2020

# Digital Authoritarianism in China and Russia: A Comparative Study

Laura H.C. Howells
*Bowdoin College*

# Digital Authoritarianism in China and Russia: A Comparative Study

An Honors Paper for the Department of Government and Legal Studies

By Laura H.C. Howells

Bowdoin College, 2020

To my parents, brother, and everyone at Bowdoin who provided encouragement and feedback along the way

**Table of Contents:**

# ACKNOWLEDGEMENTS

I would like to express deep gratitude to my advisor Professor Laura Henry and committee members Professor Aki Nakai and Professor Henry Laurence. Their expertise and perspectives were invaluable to the realization of this honors thesis.

I owe a special thank you also to Lynne Atkinson, Bowdoin Government and Legal Studies Department Coordinator and friend to many, for her endless wisdom and encouragement.

And finally, thank you to the faculty of the Bowdoin Russian Department for kindling my interest in Russian language and culture and preparing me to conduct primary research in the target language.

# ABSTRACT

Digital authoritarianism is on the rise around the world and threatens the data privacy and rights of both domestic and international Internet users. However, scholarship on digital authoritarianism remains limited in scope and case study selection. This study contributes a new, more comprehensive analytical framework for the study of Internet governance and applies it to the case studies of China and Russia. Special attention is paid to the still understudied Russian Internet governance model. After thorough literature review and novel data collection and analysis, this paper identifies relative centralization of network infrastructure and the extent and pace of change in governance as the most notable differences between the two models. These points of divergence may be explained by two theories; the varieties of authoritarianism hypothesis posits that different political systems face persistent and unique constraints to governance of the digital realm. The development trajectory theory argues that each country's technological development path foreshadows the systems' capacity for and extent of governance. This study is among the first to distinguish between Internet governance models of authoritarian regimes.

## INTRODUCTION TO DIGITAL AUTHORITARIANISM AND INTERNET GOVERNANCE

Oksana Pokhodun, then a 38 year old nurse from Russia’s Krasnoyarsk region, did not approve of any of the famous—or infamous—opposition activists like Alexei Navalny. However, she had spent several consecutive weeks in 2017 attending gatherings under the auspices of a fringe Russian nationalist organization “Artpodgotovka,” whose leaders and several other members have since been labelled “extremist” by the state (OVD-Info 2017). One morning in early 2018, a group of neighbors, police officers and FSB agents barged into Pokhodun’s home, presented a search warrant, and seized her electronic devices. In April of the same year criminal charges were filed against Pokhodun under the “Extremism Law,” Article 282, Section 28 (1) of the Russian Criminal Code (Kozkina 2018).

The prosecution’s primary evidence in the case was one of Pokhodun’s private media folders on VKontakte, the Russian analog of Facebook. This folder, which Pokhodun insisted was only accessible to her, included images varying from benign pictures of animals to memes with political humor or criticisms. More specifically, these memes criticized the Russian annexation of Crimea, the Russian Orthodox Church, and Russian President Vladimir Vladimirovich Putin (Laprad 2017). In April 2018 she was found guilty of “inciting hatred or enmity on grounds of nationality, origin and attitude to religion” and sentenced to two years in prison with a two year suspension. Although it remains unclear how or for what reason the FSB accessed Pokhodun’s private social media content, her involvement with the “Artpodgotovka” opposition group could have been enough to cause suspicion among local authorities and tip off an FSB investigation into her digital behavior.

In defense of Pokhodun, AGORA International Human Rights Group attorney Vladimir Vasin reminded the court of his client's clean record and condemned the legal tenuousness of imprisonment premised on private social media activity—a conviction on the basis of "the increased social danger of the crime and the identity of the defendant" would be baseless, he argued (OVD-Info 2018). Although the charges were eventually dropped in February 2019, Pokhodun still considers herself innocent and adamantly defends her right to privately collect photos online: "These images were not in my public domain. Nobody sees them: neither my acquaintances, nor friends" (Kozkina 2018). Pokhodun's case demonstrates the level of state surveillance of online activity in Russia and the government's resolve to preempt apparent threats to the state-approved digital information environment. Pokhodun is not the first, and will not be the last, Russian citizen prosecuted under Internet extremism laws. Between 2011 and 2017, 604 charges were brought by regional courts and the Russian Ministry of Justice under Articles 280 and 282 (on "incitement of hatred," including "religious hatred") of the Criminal Code (Library of Congress 2015; Pommeranz and Smith 2018). Recent amendments to the Criminal Code have stipulated additional penalties for extremist activity online, including for users spreading "fake news" and slandering the Orthodox Church  (Freedom House (hereafter FH) 2014).

Non-democratic Internet governance across the globe is a paramount problem of the digital age and demands increased public awareness and professional scholarship. Information control is an essential tool for regime security in authoritarian and semi-authoritarian states in particular.[1] The increasingly influential role of the Internet as a platform for information promulgation and civil society mobilization represents a potential challenge to authoritarian governments worldwide.

[1] I initially refer to Russia and China as "authoritarian" regimes for the sake of parsimony at the outset of the paper. In later sections I will complicate my analysis of the two political systems to enable a more specific consideration of these Internet governance models.

In response, states like China and Russia seek to monitor and restrict the free flow of information, especially the information which threatens their legitimacy, often invoking extremism laws and mounting prosecutions to preempt digital opposition. State control over the digital space is extremely problematic; if a state can filter what its citizens can access and learn, it can also shape its citizens' perceptions, and potentially, their electoral, social, and financial behavior. When states prevent citizens from voicing certain opinions and accessing crucial information, the public loses the ability to effectively make demands of the government. In recent years in particular, states like China and Russia have sought to "'occupy the [online] public opinion battlefield'" in alarming new ways (Creemers 2016, 44).[2]

Policymakers and scholars frequently refer to states like China and Russia, whose survival depends on agenda-setting, the moderation of certain content, and deliberate efforts to sway domestic and international public opinion, as "digital authoritarians" (Polyakova and Meserole 2019, 2). Although the term is relatively new, the concept of digital authoritarianism and the types of information controls it encapsulates (surveillance, censorship, and manipulation of public opinion) have been widely studied (Polyakova and Meserole 2019, Weber 2019; Roberts 2018a; Deibert and Crete-Nishihata 2012). While an analysis of digital authoritarian is not complete without consideration of all three types of information controls, this paper pays special attention to the ways censorship and manipulation of public opinion inform Internet governance.

The purpose of this paper is to provide answers to the following questions: What mechanisms do regimes use to regulate the digital information environment? Furthermore, how

[2] Originally from Xi Jinping, 'Speech at the National Ideology and Propaganda Work Conference', China Digital Times, (4 November 2013), available at: http://chinadigitaltimes.net/chinese/2013/11/ (originally found in Creemers 2016 44).

can we better distinguish between Internet governance techniques of similar regime types, like Russia and China? What explains these differences? This comparative analysis finds that the biggest differences between the Russian and Chinese Internet governance models are the relative centralization of each country's network infrastructure and the extent and pace of change in governance over time. These points of divergence may be explained by two theories. The varieties of authoritarianism theory posits that different political systems face persistent and unique constraints to governance of the digital realm. The development trajectory theory argues that each country's technological development path foreshadows the systems' capacity for and extent of governance.

Chapter One will begin with a consideration of the Internet as both a threat and boon to authoritarian regimes. Although this area of study is becoming increasingly consequential with the rise of global Internet penetration and the growing regulation of digital spaces, cross-jurisdictional scholarship is still somewhat limited. In this chapter I will define concepts of information flow and digital authoritarianism before thoroughly reviewing the literature review on Internet governance. I will then propose a new, more comprehensive analytical framework which improves on pre-existing models for studying Internet governance. This framework will be applied to case studies of China in Chapter Two and Russia in Chapter Three. In Chapter Four I will identify differences between the models and expound two hypotheses to explain them.

# Existing Scholarship and a Novel Analytical Framework

## The Internet: A Challenge to Authoritarian Governance or a Tool for Repression?

The prototype for the Internet as we know it today was unveiled in 1969 by the U.S. Department of Defense's Advanced Research Projects Agency (ARPA). ARPANET, a single network of communications, expanded to become a multi-network system between 1973 and 1983 with the help of Vincent Serf and Robert Kahn (Abbate 2001 50,165). Originally a publicly-funded project, the Internet was privatized in 1995 (Abbate 2001 149,176). Shortly after the Internet's transition from public to private ownership, an international governance regime was established by the Internet Corporation for Assigned Names and Numbers (ICANN) and the United Nations' World Summit on the Information Society (UNWSIS), later called the World Summit on Internet Governance (Mueller and Wilson 2010, 10).

