of its digital information environment is less centralized and therefore appears less consistent than China's, and the Russian Internet governance model is more reactive and has undergone more recent and rapid change, including the emphasis on digital, less-visible control mechanisms. The question remains whether these varieties of digital authoritarianism are likely to persist or if these two models will instead ultimately converge, as Russia's approach becomes more similar to China's.

Centralization and Coherence of Internet Governance

Whereas China's Internet governance strategy can be characterized as centralized in its hardware and software capabilities, the Russian model is significantly more decentralized in both respects (King et al., 2013; Ramesh et al., 2020). The Chinese network includes centralized "choke points" for more widespread Internet control (Ramesh et al., 2020, p. 1), meaning physical sections of the network infrastructure in which the state restricts data flow and can prohibit user access. In contrast, Russia lacks these choke points and relies instead on ISPs to block or filter content, sites, or users based on federally-maintained blacklists that must be frequently updated. Russia's governance of the Internet hinges on the successful co-optation of ISPs and other digital media platforms, whereas in China, the state itself possesses direct tools to control network infrastructure.

The degree of network infrastructure centralization in each country also determines the apparent level of administrative consistency of each Internet governance model. The Chinese model appears more comprehensive and consistent in its domain and content blocks and political administration of the Internet than its Russian counterpart. For example, researchers found that the Chinese Firewall reliably blocks inappropriate content (such as references to suicide, drug abuse, and other socially discouraged concepts), in addition to implications of political mobilization (Creemers, 2016; King et al., 2013; Weber, 2019). In contrast, the Russian model shows some stark points of inconsistency, such as variation in how policies are implemented, disparities between regional judiciaries and the executive, and changes in types of Internet control mechanisms applied over time. An analysis of the federal extremism blacklist yields a somewhat inconsistent picture of blacklisting standards in the type and frequency of content removal. Furthermore, it remains unclear how and why some individuals are prosecuted for digital content deemed illegal whereas others are spared and why outcomes of trials vary depending on the regional court. Lastly, because content filtration occurs at the ISP level and ISPs employ different blocking software and hardware tools, censorship manifests differently depending on the service provider and location of service (Ermoshina & Musiani, 2017, p. 50).

Rapid and Recent Change in Digital Governance in Russia

Whereas China adopted an interventionist approach from the initial extension of digital opportunities to Chinese citizens, Russia only belatedly developed more-concerted

TABLE 1. Comparative Timeline of Internet Laws in Russia and China

Target of network governance	Internet infrastructure	Internet service providers	Online platforms and websites	Internet users
Type of law	Internet isolation capability	Official ISP registration/ liability	Blacklist creation	Blogger registration
China	1996	2000	1996	2005
Russia	2019*	2006	2012	2014

Sources: Human Rights Watch, 2017; King et al., 2013; Creemers, 2016.
*Full Russian network isolation has not yet been realized.

Internet governance strategies. This appears to be the source of the most enduring differences between the two Internet governance models, as network infrastructure is extremely difficult to reconstruct after the fact. As a result, Russia's approach to Internet government historically has been reactive and more ad hoc. While this less comprehensive approach may have some disadvantages, it also is less resource intensive. Russia's recent, rapid expansion of Internet governance is illustrated by a comparison of the timing of legislation adopted to govern each network target in both Russia and China in Table 1. Internet isolation is the best representation of governance at the infrastructural level. Blacklist creation is a good indicator of online platform and website governance.[14] The registration and legal liability placed on ISPs as well as blogger registration laws serve as the comparative legal standards across countries at the ISP and Internet user levels of governance.

For each target of Internet governance, China was first to develop a law governing said target. While most of China's Internet governance laws were introduced in the 1990s and early 2000s, Russia's were established much later, mostly after the 2011 protests. China introduced legislation to govern the network infrastructure in 1996, but analogous legislation was only introduced in Russia with the 2019 Internet Isolation Law. Perhaps of particular importance is the fact that Russia's attempts to govern its Internet infrastructure came decades later than China's, but its ISP laws were not as delayed. Russia's belated emphasis on infrastructural control is challenged by a diverse Internet environment in which domestic and international ISPs and online platforms and websites have operated with relative freedom for decades, making authorities' centralized and universal crackdown on the Internet more difficult.