In the early days of Internet, scholars generally fell into two ideological camps—"cyberlibertarianism" or "cyberpaternalism." The cyberlibertarians believed that modern technology was a death knell for authoritarianism, and the cyberpaternalists peddled a more "realist" approach, which saw the Internet as a mere extension of the territory of a state and advocated for regulations to govern it (Krönke, et al. 2018b, a; Mueller and Wilson 2010; Müller 2018). With the benefit of a few decades' hindsight, it is clear that neither extreme view of Internet technology was an accurate prediction of the geopolitical future. After all, authoritarian regimes remain intact today and almost every state governs its digital realm in some form or another. And yet the Internet is still a platform for organizing, information sharing, and knowledge-acquisition that presents a unique challenge to authoritarian-style governance.

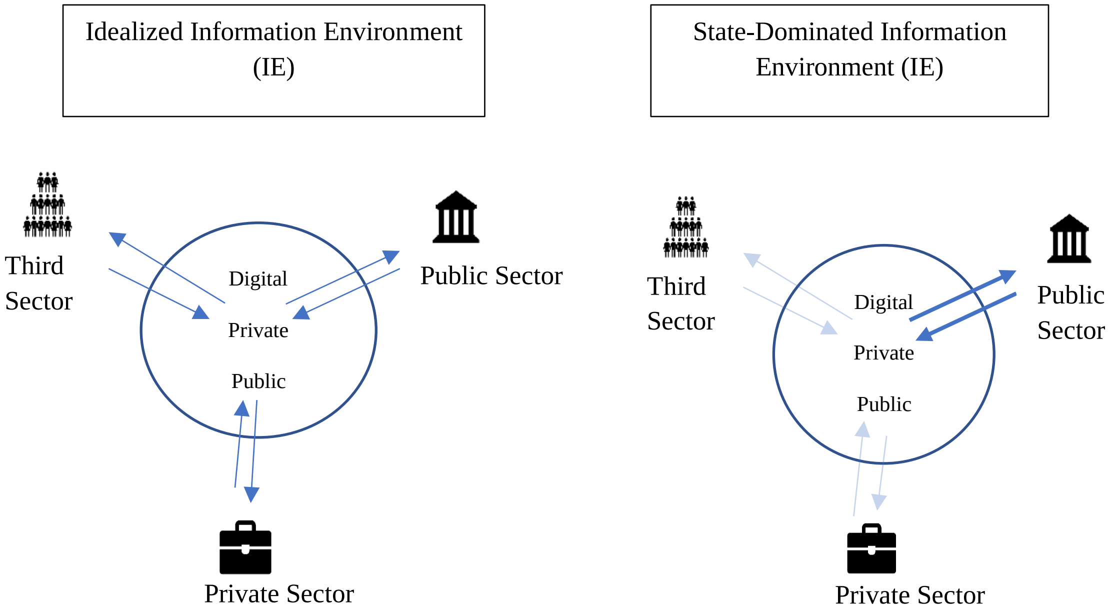
### *The Internet as a Component of the Information Environment*

The issue of information control has been central to the survival of authoritarian regimes even before the advent of the Internet. For this reason, it is useful to understand the Internet as a part of a broader "information environment," which I argue is comprised of the information shared in digital, public, and private spaces by the civil, public, and private sectors of a society. The concept of the information environment allows us to better understand the movement of information in a society and the roles each actor or stakeholder plays. Put simply, the digital realm of the information environment is both a reflection of broader state-civil society sector relations and provides greater opportunity for communication and collaboration between previously disparate groups.

In the figure below, the information environment is represented as a circle in which civil society actors (third sector- top left), the state (public sector- top right), and corporations (private sector- bottom) each contribute (inward-pointing arrow) and consume information (outward-pointing arrow). The diagram on the left-hand side represents the *idealized* information environment, in which each actor shares and receives information freely. However, in today's conditions of global Internet governance, virtually all governments, regardless of regime-type, restrict access and contribution to the information environment in some way, often on the grounds of discouraging hate-speech, extremism, or protecting minors from inappropriate content. To account for this broad trend in Internet governance, the model on the right depicts a more realistic, state-dominated information environment, in which the state determines (to varying degrees depending on the regime in question), what information users can access and share. In the case of authoritarian regimes, the state may attempt to govern in more heavy-handed ways, hindering corporations' and civil society actors' access to and participation in the information environment.

Notice that in the state-dominated IE the arrows both to and from the state are more solid, indicating that the state sets the agenda by producing, censoring, and manipulating information but also remains aware of areas of social discontent that could threaten its legitimacy. The more state-directed the domestic information environment, the more control the state has over other sectors' access to and participation in the IE, denoted by more solid arrows pointing to and from the public sector and more transparent ones in relation to the third and private sectors.

***FIGURE 1. GRAPHICAL REPRESENTATION OF THE INFORMATION ENVIRONMENT***



While the application of the term "information environment" to a digital context is relatively new, the phrase itself and the concepts which undergird it are not. In fact, information environments have been studied by various fields for decades. For example, in 1979 one author posited that the information environment is a space that shapes public perception: "Just as the physical environment determines what the source of food and exertions of labor shall be, the information environment gives specific direction to the kinds of ideas, social attitudes, definitions of knowledge, and intellectual capacities that will emerge" (Postman 1979, 324). In these early articles, scholars observed that access to and possession of information skew the distribution of power in society. McHale describes the stratifications that arise in an "information society":

> This tendency towards division into relatively separate information communities may take on a simpler form of a more homogeneous society, but one polarized by those who possess the necessary education and skills to participate fully in the information/communication process, i.e., the information 'haves' and those who are denied full participation for various reasons - the information 'have nots' (McHale 1973, 267)

In more recent years, scholars have continued to study the social, political and economic implications of being either "informationally rich or poor" (Price and Zaller 1993, 138; Jerit, et al. 2006, 267). However, policymakers and political pundits have paid greater attention to the topic than scholars in recent decades. At the forefront is the Department of Defense (DoD), which defines the IE in its 2016 report as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (Department of Defense 2016, 3). The DoD also considers the IE as "a conduit for influence on decision-making" (Department of Defense 2016, 2). The increasing ability of states to manipulate domestic and international information environments, especially in the digital realm is alarming. Even in democratic states, the information environment is ripe for influence or manipulation by foreign influence operations, such as the infamous Russian intervention around the 2016 U.S. Presidential election.

Apart from being a boon to states who seek to manipulate information, an IE can encompass both internal and external threats to a regime. As citizens of an increasingly interconnected world, we are increasingly able to create and disseminate information in all three realms of the IE. In terms of the information environment, the digital space in particular allows the unprecedented "speed and velocity," quantity, and "direction" of information dissemination, not to mention netizens' growing ease of access to information (Postman 1979, 141). The speed and quantity of information threatens regimes that attempt to control public knowledge or opinion on certain topics.

### *Information Control and Authoritarian Resilience*

Although the robust literature on varieties of authoritarianism acknowledges differences in personalistic (Chang and Golden 2010), “hybrid” (Diamond 2002), “semi-authoritarian” (Ottaway 2003), “soft authoritarian” (Schedler 2002),  “competitive authoritarian” (Levitsky and Way 2002), and ideologically-influenced one-party regimes (Huntington 2009), scholars agree that authoritarian regimes of all stripes wrestle with similar survival challenges. Whereas scholars initially conceived of authoritarian regimes as inherently vulnerable to popular uprising or other democratic influences, more recent attention has been paid to the sources of authoritarian resilience or durability.

Scholarship on authoritarian durability can be divided into three distinct phases (Gerschewski 2013, 14). In the first phase (1930-1960), scholars posited that “terror and ideology” motivated “totalitarian” survival (Arendt 1953; Schorske and Brzezinski 1958). Secondly, in the subsequent two decades, experts shifted their attention to consider socioeconomic explanatory factors for durability (Collier 1979; Remmer and Merkx 1982; Sondrol 1991). It was in this same Cold War context that George Schultz postulated that “totalitarians” faced what has since been coined the “dictator’s dilemma”: whereas authoritarians strive to control information (and information technologies) in accordance with state-approved values, to excessively filter content or deny access to technology is to lose the pulse of public opinion, another potential threat to regime security (Kedzie 1997, 1). Such is the problem facing China and Russia.