Russia's more recent emphasis on governing its network infrastructure signifies a broader trend toward less visible, more technical digital control mechanisms. Data in Table 2, aggregated from yearly reports by AGORA International Rights Group and Roskomsvoboda, depict the complex changes in Russian Internet

14. In Russia, individuals can also be blacklisted, but the 2012 blacklist law specifically governs websites and content therein.

TABLE 2. Digital and Non-Digital Mechanisms of Internet Governance in Russia 2015–19

Mechanism type	Control mechanism	2015	2016	2017	2018	2019
Non-digital (legislative, judicial, extra-judicial)	Regulatory proposals (Legislative)	48	97	114	82	62
	Criminal investigations	202	298	411	384	200
	Civil suits	49	170	39	58	79
Digital	Blacklisting by government entities	7,300	24,000	2,196	161,171	272,785
	Impediment of access to web resources*	1,721	35,019	88,832	488,609	161,490
	Government-ordered Internet shutdowns	N/A	N/A	N/A	N/A	8

Source: Internet Freedom in 2018 and 2019 Reports, AGORA and Roskomsvoboda.

* This category of data provided by Roskomsvoboda and AGORA in their annual Internet Freedom reports includes content on Runet that social media companies decide to remove due to a variety of reasons, but independent of formal government demands or the web resource's inclusion on a blacklist.

governance mechanisms between 2015 and 2019 (AGORA and Roskomsvoboda 2020).[15]

Some of the shifts in a variety of control mechanisms utilized by the Russian government in the last four years are striking, perhaps pointing to the lack of consistent governance or rather a shift in governance focus over time toward more digital governance mechanisms. The number of "regulatory proposals," including proposals for legal amendments or new bills, has varied from year to year with a high of 114 in 2017. Whereas the utilization of such non-digital control mechanisms has decreased over time, the incidence of digital mechanisms of Internet control has significantly increased in the same period. The documented evidence of impediments to web access and blacklisting of platforms and content by government entities has surged since 2016. Since 2018 regional service blackouts have been executed in both Ingushetia and Moscow. Meanwhile, after an increase in 2015, instances of "civil suits" have decreased by 53% since 2016. This data suggests a trend toward the greater use of less visible, digital mechanisms (such as blacklists, automated filters, and access restrictions) by government entities in place of more traditional, non-digital legislation and enforcement through prosecution. This hypothesis is supported by scholars such as Sivetc, who argue that governments prefer to govern their Internet space with more informal infrastructural controls than by formal legal mechanisms (Sivetc, 2019a, p. 28).

THE FUTURE OF INTERNET GOVERNANCE: ENDURING DIFFERENCES OR EVENTUAL CONVERGENCE?

In light of the recent and rapid changes to Russia's Internet governance, is it likely to remain a distinct model of digital authoritarianism or are we witnessing a convergence of

15. For a complete list of each cataloged governance mechanism, see the full 2019 report and accompanying spreadsheet by Roskomsvoboda and AGORA (available in Russian and English).

the two approaches? In other words, has this analysis captured persistent or fleeting differences in these countries' approaches to Internet governance? On the one hand, Internet governance strategies may grow more similar as Russia develops its use of less visible, digital controls in keeping with the Chinese model and attempts to construct more comprehensive and consistent Internet governance over time. On the other hand, growing similarity in digital governance could be limited by the entrenchment of international social media platforms in Russia, public opposition to digital censorship, and the relative dearth of investment in cutting-edge technology by Russia.

The case for persistent differences is rooted in path dependence. Russia's Internet governance model developed in conjunction with international Internet services and platforms that are less accountable to the state. Whereas the Chinese digital realm was governed in a top-down fashion from the late 1980s onward, Russian Internet governance originated much later, intensifying around 2011. As a result, convergence with the more extensive Chinese style of governance may be impossible without costly disruption to the existing technological infrastructure and the potential political backlash of cracking down on user freedoms. Soldatov and Borogan argue that Russia's relatively late engagement with Internet governance is a missed opportunity for coevolution with the technology: "Attacks on Internet freedom began only in the summer of 2012, by which time RuNet already had its key characteristics: its infrastructure was built on Western technology, and filtering and blocking functions were not initially laid in its foundation. Moreover, RuNet did not grow up inside the 'great firewall,' nor did an army of government censors follow every step of local Internet users" (Soldatov & Borogan, 2017, p. 56).

Moreover, the Chinese government also has overseen the development of countless domestic alternatives to Western social media platforms and information providers from an early stage. In contrast, Russian citizens have enjoyed decades of access to international Internet resources and services, many of which flout Russian legislation and data storage requirements. While domestic Russian social media platforms like VK and Odnoklassniki are more popular on average than foreign platforms like YouTube, Facebook, WhatsApp, and Instagram, the latter remain a significant part of the media market in Russia, unlike in China.[16] Perhaps due to the relative freedom of access that Russian Internet users have enjoyed for decades, Russian citizens express strong opposition to censorship. According to a 2015 Pew Research Center survey, as many as 79% of Russians say it is at least somewhat important "that people can use the Internet without state/government censorship in our country," only a few percentage points lower than Britons (82%) and Americans (91%) surveyed in the same poll (Wike, 2016). In the long run, the Russian public's desire for Internet freedom, manifested as access to a variety of international and domestic social media platforms and news sources, may limit the state's ability to impose *visible* restrictions while maintaining regime legitimacy and stability.

16. For more about trends in the Russian media space, see this 2020 Levada Center Report: https://www.levada.ru/2020/05/20/rossijskij-medialandshaft-2020-2/.

Third, Russian digital governance may also be limited by the relatively small investment in the information and communications technologies (ICT) sector and cutting-edge technology. Even today, China's global ICT exports greatly outstrip Russia's. According to the OECD, Russia's ICT goods exports totaled $1.634 billion (under half a percent of its GDP) compared to China's approximately $550 billion (over 2% of its GDP) in 2019 (OECD, 2020b). China surpasses Russia by orders of magnitude not only in ICT goods exports but also in research and development expenditures. Whereas in 2018 China spent approximately $526 billion—nearly 2.2% of its much larger total GDP—on R&D, Russia spent just shy of 1%, or $36.4 billion, of its GDP (OECD, 2020a). Without prioritizing domestic technology innovation and export, Russia may be limited in its ability to expand domestic and international surveillance and censorship.

Despite these significant obstacles that have led to a more decentralized and less costly Russian Internet governance strategy, recent changes have suggested a trend toward less publicly visible, more technologically sophisticated control mechanisms, a trend that shares some similarity with China's governance strategy. Whereas more traditional mechanisms like legislation and prosecutions can be tracked and monitored by watchdog groups, digital restrictions like sophisticated infrastructural changes are difficult to detect and less comprehensible to the average Russian citizen. For example, the full realization of a sovereign Runet would require an overhaul of Russia's present digital infrastructure, but would be mostly out of the view of the average Russian citizen, unlike laws and prosecutions. It remains to be seen whether the Russian model for Internet governance will eventually converge on the centralized Chinese model or remain decentralized and distinct. It is possible that the Russian regime will increase its capacity to control the Internet's impact on society. Scholars still debate whether it is the case that, "rather than the Internet having transformed Russia, it was Russia that adapted the Internet to fit its values" (Sherstoboeva, 2020, p. 90).

Whether Russia's approach to Internet governance represents a durable model or simply captures the efforts of a less centralized political system aspiring to China's level of digital control, elements of both governance strategies, such as laws and mechanisms of governance and Internet technology components, have been exported to other authoritarian regimes. Polyakova and Meserole assert that "at least 18 countries currently use Chinese surveillance and monitoring systems, and at least 36 governments have held Chinese-led trainings and seminars on 'new media' or 'information management'" (Polyakova & Meserole, 2019, p. 6; Deibert & Rohozinski, 2010). Russia's more decentralized control strategy is more cost-effective and flexible, and therefore can be adapted to a variety of regimes. Components of the Russian SORM technologies and elements of its legal regime for Internet governance have been exported in part to all former Soviet republics, except Armenia, Georgia, and the Baltic states (Deibert & Rohozinski, 2010; Polyakova & Meserole, 2019, p. 10).

Although decentralized Internet governance models long have been considered less powerful or effective than centralized systems such as those of China or Iran, in some ways the cheaper and less comprehensive Russian model serves as a "blueprint" for other countries to adopt digital authoritarian controls in which "large-scale censorship can be

achieved in decentralized networks through inexpensive commodity equipment" (Ramesh et al., 2020, p. 1). Russia's model allows the state to offset software and hardware costs onto proxies, including ISPs, and, because ISPs use different blocking tools, there is a level of inconsistency and randomness that prevents systematic circumvention (Ramesh et al., 2020, p. 2). However, as noted above, reliance on ISPs for implementation of Internet regulations often leads to inconsistent execution of control mechanisms, and can ultimately prevent a complete and successful execution of Internet isolation.