The third and present phase of scholarship on authoritarian or “autocratic” resilience, whose emphasis is on “strategic repression and co-optation,” was ushered in by Geddes’ article in 1999 (Brancati 2014; Gandhi and Przeworski 2007; Geddes 1999; Gerschewski 2013, 18; Nathan 2003; Slater and Fenner 2011). In addition to repression and co-optation, Slater and Fenner assert that authoritarian states ensure their durability through “infrastructural mechanisms,” including registering citizens and extracting revenues (Slater and Fenner 2011, 15). Gerschewski posits that maintaining legitimacy is an essential factor for authoritarian durability (Gerschewski 2013, 18). Brancati describes a trend in the literature which posits that authoritarian states nominally adopt democratic institutions for the sake of mitigating internal and external threats (Brancati 2014, 314). According to this theory, states use ostensibly democratic practices to ensure their survival by (1) signaling their supremacy to potential opponents, (2) identifying areas of public discontent, (3) winning allies, (4) protecting the economy (a source of legitimacy), and (5) monitoring upper-level government officials (Brancati 2014, 314-320).

Although scholars disagree on a single set of explanatory factors for authoritarian resilience, most concur that authoritarian regimes encourage individual and corporate dependence on the state and manipulate the information environment by surveilling areas of public discontent and controlling the spread of threatening information. This phenomenon will be considered in both case studies to come. These tenets of authoritarian resilience apply not just to the information environment broadly, but also to its sub-sections, notably, the digital realm. To both guard against digital threats to their survival and make use of the Internet as a tool for repression, authoritarian governments impose strict governance measures on the Internet that take the form of infrastructural and content-layer interventions.

## The Concept and Study of Internet Governance

In this section I will bring together two independent branches of literature: the more technical study of Internet technologies and governance, which explains the hardware and software used for Internet control, and political science scholarship, which considers Internet governance in terms of regime type, political structures, and interactions between various stakeholders.

The literature on Internet controls remains divided on preferred terminology. Some experts and practitioners prefer to employ the term “governance” to describe how authorities create rules and paradigms for Internet participation and behavior, whereas others argue that the term “regulation” is more apt (Mueller and Wilson 2010; Münkler 2018, 141). According to Mueller and Wilson, “Governance is the simplest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies” (Mueller and Wilson 2010, 9). Similarly, the United Nations exclusively defines and employs the term “cyber governance,” avoiding the term “regulation” altogether (Münkler 2018, 141, as cited in the UN working Group on Internet governance 2005).[3] Münkler argues that, unlike “regulation,” the term “governance” is only appropriate when performed “in a reflexive manner” (Münkler 2018, 143). In contrast, Müller’s definition of “regulation” encapsulates the idea of prophylactic agenda-setting (Müller 2018, 34 as cited in Julia Black “What is Regulatory Innovation” 2005).[4] Despite the vibrant scholarly debate on usage, the two terms have been

[3] The UN defines governance as “the development and application by Governments, the private sector, and civil society in their respective roles, of shared principles, norms, rules, decision-making procedures and programs that shape the evolution and the use of the Internet.” (Mueller and Wilson 2010, Münkler 2018 141, from Report from the UN working Group on Internet governance 2005).

[4] Müller gives the following definition for “regulation”: “the sustained and focused attempt to alter the behavior of others according to standards or goals with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification” (Müller 2018 34).

applied somewhat interchangeably to the phenomenon of Internet control. For the sake of clarity and consistency, I will hereafter use the term "governance". I have chosen this term because the concept, in accordance with traditional political science interpretations, describes situations in which multiple "interdependent" actors interact in formal and informal ways, an apt characterization of the Internet system and its stakeholders (Mueller and Wilson 2010, 9).

The Internet can be understood as a three-layered structure consisting of physical infrastructure, logical infrastructure (such as IP addresses), and a content layer (Krönke, et al. 2018a, 17). The physical infrastructure is generally governed by regional or state-level powers, the logical by international non-governmental entities such as the Internet Corporation for Assigned Names and Numbers (ICANN), and the content layer by a combination of governing entities (Krönke, et al. 2018a, 21). When states wish to govern their physical infrastructure, they can create "chokepoints" which limit or filter certain data or block sites from operating on domestic servers. Whereas the logical infrastructure is difficult for states to control, the content layer is perhaps the easiest to manipulate.

In spite of its relatively recent origins, the literature on Internet governance is growing quickly to include different typologies to explain variations in governance on the grounds of regime type. However, many of the analytical studies of Internet governance have remained isolated and under-synthesized. Some preexisting approaches use overly simplistic dichotomies, such as "complete" or "partial control" (Müller 2018) and "pure unenforced self-organization" or "direct regulation by government-imposed regulatory bodies" (Marsden 2011; Müller 2018, 41). Many of the existing typologies fall short of accounting for the varied technical capacity of each country's network infrastructure and do not identify or describe specific mechanisms for control of the Internet. Deibert and Rohozinski propose three "generations" of Internet governance: (1)

less sophisticated software techniques to block websites and servers, (2) constructing a legal and technical capacity to block unwanted content and sites, and (3) a “highly-sophisticated, multidimensional approach” in which states are able to “compete with potential threats” using domestic manipulation, surveillance, and data mining (Deibert and Rohozinski 2010, 27). While this typology accounts for variations in technological capacity, it neither engenders a systematic analysis of governance at each level of the network nor directly accounts for the roles of various Internet stakeholders such as users and Internet service providers (ISPs).

Moreover, paradigms for explaining various forms of Internet governance, such as the one created by Freedom House, fail to account for the differences among similar regime types. Freedom House publishes an annual “Freedom on the Net” report, which compiles information on various “types of key Internet controls” (KICs) such as “blocking social media or communication platforms” into a score that places countries in one of three categories: “free,” “partly free,” and “not free.”[5] In the 2019 report, Russia and China were both found to have utilized all nine types of KICs, yet their Internet governance models differ in numerous ways which the model fails to represent (FH 2019a). In the next section I propose a new analytical framework to improve the study of Internet governance. This new analytical tool will enable direct and detailed comparison at every level of network governance between case studies of any regime type, highlighting well-informed conclusions about relative differences in governance development, degree of infrastructural centralization, and breadth of legal mandates.

[5] Freedom House designates nine “types of key Internet controls” (KICs): 1) blocking social media or communication platforms, 2) blocking social, political, or religious content, 3) deliberately disrupting ICT networks, 4) progovernment commentators manipulating online discussions, 5) instituting new law or directive increasing censorship or punishment, 6) instituting new law or directive restricting anonymity or increasing surveillance, 7) arresting, imprisoning, or prolonging detainment of ICT user or blogger for political or social content, 8) physically attacking or killing ICT user or blogger, 9) mounting technical attack(s) against government critics or human rights organizations. (For more, see Freedom House’s Freedom on the Net 2018 report, page 22).

### *Towards a More Comprehensive Framework*

The figure below represents a new analytical framework which expands upon existing models of Internet governance. This framework is a unique tool which unites technical and non-technical approaches to Internet governance, can be applied in any case or regime, and should accompany a consideration of political, social, and economic context in each case. The goal of this framework is to more precisely account for the different ways in which states govern the Internet, regardless of their regime classification. An application of this analytical framework to the cases of Russia and China will shed light onto the different models of authoritarian Internet governance, to illuminate how regimes of the same broad classification differ in practice.

Of all the preexisting models, the network description which Howard et al. present is particularly useful as it identifies four sub-sections of the Internet (Howard, et al. 2011, 5). However, I improve upon this designation by expanding the "proxy" level to include all corporations (including domestic and international social media firms, search engines, and businesses with online functionality) and enumerating specific governance or control mechanisms at each level of the network. My more extensive framework, pictured below, demonstrates that regimes may govern the "full network" (the entirety of the Internet's physical infrastructure), "sub-networks" (websites), "proxies" (Internet service providers and other corporations), and "network-nodes" (individuals). States can leverage control over the Internet by isolating the network infrastructure, conducting regional shutdowns, blocking, blacklisting, or filtering websites, prosecuting, blocking and denying service to Internet service providers and other companies, and lastly prosecuting, blocking, or mounting physical or technical attacks against Internet users for their digital behavior. These mechanisms motivate another, indirect mechanism of state control: encouraging digital self-censorship.[6]

***FIGURE 2. NOVEL INTERNET GOVERNANCE ANALYTICAL FRAMEWORK***

| **Level of Network Governance** | **Non-Technical Alias** | **Associated Control Mechanisms** |
|---|---|---|
| Full Network | Internet | Isolation, Regional Blackouts |
| Sub-Networks | Websites | Blacklisting, Blocking, Filtering |
| Proxies | Corporations | Prosecution, Blocking, Denial of Service |
| Network-Nodes | Users | Prosecution, Blocking, Self-Censorship, Physical Attack |

As forthcoming applications of this framework to the cases of China and Russia will demonstrate, states can govern their domestic digital environments at any level of the network. A state seeking to control its digital information environment can adopt complicated infrastructural measures by isolating the entire network, or manually block sub-sections of the Internet (websites). It can also encourage state-dependence of Internet Service Providers (ISPs) and other corporations

[6] Here I have layered some of the Freedom House mechanisms (ex: physical or technical attacks on users) and added self-censorship of content, which is missing from the Howard et al. paradigm.

whose business relies on Internet connection, or target users in various legal or physical ways on the basis of the content they create, share, or consume on the Internet. States who employ these controls often promote a culture of self-censorship, in which individuals restrict digital behavior in fear of a variety of repercussions.

The global trend towards more extensive Internet governance is troubling. Freedom House estimated that by the release of its 2019 "Freedom on the Net" report, 46% of citizens around the world would live in countries with full Internet blocks, 46% in countries that have blocked certain websites or social media platforms, 65% where individuals were attacked or killed for online activity, and 71% where individuals were arrested or imprisoned for posting content on political, social, or religious issues (Shabaz and Funk 2019, 2). As more states embrace controls over sections of the worldwide web, they deprive civil society and private sector actors of power and participation in the information environment.

## Methodology

In the following chapters the new analytical framework will be applied to the Chinese and Russian cases in order to highlight differences in authoritarian approaches to Internet governance. To better ascertain what it means in practice for digital authoritarians to assert control over an information environment, I will employ the comparative method between the two case studies. I chose China as the first case study because it possesses the world's most infamous and extreme Internet governance model. While scholarship on Chinese digital authoritarianism is robust and rich, there is a dearth of comparable material on the Russian system. Apart from contributing to the understudied are of research on Russia's Internet governance model, I chose to study Russia because in recent years its governance model has been increasingly widely exported to neighboring and distant countries. Therefore, understanding the Russia model is one of the keys to comprehending the future of global Internet governance. Moreover, this comparative study is one of the first attempts to demonstrate how the literature on varieties of authoritarianism can be applied to Internet governance.

First, I use my analytical framework to systematically analyze the mechanisms which China and Russia use to govern the Internet at each level of the network. Special emphasis will be placed on the Russia case study due to its relative lack of scholarly attention. To contribute to a more nuanced and detailed view of Russia's information controls, I engage in novel data collection and analysis of the Russian Federation's only public blacklist, the list of "extremism materials" ("Список Экстремистов"  2019). I also aggregate data on relevant legislation from the Ministry of Justice website, Freedom House, AGORA International Human Rights Group and Human Rights Watch reports, as well as prosecution records from various media sources and non-profit reports to account for recent trends in Russian governance of the digital realm.

Second, I compare the two case studies and conclude that the models differ on several significant grounds, namely in the degree of network centralization and extent and pace of change in governance. I argue that these points of divergence may be explained by two theories, varieties of authoritarianism or distinct development trajectories. Lastly, I contribute to the existing dialogue in the field by articulating a future research agenda,  paving the way for a more nuanced study of Internet governance.

# INTERNET GOVERNANCE IN CHINA

China and Russia go to great lengths to govern the Internet by surveilling, manipulating, and censoring digital information. Boasting an impressive 829 million Internet users, or 59.6% of its population, China has the ability to shape the perspectives and digital experiences of almost 20% of the world's population through Internet governance and control measures (FH 2019a, 4). In comparison, the total number of Internet users in Russia is much lower but Internet penetration is proportionally higher; the number of Internet users reached 116.8 million, or about 76 percent of the population of the Russian Federation, by the fourth quarter of 2018 (Shabaz and Funk 2019, 29). Russia's Internet users represent about one sixth of all Internet users in Europe (Ramesh, et al. 2020, 2).

The sheer number of Internet users represents an enormous governance challenge for Russia and China. Nevertheless, Internet governance, including the manipulation of domestic information environments, is essential to regime survival in both cases. How do Russia and China rationalize their extensive Internet controls to citizens and foreign onlookers? Are their public justifications similar? To understand how states use Internet control mechanisms, it is useful to consider China, one of the most extreme digital authoritarians, and then Russia, whose governance system is notably different. This chapter will begin with a comparison of official policy positions of Russia and China on Internet governance and later transition into an analysis of China as the archetypal case of digital authoritarianism using the new analytical framework detailed in the previous chapter.

## Justifications for Restrictive Internet Governance

Both Russia and China publicly tout a broad mandate to govern the Internet in their respective territories and demand that international institutions honor this digital extension of sovereignty. An analysis of Russian and Chinese official domestic positions on Internet governance will shed light onto the foundational principles of each model. A comparison of the 2010 "White Paper on The Internet in China" and 2016 "Information Security Doctrine of the Russian Federation"[7] demonstrates that the states invoke many of the same political justifications for Internet governance. Both states treat Internet governance as a matter of national security, underscore the promotion of ethnic harmony and unity of historical narratives online, and assert that such governance strategies are compatible with civil rights.

Firstly, both the Russian and Chinese white papers invoke the protection of national security as a rationale for Internet governance, using remarkably similar language to underscore this necessity. In the words of the 2010 Chinese document, "Internet security is a prerequisite for the sound development and effective utilization of the Internet.... Effectively protecting Internet security is an important part of China' s Internet administration, and an indispensable requirement for protecting state security and the public interest" ("White Paper: The Internet in China" 2010). Likewise, the 2016 Russian decree begins by highlighting the importance of Internet governance

[7] These two white papers have been chosen as points of comparison because they are the most recent publicly-issued documents that describe each country's information environments and controls thereon. Although it would be preferable to compare documents closer in date (and in particular a Chinese document after Xi's 2013 tenure began), there have been no white papers or policy documents that exclusively explain the Internet governance model in China since the 2010 document in question. The 2010 white paper serves as a foundation for more recent, general defense publications in which cybersecurity is only one of many areas of national security. For the most recent information about defense strategy in cyberspace, see the 2019 Chinese Defense White Paper, "China's National Defense in the New Era," http://www.xinhuanet.com/english/download/whitepaperonnationaldefenseinnewera.doc.

to national security: “This [Information Security] Doctrine is a system of official views on ensuring the national security of the Russian Federation in the information sphere,” in which the “information sphere” is defined as “the totality of information, objects of informatization, information systems, sites in the information and telecommunication network ‘Internet’” (Russian Federation (hereafter RF) 2016). This point of crossover between the Chinese and Russian systems must be seen in a broader context of global Internet governance; the “securitization” of the Internet is not limited to authoritarian states like Russia and China, but is also entrenched in democratic models like the U.S. and Britain, which have recently “reframed [Internet security] as a national security issue” (King, et al. 2013; Mueller and Wilson 2010, 160). In fact, one research group found that “National security was the most commonly cited reason… to intervene with Internet access” regardless of a country’s regime type (Howard, et al. 2011, 7). Despite the seemingly ubiquitous justification for Internet governance on national security grounds around the world, it is important to note that in authoritarian systems, citizens have diminished opportunities to advocate for freedoms or access information that contradicts official state discourse. Moreover, in authoritarian systems like Russia and China, it is difficult for opposition groups to challenge the state when national security is invoked as a justification for greater digital restrictions.

Not only do the Russian and Chinese systems invoke national security as a justification for management of domestic Internet, both highlight the need to combat digital threats to ethnic, territorial, and cultural unity. Each responsible for a large and diverse population, Russia and China alike must guard against insurrections in the many ethnically distinct regions under their jurisdiction, such as Xinjiang or Ingushetia. China’s white paper condemns the following digital information as illegal: “information that contains contents subverting state power, undermining national unity, infringing upon national honor and interests, inciting ethnic hatred and secession, advocating heresy, pornography, violence, terror and other information that infringes upon the legitimate rights and interests of others” ("White Paper: The Internet in China"  2010). Moreover, references to the Tiananmen Square massacre, Falun Gong movement, ethnic separatism in Xinjiang, and more recently, reinterpretations of Mao and the Communist Party’s past are placed under the same umbrella (Zhao 2016). Similarly, the Russian decree outlaws all information and activities which “propagate extremist ideology, spread xenophobia, ideas of national exclusivity in order to undermine sovereignty, political and social stability, forcibly change the constitutional system, and violate territorial integrity Russian Federation” (RF 2016). Most notable among illegal content are reinterpretations of World War II, glorifications of Nazism, and calls for separatism, especially in regions with non-majority ethnic or religious identities, such as Chechnya. These types of content are flagged and placed on blacklists like the extremism list analyzed in the next chapter.