CONCLUSION

Digital authoritarianism poses a threat not just to domestic citizens but also to the global Internet infrastructure and users around the world. To thoroughly assess digital governance mechanisms utilized by democratic and undemocratic regimes alike, we devised an analytical framework that conceptualizes Internet governance as a series of mechanisms directed at different targets, from network infrastructure to individual users. This framework unites technical and nontechnical approaches to Internet governance, can be applied in any case or regime type, and enables direct and detailed comparison of specific targets. Our approach also accounts for a state's capacity to govern the Internet using tools that are both highly visible to the public and more traditional (such as laws) and those that are more technologically advanced and surreptitious (such as a variety of blacklisting and filtration tools and full isolation). A comparative analysis of China and Russia using this framework reveals several notable differences in the models: the extent and relative degree of centralization in Internet governance and a proactive versus reactive approach to governance. Our analytical framework contributes a more nuanced understanding of Russian Internet governance in its own right, instead of as a lesser version of the more extreme and widely studied Chinese case.

The trend toward less visible, more technologically advanced mechanisms of Internet governance in Russia is emblematic of a global phenomenon that endangers domestic citizens' access and contribution to the digital information environment. In addition, due to the global reach of the Internet, the extraterritorial effects of domestic legislation in Russia and China are stark and will become more dire for Internet users of all nationalities. For example, data localization laws that require US-incorporated social media companies to store data on local servers under domestic surveillance potentially jeopardize the privacy of millions of Internet users. Many Internet users are not even aware that their data are stored in other localities and are subject to surveillance by foreign governments.

As technology becomes increasingly intertwined with politics, all regimes strive to govern their domestic Internet, including their citizens' online speech, blurring the line between democratic and authoritarian Internet governance. The number of digital authoritarian tools at *any* regime's disposal is increasing rapidly, including tools that evade detection by most citizens. Similarly, the global proliferation of surveillance technologies will provide states with a trove of data on Internet users' opinions, fears, and

motivations, enabling even more customized and clandestine censorship and behavior modification.

Nevertheless, specific forms of Internet governance will vary based on regime type and state capacity, even among authoritarian regimes. For example, different varieties of authoritarianism have different legitimation strategies—whether based on ideology, personal rule, economic performance, or security. These features shape motivations for the use of tools to control digital spaces. Guriev and Treisman (2019) have argued that "informational autocrats" can perpetuate their rule by exploiting "the gap in political knowledge between the 'informed elite' and the general public" (p. 101). This flexible method of rule can be combined with different political messages and narrowly targeted at different audiences—such as to enhance perceptions of regime competence (Guriev & Treisman 2019, p. 102). Alternatively, Xu (2021) finds that authoritarians can use information from digital surveillance in "resolving their information problem in identifying radical opponents and enabling them to substitute preventive repression for co-optation to prevent social unrest" (p. 323). Future research on varieties of authoritarianism should encompass studies on Internet governance and digital authoritarianism more generally.

We have demonstrated the ways in which authoritarian regimes' Internet governance models can differ based on the targets and mechanism of governance prioritized. The Internet governance framework allows for systematic cross-national comparison of various models. Careful comparative studies of Internet governance models of like and disparate regime types have the potential to propel the interdisciplinary research field and increase public understanding of digital authoritarianism. In addition, one of the many remaining gaps in scholarship of Russian digital authoritarianism is in determining the future trajectory of Internet governance, especially vis-à-vis China's model. The development of Russia's Internet governance model over time may serve to predict trends in other countries that have already adopted a similar, decentralized model and have acquired Russian security technologies. ■

ACKNOWLEDGMENTS

The authors would like to thank Henry Laurence, Aki Nakai, Michael Hawley, and Sasa Jovanovic for their helpful comments on earlier versions of this manuscript.

Corresponding author email: lhenry@bowdoin.edu

REFERENCES

AGORA. (2019) Svoboda Interneta 2018: Delegirovanie Repressii [Internet Freedom 2018: Delegation of repression]. Available from: https://agora.legal/articles/Doklad-Mezhdunarodnoi-Agory-%C2%ABSvoboda-Interneta-2018-delegirovanie-repressiy%C2%BB/18 [Accessed 5 February 2019].