The Russian and Chinese white papers also both claim to govern the Internet on the grounds of protecting civilians’ constitutional or other legally-protected rights. In China’s case, this protection of civilian rights comes with a caveat which underscores the social contract of Chinese citizenship and mere temporary or permanent residence in China: “Citizens of the People's Republic of China *and foreign citizens*, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security” ("White Paper: The Internet in China"  2010, italics my own). Similarly, the Russian document legitimizes its Internet governance model by citing a constitutional defense of civilian rights. Among the “National interests in the information sphere,” is “ensuring and protecting the constitutional rights and freedoms of man and citizen with regard to obtaining and using information... providing information support for democratic institutions, mechanisms of interaction between the state and civil society, as well as the use of information technology in the interest of preserving cultural, historical and spiritual moral values Russian nationalities of the people" (RF 2016). Given the extensive policy crossover between the Russian and Chinese white papers on Internet governance, an exploration of governance at each network level is required to understand how Internet governance may be different in practice.

### Chinese Internet Governance at each Network Level

China is one of the most widely-known and extreme examples of digital authoritarianism, perhaps because it has long strived to be a 'strong Internet power' (*wangluo qiangguo*) that could rival the West, and more specifically, the United States (Creemers 2016, 85). In part due to the country's early Internet controls and growing economy, scholarship on the Chinese Internet governance model is rich and varied. Many scholars have written about how the model affects protest potential and mobilization efforts (Chi 2012; King, et al. 2013; Laskai 2017; Lu and Zhao 2018b; MacKinnon 2011; Tkacheva, et al. 2013). Some scholars have contributed qualitative analysis to the study of Chinese Internet censorship (Creemers 2016; Chi 2012; Groot 2017; Kolton 2017; Lam 2013; MacKinnon 2011; Polyakova and Meserole 2019; Roberts 2018a; Williams 2013), while others have applied quantitative and other technical methods to understand the Chinese government's censorship decisions by conducting large-scale digital analyses (King, et al. 2013; Lu and Zhao 2018b; Yang and Mueller 2019).

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, 2). This chapter's detailed analysis of Chinese Internet governance at each level of the network confirms the comprehensive and sophisticated nature of its model. An increasingly centralized web of Chinese institutions targets each of the four components of the Internet system (the network itself, websites, corporation and ISPs, and individuals) and places special emphasis on higher level network governance.

### *Internet Governance Institutions*

China's Internet governance model was created by a flurry of laws in the mid-1990s. The first piece of legislation governing the Internet was the 1994 State Council Order No. 147 which subverted the Internet to the national security interests of the state (Roberts 2018b, 104). The "Great Firewall" (also called the "Golden Shield") was created in the 1996 by State Council Order No. 195 and epitomizes extreme Internet control mechanisms on a full-network level (Polyakova and Meserole 3). [8] From 1994-2015 the Chinese Internet governance model relied on approximately 50 governing bodies to pass 200 policies (Miao, et al. 2018, 3).[9] The most active agencies for Internet governance policies are the Ministry of Industry and Information Technology (MIIT), Ministry of Public Security (MPS), and the Cyberspace Administration of China (CAC), all entities which report directly to the Chinese Communist Party (CCP) (Miao, et al. 2018, 4).

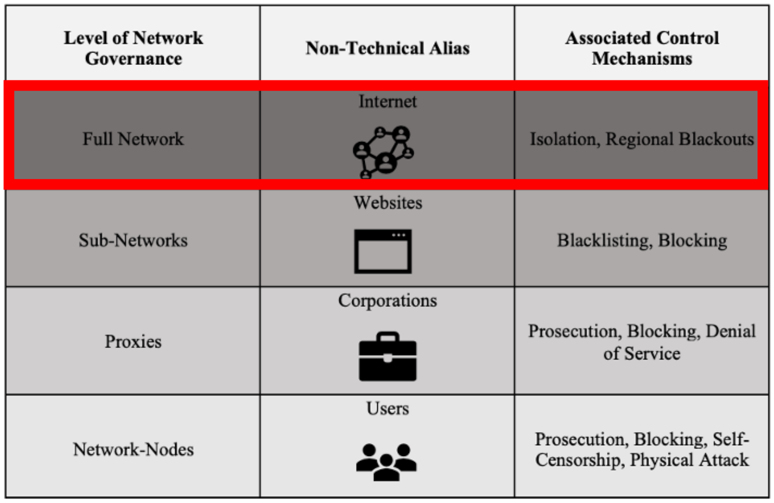
Although China's Internet governance strategy had notable flaws by way of division of labor and resource allocation in its early days, recent changes to the model under President Xi Jinping (2012–) are widely believed to have increased the state's systematic governance of the

[8] The term "Chinese Firewall" originated in the following Wired article in 1997: Barme, Geremie; Ye, Sang. 1997. "The Great Firewall of China." accessed September 17. https://www.wired.com/1997/06/china-3/.

[9] For more detailed overviews of all the institutional hierarchy of Internet governance in China, see Yang and Mueller 2019, Creemers 2016, and Miao, et al. 2018 or Roberts 2018b).

Internet (Creemers 2016, 93; Roberts 2018b, 107). In 2013, Xi admitted that the Internet governance infrastructure he inherited "has obvious problems, including multiple authorities, overlapping powers, mismatch of authority and responsibility, as well as inefficiency" (Miao, et al. 2018 5). In 2014 Xi established and chaired a new Central Leading Group for Cybersecurity and Informatization, which firmly united Internet governance institutions such as the State Internet Information Office (SIIO) and several technical bodies under one roof: the CAC. With the introduction of the Cybersecurity Law in 2017, Xi formally concentrated Internet governance responsibility in the hands of the CAC, which answers directly to the Central People's Government (State Council) and which Xi himself chairs (Iasiello 2017; Krönke, et al. 2018a, 19-20; Lu and Zhao 2018a, 3297; Miao, et al. 2018; Yang and Mueller 2019, 453). The Chinese Internet governance system under Xi Jinping is highly-centralized and institutionalized by the CCP at all levels of network governance, and prioritizes information management at the higher, gatekeeper levels of the network (Roberts 2018b, 110).

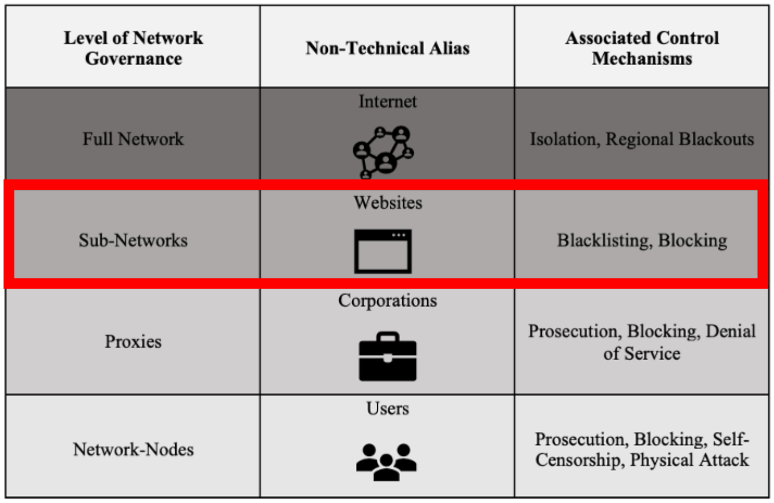
### *Full Network Level Governance*



| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Full Network | Internet | Isolation, Regional Blackouts |
| Sub-Networks | Websites | Blacklisting, Blocking |
| Proxies | Corporations | Prosecution, Blocking, Denial of Service |
| Network-Nodes | Users | Prosecution, Blocking, Self-Censorship, Physical Attack |

The Chinese system of centralized Internet traffic “chokepoints” is perhaps the most technologically advanced in the world (Ramesh, et al. 2020, 1). The centralization of the network infrastructure enables the state to systematically block servers and sites. The infrastructure is also isolated from international Internet traffic, allowing the state to control Internet access on a country-wide or regional level. The “one button” Internet kill switch has been successfully employed on numerous occasions, proving China’s centralized capacity to govern its digital environment. 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 (FH 2019a, 6; Griffiths 2019, 156).

### ***Sub-Network or Website Level Governance***



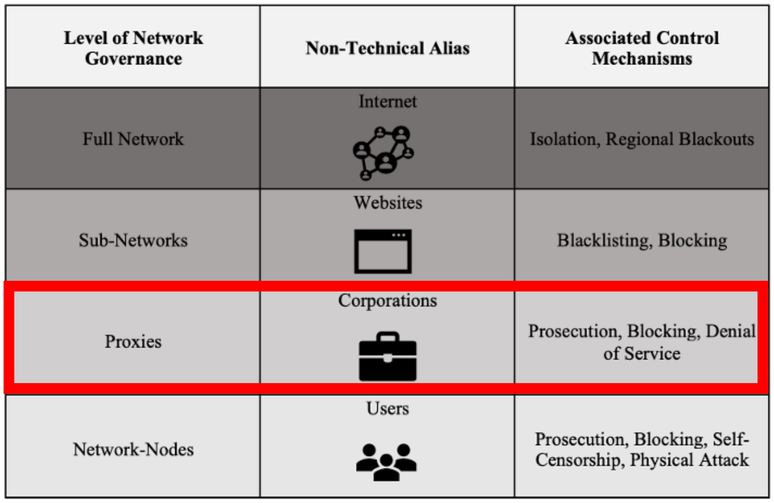
| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Full Network | Internet | Isolation, Regional Blackouts |
| Sub-Networks | Websites | Blacklisting, Blocking |
| Proxies | Corporations | Prosecution, Blocking, Denial of Service |
| Network-Nodes | Users | Prosecution, Blocking, Self-Censorship, Physical Attack |

Apart from its full-network capabilities, the Firewall also blocks “subnetworks” or websites like Twitter, Google, Facebook and YouTube as well as virtual private networks (VPNs), which allow users to connect to filtered content by disguising the location of their IP addresses (Kolton 2017, 120). Domestic variants of Facebook and Twitter, RenRen and Sina Weibo, provide similar services to Chinese users and are easier for the Chinese state to govern and surveil given their localized operation (Creemers 2016, 86; King, et al. 2013, 2). Government-issued blacklists exist but are not publicly accessible (FH 2019a, 15). In 2009, the state instituted a mandatory filtering software for all computers called the "Green Dam Youth Escort," but the program failed to gain traction and funding (Cheung and Yun 2013). Since the 2000s, the Firewall's censorship capabilities have become more extensive (Roberts 2018c, 223).

To give a sense of the scale of Chinese Internet governance at the sub-network level, in the first three weeks of 2019, China blocked over 700 websites and 9,000 mobile apps (Polyakova and Meserole 2019, 3). As recently as June 2019 the Chinese government embarked on a new "rectification campaign" to purge the Internet of websites it considered to be "failing their obligation" to safety and factual standards (Reuters 2019). Human rights groups such as Amnesty International, Human Rights Watch, and Freedom House were blocked by automatic filtering mechanisms as of late 2019 (FH 2019a).

Chinese Internet control efforts enlist thousands of citizens to remove certain information the state deems unsavory or extremist. Three known groups police the web in official and non-official capacities, including the Internet Police and Internet Monitors (consisting of 20,000-50,000 citizens), "50 cent party members" (250,000-300,000) (King, et al. 2013, 1), and hundreds of thousands of "youth league online commentators" (FH 2019a, 18). The "50 cent party members" —who are indeed paid 50 Chinese cents per social media post—were first detected as early as 2004 (Cheung and Yun 2013) and publicly encouraged by President Xi Jinping on several occasions, most notably in 2013 (Zhao 2016, 1180). Social media platforms like Sina Weibo now employ thousands of "content supervisors" to ensure compliance with new Internet laws (FH 2019a, 13; King, et al. 2013, 1). These sites have good reason to fear state retaliation. In 2015 scholars attributed an aggressive program nicknamed the “Great Cannon,” to the Chinese state. This program has engaged in Distributed Denial of Service (DDoS) activity, a process which floods sites with requests and information that ultimately temporarily disables the server (Marczak, et al. 2015).

### *Proxy or Corporation Level Governance*



| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Full Network | Internet | Isolation, Regional Blackouts |
| Sub-Networks | Websites | Blacklisting, Blocking |
| Proxies | Corporations | Prosecution, Blocking, Denial of Service |
| Network-Nodes | Users | Prosecution, Blocking, Self-Censorship, Physical Attack |

For decades, China has had a vibrant Information and Communications Technology (ICT) industry which has led to the proliferation of various cutting-edge technologies for domestic and international use. Among the popular domestic products are search engines and Internet service providers Tencent, 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). In 2019 Weibo boasted 374 million users, surpassing the number of users on its American counterpart, Twitter in 2017 (BBC 2017; Statista 2020). The large size and domestic origins of these companies allows the Chinese state to more easily govern the digital information environment; as one scholar argues, “ The sheer size of companies such as Baidu, Alibaba and Tencent means that effective control over a few companies enables the state to regulate the majority of online activities" (Creemers 2016, 95).

Apart from software and hardware control means, China's legislative system upholds an infamous array of cyber laws that target "proxies" or corporations (including ISPs, social media platforms, and search engines), attempting to foster private sector dependence on the state as a means of maintaining power over the dissemination of information (Slater and Fenner 2011). Although many ISPs and other proxies are not state-owned, they are subject to strict legal statutes which govern their data storage and content management practices. As early as 1996, ISPs were required to register with and be approved by the state. In 2000, State Council Order No. 292 required ISPs to adhere to censorship standards outlined by the executive. Partially or wholly state-owned corporations now operate as the gatekeepers for China's domestic Internet traffic as it interacts with the global web, serving at the pleasure of the CAC. These state-aligned or operated entities also oversee ISPs, ensuring their adherence to standards outlined by the Ministry of Industry and Information Technology (FH 2019a, 6).

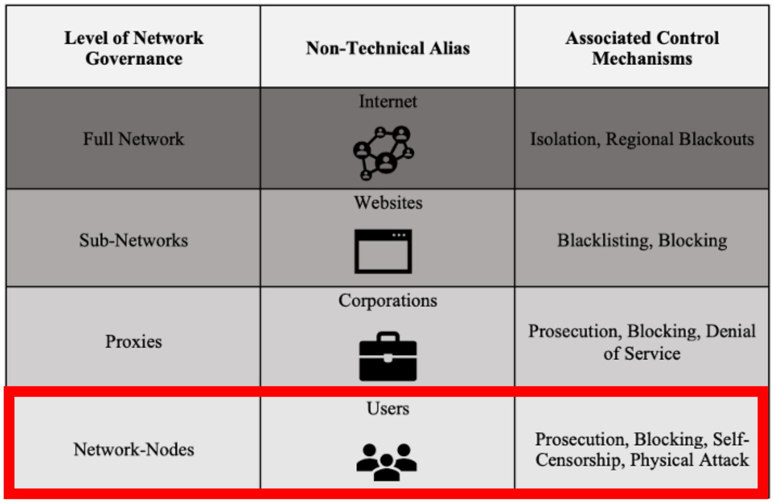
One of the most recent state restrictions on proxies is the 2015 "anti-terror" law which "compels technology companies to help decrypt information," providing Chinese authorities access to encrypted data (Iasiello 2017, 11).[10] A 2015 amendment to the Chinese Criminal Law and 2017 Cybersecurity law stipulate criminal liability for ISPs who fail to "stop transmission" of extremist content or to "shut down related services" (FH 2019a, 6-7). Article 286a, Section 1 of this new amendment reads: "Any network service provider that fails to perform the information network security management obligation as prescribed in any law or administrative regulation and

[10] For more on the exact content of the 2015 Anti-Terrorism Legislation, see Lawfare's analysis and the Chinese-language sources cited (Bissell 2015).

refuses to make corrections after being ordered by the regulatory authority shall be sentenced to imprisonment" (Xuan 2018, 72). This criminal liability fosters ISP deference to, and at times dependence on, the Chinese government. More specifically, the law restricts the anonymity of users and compels domestic and foreign corporations to 'immediately stop transmission' of banned content to store user data on domestic servers (FH 2018, 6). A 2018 law introduced by the CAC attempts to curtail political mobilization by compelling ISPs and related corporations that have "the capacity for social mobilization," such as social media or communication platforms used for political organizing, or are "of public opinion nature" to submit to "voluntary" assessments of their ability to uphold security standards (FH 2019a, 21). Moreover, ISPs are required to open their premises and provide user data to official search and seizure by security services (FH 2019a, 30).