AGORA and Roskomsvoboda. (2020) Svoboda Interneta 2019: Plan "Krepost" [Internet freedom 2019: "Fortress" Plan]. Available from: https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf [Accessed 4 February 2020].

Barme, G., & Ye, S. (1997) The Great Firewall of China. https://www.wired.com/1997/06/china-3/ [Accessed 29 August 2021].
Baumgartner, P. (2019) Curb your criticism? First Russian fined for "disrespecting" Putin doubles down on critique of president. RFE/RL, 25 April. Available from: https://www.rferl.org/a/first-russian-fined-for-disrespecting-putin-doubles-down-on-critique-of-president/29903929.html [Accessed 29 August 2021].
Black, J. (2005) What is regulatory innovation? In: Black, J., Lodge, M. & Thatcher, M (eds.) *Regulatory innovation*. Cheltenham, UK, Edward Elgar Publishing. Available from: https://EconPapers.repec.org/RePEc: elg: eechap:3769_1 [Accessed 29 August 2021].
Brancati, D. (2014) Democratic authoritarianism: Origins and effects. *Annual Review of Political Science*. 17 (1), 313–326.
Chang, E. & Golden, M. A. (2010) Sources of corruption in authoritarian regimes. *Social Science Quarterly*. 91 (1), 1–20.
Chi, E. (2012) The Chinese government's responses to use of the Internet. *Asian Perspective*. 36 (3), 387–409.
China Digital Times. (2013) Xi Jinping, "Speech at the National Ideology and Propaganda Work Conference," 4 November. Available from: http://chinadigitaltimes.net/chinese/2013/11/ [Accessed 29 August 2021].
Creemers, R. (2016) Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*. 26 (103), 85–100.
Daucé, F., Loveluck, B., Ostromooukhova, B. & Zaytseva, A. (2020) From citizen investigators to cyber patrols: Volunteer Internet regulation in Russia. *Laboratorium: Russian Review of Social Research*. 11 (3), 46–70.
Deibert, R. & Crete-Nishihata, M. (2012) Global governance and the spread of cyberspace controls. *Global Governance*. 18 (3), 339–361.
Deibert, R. & Rohozinski, R. (2010) Control and subversion in Russian cyberspace. In: Palfrey, J. & Zittrain, J. (eds.) *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA, MIT Press. Available from: https://doi.org/10.7551/mitpress/8551.003.0007 [Accessed 29 August 2021].
Diamond, L. (2002) Thinking about hybrid regimes. *Journal of Democracy*. 13 (2), 21–35.
Ermoshina, K. & Musiani, F. (2017) Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era. *Media and Communication*. 5 (1), 42–53.
Faulconbridge, G. (2014) Father of Web tells Russia's Putin: Internet is not a "CIA project." Reuters. Available from: https://www.reuters.com/article/us-web-russia-putin/father-of-web-tells-russias-putin-Internet-is-not-a-cia-project-idUSKBN0JP1E420141211 [Accessed 29 August 2021].
Freedom House (FH). (2018) Freedom on the Net 2018. *Freedom on the Net Annual Reports*. Available from: https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf [Accessed 15 September 2021].
Freedom House (FH). (2019a) Freedom on the Net 2019: The crisis of social media. *Freedom on the Net Annual Reports*. Available from: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf [Accessed 15 September 2021].
Freedom House (FH). (2019b) Freedom on the Net 2019: Russia country report. *Freedom on the Net Annual Reports*. Available from: https://freedomhouse.org/country/russia/freedom-net/2019 [Accessed 15 September 2021).
Gandhi, J. & Przeworski, A. (2007) Authoritarian institutions and the survival of autocrats. *Comparative Political Studies*. 40 (11), 1279–1301.
Gazeta.ru. (2019) Finishnaia priamaia: Sovfed odobril zakon o nadezhnom Runete [The home stretch: The Federation Council approved the Law on Reliable Runet]. Available from:

https://www.gazeta.ru/tech/2019/04/22/12315799/sovfed_runet.shtml?updated [Accessed 22 April 2019].
Geddes, B. (1999) What do we know about democratization after twenty years? *Annual Review of Political Science*. 2, 115–144.
Gerschewski, J. (2013) The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. *Democratization*. 20 (1), 13–38.
Griffiths, J. (2019) *The Great Firewall of China: How to build and control an alternative version of the Internet*. London, Zed Books.
Guriev, S. & Treisman, D. (2019) Informational autocrats. *Journal of Economic Perspectives*. 33 (4), 100–127.
Howard, P. N., Agarwal, S. D. & Hussain, M. M. (2011) The dictators' digital dilemma: When do states disconnect their digital networks? *Issues in Technology Innovation*. Available from: https://www.brookings.edu/wp-content/uploads/2016/06/10_dictators_digital_network.pdf [Accessed 29 August 2021].
Human Rights Watch. (2013) China: Draconian legal interpretation threatens online freedom. Available from: https://www.hrw.org/news/2013/09/13/china-draconian-legal-interpretation-threatens-online-freedom [Accessed 29 August 2021].
Human Rights Watch. (2017) Online and on all fronts: Russia's assault on freedom of expression. Available from: https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression [Accessed 15 September 2021].
Human Rights Watch. (2020) Russia: Growing Internet isolation, control, censorship. Available from: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship [Accessed 29 August 2021].
Huntington, S. P. (2009) How countries democratize. *Political Science Quarterly*. 124 (1), 31–69.
Iasiello, E. (2017) China's cyber initiatives counter international pressure. *Journal of Strategic Security*. 10 (1), 1–16.
Kedzie, C. (1997) Communication and democracy: Coincident revolutions and the emergent dictators (doctoral dissertation), Rand Corporation. Available from: https://www.rand.org/pubs/rgs_dissertations/RGSD127/sec2.html [Accessed 29 August 2021].
Kharpal, A. (2019) Everything you need to know about WeChat—China's billion-user messaging app. CNBC, 4 February. Available from: https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html [Accessed 29 August 2021].
King, G. Pan. J. & Roberts, M. E. (2013) How censorship in China allows government criticism but silences collective expression. *American Political Science Review*. 107 (2), 326–343.
Kolomychenko, M. (2018). Russia stifled mobile network during protests: Document. Reuters. Available from: https://www.reuters.com/article/us-russia-protests-Internet/russia-stifled-mobile-network-during-protests-document-idUSKCN1NL1I6 [Accessed 29 August 2021].
Kolozaridi, P. & Muravyov, D. (2021) Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case. *First Monday*. 26 (5). Available from: https://doi.org/10.5210/fm.v26i5.11687 [Accessed 29 August 2021].
Kolton, M. (2017) Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence. *Cyber Defense Review*. 2 (1), 119–154.
Krönke, C., Müller, M. W., Wenguang, Y. & Wei, T. (eds.) (2018) Introduction: Paradigms of Internet regulation in the European Union and China. In: Müller, M. W., Krönke, C., Yu, W. & Tian, W. (eds.) *Paradigms of Internet regulation in the European Union and China*. Baden-Baden, Nomos Verlagsgesellschaft, pp. 15–31.
Lam, W. W.-L. (2013) China: State power versus the Internet. In: Williams, L. & Rich, R. (eds.) *Losing control: Freedom of the press in Asia*. Canberra, Australia, ANU Press, pp. 37–57.
Laskai, L. (2017) "Nailing jello to a wall." In: Golley, J., Jaivin, L. & Tomba, L. (eds.) *Control*. Canberra, Australia, ANU Press, pp. 191–208.