Some scholars grapple with the question of corporate liability in enabling Chinese Internet control, identifying Silicon Valley giants like Google, Microsoft, Yahoo and Cisco as potential abettors (Griffiths 2019; Laskai 2017; Williams 2013). Many companies have acquiesced to the demands of the Chinese government in ideological disputes, for example over the "One Country-Two Systems" policy, in which China asserts that Hong Kong and Macau are regions of its mainland territory, not independent states. Marriott opted to change its classification of Taiwan, Hong Kong, Tibet, and Macau from "countries" to Chinese territories on its website, acceding to pressure from the CAC and in hopes resuming business operations in China. Marriot's service was unblocked "after the company issued a statement asserting its support for the 'sovereignty and territorial integrity of China' and distancing itself from 'separatist groups,'" a significant content-level change (FH 2018, 7). In early 2020 Samsung came under fire for allegedly collaborating with the firm Qihoo 360, a Chinese security company who receives Samsung user data through the "Device Care" application pre-loaded on all devices. Qihoo 360 has been known to adhere closely to national censorship directives, causing some users to worry about the type of personal data collected and shared with the state (Brandom 2020). For the most part, companies voluntarily comply with Chinese laws or are forced through denial of service or fines to obey.

### *Network-Node or Individual Level Governance*



| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Full Network | Internet | Isolation, Regional Blackouts |
| Sub-Networks | Websites | Blacklisting, Blocking |
| Proxies | Corporations | Prosecution, Blocking, Denial of Service |
| Network-Nodes | Users | Prosecution, Blocking, Self-Censorship, Physical Attack |

Although the Chinese model is constructed to prioritize governance of higher levels of the network rather than the network-nodes level, there are plenty of mechanisms in place to shape most users' online behavior. Despite the fact that the Chinese government doesn't seek to censor individual or isolated criticisms of the government and its leaders but rather to thwart collective action, information about certain political issues, like Falun Gong and Tiananmen Square, are nonetheless prohibited and Internet users who write about these topics are subject to legal and social penalties (Griffiths 2019, 46; King, et al. 2013, Laskai 2017; Polyakova and Meserole 2019; Williams 2013). The Chinese Internet Governance model also relies on surveillance of public opinion to adequately preempt collective action or popular uprising. 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, 90).

China's legal system is empowered with a broad mandate for governing the digital information environment. The "ambiguity" in Chinese Internet legislation is generally understood as a means to "give the state maximal flexibility in enforcement" (Roberts 2018b, 107). In recent years the state has cracked down on digital anonymity, perhaps to more easily prosecute individuals and promote self-censorship online. For example, in 2012, Chinese "micro-bloggers" were forced to register with the government and digital anonymity was altogether outlawed for all Internet users (King, et al. 2013; Lee, et al. 2012). This law, an update to the 2005 decree by the Ministry for the Information Industry (MII), discourages the use of aliases on digital messaging apps or any online platform (Reporters Sans Frontièrs (hereafter RSF) 2005). All bloggers, regardless of the number of views or page visits, must provide personal details to the government for surveillance purposes. In 2013 a law was passed requiring all smartphone users to register their devices with national identification cards and an amendment to an existing criminal law prohibiting "defamation, creating disturbances [article 293], illegal business operations, and extortion" extended its jurisdiction to include violations in cyberspace (Human Rights Watch (hereafter HRW) 2013; King, et al. 2013).

These laws have serious consequences for some Internet users and journalists. In 2013 and 2015 two popular bloggers were charged with defamation and other trumped up charges (Zhao 2016b, 1181). According to one nonprofit at least 34 of the 47 journalists jailed in China as of December 2018 were on the grounds of online content (FH 2019a, 26). Some Internet users charged with "subversion" and "separatism" can receive sentences as severe as life in prison thanks to a 2015 amendment to the criminal code, with harsher sentences for members of fringe ethnic and religious groups (FH 2019a, 25). One of the most extreme cases of state-ordered violence was the crackdown in China's religious minority (Uyghur) Xinjiang province. In 2014, under the guise of counter-terrorism, the state rolled out the "Strike Hard Campaign Against Violent Terrorism," which included running key-word searches in private messages and targeting Uyghur individuals to neutralize potential threats to the regime (Cockerell 2019; Polyakova and Meserole 2019).[11] This ethnic targeting leads many citizens to self-censor for their own wellbeing, avoiding mentions of political topics like the 2009 Urumqi or 2012 Kashgar riots or Tiananmen Square protests (Cockerell 2019). Article 246 of the criminal law in China targets any netizen who "publicly humiliates" or "invents stories" online (HRW 2013). Many of the laws China invokes to punish its Internet users and encourage widespread self-censorship are similar to provisions in the Russian legal system, such as articles of the Russian Criminal Code punishing subversion and "fake news."

While there is general agreement about the sophistication and scale of content filtering by the Chinese state, scholars disagree about the state's content censorship priority; King et al. categorize this rift in the literature as a schism between the "state critique theory" in which political content is the main target (Chi 2012, 397; Esarey and Qiang 2011; Lu and Zhao 2018b), the theory of "collective action potential," in which collective action or mobilization is the priority of the state censorship strategy (King, et al. 2013), and those critics who straddle the two categories (Herold and Marolt 2011; Polumbaum 2012). According to Chi, the Chinese government prohibits users in its territory from posting content online that fits into any of nine categories which range from information threatening national security or social stability, undermining the state's religious

[11] This campaign also served as a test of myriad advanced technologies and techniques such as surveillance through robotic doves (Chen 2018), spyware applications on portable devices (Cockerell 2019), GPS and Satnav (Wong 2017), as well as DNA collection in XinJiang (Haas 2017).

or political stance, to pornographic or explicit content (Chi 2012, 397).[12] The pressure imposed by legislation, prosecution, and other formal mechanisms encourages the more informal mechanism of self-censorship, which scholars argue has become a cultural mainstay in China (Laskai 2017, 5; Lu and Zhao 2018b; Repnikova 2017; Yang and Mueller 2019).

The Chinese censorship model is sophisticated, but selective, in that it prioritizes control over gatekeeping proxies more than it strictly polices individual usage. Moreover, Roberts posits that the Chinese model strategically utilizes "porous censorship," in which a variety of content is made available to users to convince them that censorship is not widespread, even if in reality it is (Roberts 2018c, 224). While this model works for the vast majority of citizens, a small, tech-savvy subsection of Chinese Internet users have become highly adept at finding ways around the Firewall, such as using VPNs to access censored content or employing analogies, nicknames and other esoteric rhetorical strategies to veil their digital content from censors (King, et al. 2013, 3; Roberts 2018b, 111). Freedom House estimates that in 2018 at least 20 million or about 2.5% of Chinese Internet users utilized circumvention tools like VPNs (Shabaz and Funk 2019). Chinese netizens have also been known to substitute political or sensitive words for others that sound or look similar. Nevertheless, the Chinese filtering regime for individual posts on social media has been described by some scholars as possessing "large scale military-like precision" (King, et al. 2013, 5). While at the moment the vast majority of Chinese Internet users remain content with the

[12] The specific nine categories are the following: 1) Information critical of the constitution. 2) Information that endangers national security, reveals state secrets, undermines state sovereignty, or injures national unity. 3) Information that harms national dignity and interests. 4) Information that provokes hatred and discrimination among nationalities and injures national solidarity. 5) Information that undermines state religious policy and advocates cult and feudal superstitions. 6) Information that disseminates rumors, disrupts social order, and injures social stability. 7) Information that disseminates obscenities or pornography or promotes gambling, violence, murder, or terrorism. 8) Information that defames or slanders others or impinges on the legal interests of others. 9) Information that is otherwise prohibited by law and administrative regulations (originally found in Zhou 2006).

information and resources at their fingertips and have few reasons to circumvent the censorship regime, Roberts warns that, “Moments when enough citizens are motivated enough to learn how to outsmart government media control are those when the information management strategy comes under the most pressure” (Roberts 2018b, 112).