Levitsky, S. & Way, L. (2002) The rise of competitive authoritarianism. *Journal of Democracy*. 13 (2), 51–65.
Lonkila, M., Shpakovskaya, L. & Torchinsky, P. (2019) The occupation of Runet? The tightening state regulation of the Russian-language section of the Internet. In: Wijermars, M. & Lehtisaari, K. (eds.) *Freedom of expression in Russia's new mediasphere*. Abingdon, UK, Routledge, pp. 17–38.
Lu, J. & Zhao, Y. (2018) Implicit and explicit control: Modeling the effect of Internet censorship on political protest in China. *International Journal of Communication*. 12, 3294–3316.
MacKinnon, R. (2011) China's "Networked Authoritarianism." *Journal of Democracy*. 22 (2), 32–46.
Maréchal, N. (2017) Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*. 5 (1), 29–41.
Marsden, C. T. (2011) *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*. Cambridge, Cambridge University Press.
Meduza. (2019b) What is Center E? A former agent for Russia's secretive anti-extremism center explains how "Eshniki" crack down on protesters and prosecute online activity. Available from: https://meduza.io/en/feature/2019/08/29/what-is-center-e [Accessed 29 August 2021].
Miao, W., Zhu, H. & Chen, Z. (2018) Who's in charge of regulating the Internet in China: The history and evolution of China's Internet regulatory agencies. *China Media Research*. 14 (3), 1–7.
Ministry of Justice of the Russian Federation. (2019) Extremism List [Spisok Ekstremistov]. Available from: http://data.gov.ru/opendata/7707211418-spisokekstremistov [Accessed 29 August 2020].
Moscow Times. (2019) Russia moves to grant government the power to shut down the Internet, explained. Available from: https://www.themoscowtimes.com/2019/02/12/russia-moves-grant-government-power-shut-down-Internet-explained-a64470 [Accessed 29 August 2021].
Mueller, M. (2010) *Networks and states: The global politics of Internet governance*. Information Revolution and Global Politics series. Cambridge, MA, MIT Press.
Müller, M. W. (2018) Mapping paradigms of European Internet regulation. In: Müller, M. W., Krönke, C. Yu, W. & Tian, W. (eds.) *Paradigms of Internet regulation in the European Union and China*. Baden-Baden, Nomos Verlagsgesellschaft, pp. 31–49.
Münkler, L. (2018) Space as a paradigm of Internet regulation. In: Müller, M. W., Krönke, C., Yu, W. & Tian, W. (eds.) *Paradigms of Internet regulation in the European Union and China*. Baden-Baden, Nomos Verlagsgesellschaft, pp. 139–158.
Nathan, A. (2003) Changing of the guard: Authoritarian resilience. *Journal of Democracy*. 14 (1), 6–17.
Nocetti, J. (2015) Contest and conquest: Russia and global Internet governance. *International Affairs*. 91 (1), 111–130.
Organisation for Economic Co-operation and Development (OECD). (2020a). Gross domestic spending on R&D. Available from: https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm [Accessed 29 August 2021].
Organisation for Economic Co-operation and Development (OECD). (2020b) ICT goods exports. Available from: https://data.oecd.org/ict/ict-goods-exports.htm [Accessed 15 September 2021].
Polyakova, A. & Meserole, C. (2019) Exporting digital authoritarianism. Available from: https://www.brookings.edu/research/exporting-digital-authoritarianism/ [Accessed 29 August 2021].
Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., Sprecher, S., Ikram, M. & Ensafi, R. (2020) Decentralized control: A case study of Russia. Paper presented at the Network and Distributed Systems Security (NDSS) Symposium 2020, San Diego, CA, 23–26 February.
Reuters Internet News. (2021) Russia extends punitive Twitter slowdown until mid-May. Available from: https://www.reuters.com/article/us-russia-twitter/russia-extends-punitive-twitter-slowdown-until-mid-may-idUSKBN2BS0GT [Accessed 29 August 2021].

Reuters Technology News. (2020) Russia lifts ban on Telegram messaging app after failing to block it. Available from: https://www.reuters.com/article/us-russia-telegram-ban-idUSKBN23P2FT [Accessed 29 August 2021].

Roberts, M. (2018) *Censored: Distraction and diversion inside China's Great Firewall*. Princeton, NJ, Princeton University Press.

Robinson, O. (2018) The memes that might get you jailed in Russia. BBC, 23 August. Available from: https://www.bbc.com/news/blogs-trending-45247879 [Accessed 29 August 2021].

Rudnik, P. (2017) Russia: New legislation restricts anonymity of Internet users. Library of Congress Global Legal Monitor. Available from: https://www.loc.gov/law/foreign-news/article/russia-new-legislation-restricts-anonymity-of-internet-users/#:˜: text=276%2DFZ%20of%20July%2029, information%20resources%20that%20are%20designated [Accessed 29 August 2021].

Russian Federation. (2016). Federal decree: Information Security Doctrine of the Russian Federation. Office of the President of the Russian Federation. Available from: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html [Accessed 27 September 2021].

Russian Federation. (2019) On approval of the Procedure for Centralized Management of the Public Communication Network. Government of the Russian Federation. Available from: http://publication.pravo.gov.ru/Document/View/0001202002170013 [Accessed 4 November 2021].

Schedler, A. (2002) The menu of manipulation. *Journal of Democracy*. 13 (2), 36–50.

Shahbaz, A. & Funk, A. (2019) Freedom on the Net 2019. *Freedom on the Net Annual Reports*. Available from: https://www.freedomonthenet.org/country/russia/freedom-on-the-net/2019 [Accessed 29 August 2021].

Sherstoboeva, E. (2020) Regulation of online freedom of expression in Russia in the context of the Council of Europe Standards. In: Davydov, S. (ed.), *Internet in Russia: An integral study of the Runet and its impact on social life*. City University of Hong Kong School of Law Legal Studies Research Paper No. 2020-004, pp. 83–100.

Sivetc, L. (2019a) State regulation of online speech in Russia: The role of internet infrastructure owners. *International Journal of Law and Information Technology*. 27 (1), 28–49.

Sivetc, L. (2019b) The blacklisting mechanism. In: Wijermars, M. & Lehtisaari, K. (eds.) *Freedom of expression in Russia's new mediasphere*. Abingdon, UK, Routledge, chapter 2, pp. 17–38.

Slater, D. & Fenner, S. (2011) State power and staying power: Infrastructural mechanisms and authoritarian durability. *Journal of International Affairs*. 65 (1), 15–29.

Soldatov, A. & Borogan, I. (2017) *The red web: The Kremlin's war on the Internet*. 2nd ed. New York, Hachette Book Group

Stadnik, I. (2019) Internet governance in Russia: Sovereign basics for independent Runet. Paper presented at TPRC47: The 47th Research Conference on Communication, Information and Internet Policy. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421984 [Accessed 15 September 2021].

Stadnik, I. (2021). Control by infrastructure: Political ambitions meet technical implementations in RuNet. *First Monday* 26 (5). Available from: https://doi.org/10.5210/fm.v26i5.11693 [Accessed 29 August 2021].

Tkacheva, O., Schwartz, L. H., Libicki, M. C., Taylor, J. E., Martini, J. & Baxter, C. (2013) The Internet in China: Threatened tool of expression and mobilization. *Internet Freedom and Political Space*. Santa Monica, CA, RAND Corporation, pp. 93–118.

Verkhovsky, A. (2019) A new turn of the Kremlin's anti-extremist policy. *PONARS Policy Memos*. Available from: http://www.ponarseurasia.org/point-counter/article/new-turn-kremlins-anti-extremist-policy [Accessed 29 August 2021].

Weber, V. (2019) The Worldwide Web of Chinese and Russian information controls. Working paper, Centre for Technology and Global Affairs, University of Oxford. Available from: https://www.ctga.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf [Accessed 29 August 2021].

Wijermars, M. & Lehtisaari, K. (eds.) (2019) Introduction. In: Wijermars, M. & Lehtisaari, K. (eds.) *Freedom of expression in Russia's new mediasphere*. Abingdon, UK, Routledge, pp. 1–14.

Wike, R. (2016) Broad support for Internet freedom around the world. *Pew Research Center Reports*. Available from: https://www.pewresearch.org/fact-tank/2016/02/23/broad-support-for-Internet-freedom-around-the-world/ [Accessed 29 August 2021].

Williams, L. (2013) Censors at work, censors out of work. In: Williams, L. & Rich, R. (eds.) *Losing control: Freedom of the press in Asia*. Canberra, Australia, ANU Press, pp. 1–15.

Xinhua. (2019) China to lead global cybersecurity market growth in next 5 years. Available from: http://www.china.org.cn/business/2019-09/09/content_75186972.htm [Accessed 29 August 2021].

Xu, X. (2021) To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science*. 65 (2), 309–325.

Xuan, C. (2018) Boundary of criminal responsibility of Internet service providers. In: Müller, M. W., Krönke, C., Yu, W. & Tian, W. (eds.) *Paradigms of Internet regulation in the European Union and China*. Baden-Baden, Nomos Verlagsgesellschaft, pp. 69–82.

Yang, F. & Mueller, M. L. (2019) Internet governance in China: A content analysis. In: Yu, J. & Guo, S. (eds.), *The Palgrave handbook of local governance in contemporary China*. Singapore, Springer, pp. 441–463.