## Conclusions from the China Case

The Chinese model for Internet governance is advanced, centralized, and complex. Due to its early control over upper levels of the network, such as the construction of the Firewall and laws coopting the information gatekeeping proxies, the Chinese state has been able to execute a top-down, systematic approach to Internet governance, relying less on retroactive controls on individual users. Such extensive and centralized Internet governance can only be achieved with a large federal budget (Soldatov 2017, 56). 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). One could imagine that a figure which includes the operating budgets of institutions like the CAC, network infrastructure maintenance, and emerging technology expenditures would be even larger.

Although China utilizes technologically advanced and more traditional legal mechanisms for control at every level of the network, the state is not altogether immune from challenges to its authority. Some might argue that China’s “dictator’s dilemma” comes in the form of economic innovation and growth; as one scholar puts it, “The Communist Party of China recognizes that without information technology it cannot fuel its economic ambitions and thus continue to deliver even modest economic growth” (Williams 2013, 6). However, this information technology is inextricably tied to the Internet, posing a challenge for both effective governance and economic viability, after all, authoritarian controls often inhibit innovation. The short-term efficacy of its Internet restrictions may prove troublesome for long-term economic growth.

# INTERNET GOVERNANCE IN RUSSIA

In recent years Russia has earned a place as one of the most extreme digital authoritarians. Although China was named "the world's worst abuser of Internet freedom for the fourth consecutive year" in the 2019 Freedom on the Net report, Russia was identified as a growing threat to user rights (Shabaz and Funk 2019, 5). While China's Internet governance model is widely studied by political scientists and policymakers, less is known or written about Russia's digital information environment (Barme and Ye 1997; Griffiths 2019; Krönke, et al. 2018b; Lam 2013; MacKinnon 2011, 44; Polyakova and Meserole 2019). Although it is indisputable that China's sophisticated and effective Internet governance model is admired by some other authoritarian regimes, newer authoritarian Internet governance models—like Russia's—are not mere carbon copies of China's (King, et al. 2013; Ramesh, et al. 2020; Polyakova and Meserole 2019; Ramesh, et al. 2020). Instead, this chapter demonstrates that Russia's model is technologically and institutionally distinct from China's.

In this chapter the Russian model of Internet governance will be introduced by tracing post-Soviet Russia's first connection to the global web and the state's early attempts to impose legal restrictions on the Internet. This section will illustrate Russia's oscillation between control and relaxation of its digital information environment. Next a systematic analysis of Russian Internet governance through the lens of the new analytical framework will highlight mechanisms employed at each network level. Given that less scholarly attention has been paid to Russia's Internet governance strategy, in this chapter I engage in several novel data collection strategies including identifying and analyzing a dataset on extremism cases in Russia, aggregating and identifying patterns in prosecution records, and creating data visualizations of legislation and judicial action. This chapter will highlight the unique traits of Russian Internet governance.

### Post-Soviet Russia and the Internet Puzzle

After the 1991 collapse of the Soviet Union and promise of democratization, the Russian state would somewhat sparingly monitor its growing digital information environment until it faced a direct threat to its regime survival. In 1994 the creation of the Russian domain extension .ru ushered in RuNet (Griffiths 2019, 256). Just a year later, ISPs were forced to adopt the "System of Operative Investigative Measures" (SORM) which enabled the Federal Agency of Government Communications and Information (FAPSI) and FSB to "spy on users' communications" (Griffiths 2019, 257l; Polyakova and Meserole 2019). Since its inception, SORM has provided the state security apparatus with widespread access to the communications and activities of private citizens. First introduced as a system for monitoring telephone communication (SORM-1), the technology has been updated periodically to include surveillance of Internet traffic (SORM-2) and storage of user data in its most recent iteration (SORM-3) (Soldatov 2017, 49). The mandatory installation of SORM surveillance technology essentially permits the FSB warrantless access to any Internet user's metadata so long as it is stored on domestic Russian servers.

For a little over a decade, very few changes were made to the Internet governance model under Presidents Putin and Medvedev. Although SORM technology existed and enabled advanced digital control, the state played a minimal role in the digital IE. However, when tens of thousands of protesters took to the streets of Moscow in 2011 and 2012, congregating at Bolotnaya Square across the river from the Kremlin, then-President Medvedev and Prime Minister Putin took notice.

To the state's horror, the mass mobilization of citizens opposing the "election fraud" that had put Putin back in office were organized mainly on U.S.-based social media sites (Soldatov 2017, 56).

After the 'color revolutions' in the surrounding Commonwealth of Independent States (CIS), the Bolotnaya protests marked a turning point or critical juncture for digital freedoms in Russia as the state became emboldened to assert its claim over the domestic digital information environment (Faulconbridge 2014; HRW 2017).[13] Putin's characterization of the Internet as a "CIA project" in April 2014 underscored his deep-seated fear that the digital information environment could undermine his government, just like the Arab Spring protests had galvanized citizens and brought chaos to other regions (Nocetti 2015, 112). The pace of change in Russian Internet governance increased dramatically thereafter (Deibert and Rohozinski 2010; Soldatov and Borogan 2017, 56).

In the wake of the protests, "Russian law enforcement agencies started to closely monitor closely the impact of the political use of networked technologies upon social mobilization and democratic transition" (Nocetti 2015, 113). Invoking justifications of safeguarding the nation from extremism, violence and offensive content, the Russian state has rapidly implemented a series of amendments to the Russian Criminal Code and new legislation that fortify each level of network governance encapsulated in the analytical framework. A group of amendments to the Criminal Code in 2016 increased punishments for Internet users deemed to be "inciting hatred" or making "public calls for terrorism" (Roudik 2016). In addition, a 2015 Minkomsvyaz (Ministry of

[13] Capoccia and Kelemen define "critical junctures" as "relatively short periods of time during which there is a substantially heightened probability that agents' choices will affect the outcome of interest…This definition captures both the notion that, for a brief phase, agents face a broader than typical range of feasible options and the notion that their choices from among these options are likely to have a significant impact on subsequent outcomes" (Capoccia and Kelemen 2011, 348).

Communication) order, obliges operators and service providers to both pay for and install the SORM "black box," enabling the Federal Security Service (FSB) to access user data and all digital communications and Internet traffic from ISPs without so much as a search warrant (Soldatov and Borogan 2017, 68). This legislation introduced the third generation of SORM technology, which, combined with Deep Packet Inspection (DPI) technology, ushers Russia into a new era of Internet governance capability (Soldatov and Borogan 2017, 51).

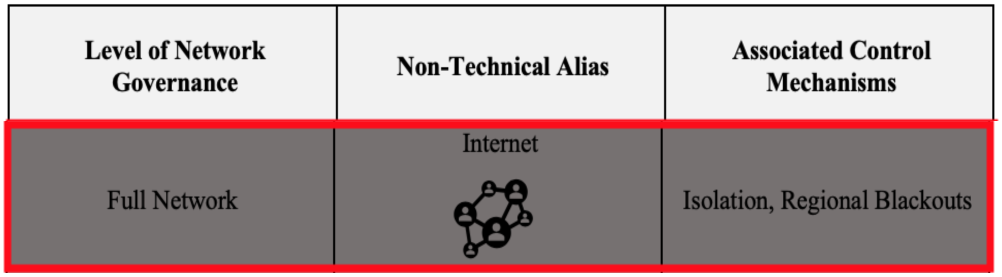
## Russian Governance at each Network Level

In this section the Russian Internet governance model will be examined systematically by each level of network control. Russia, like China, governs its Internet at each of the four levels specified in the framework. Russia's extensive Internet governance model is newer than China's but rapid, recent changes to Russia's legal and technological capacities have caused domestic and international observers to liken it to some of the most extreme digital authoritarians, such as China and Iran (Deibert and Rohozinski 2010; Nocetti 2015; Polyakova and Meserole 2019).

### *Internet Governance Institutions*

In comparison to the Chinese system, Russia's hierarchy of Internet governance institutions is significantly less centralized, with authority shared among many distinct and relatively autonomous governing bodies. Nocetti argues that, "Contrary to common preconceptions, there is no homogeneity of views on Internet governance and cyber security matters within the Russian decision-making elite" (Nocetti 2015, 118). Among the political entities directly involved in Internet governance agenda-setting are the presidential administration, Security Council, Ministry of Communications, Ministry of Internal Affairs, a variety of federal law enforcement agencies, and “vigilantes” loosely yet officially tied to the state. Upwards of 11 agencies are responsible for blocking sites and content, ranging from Roskomnadzor, a subdivision of the Ministry of Telecommunications (Minkomsvyaz) to the Federal Tax Service and the Federal Service for Alcohol Market Regulation (for more, see Figure 3 in “Sub-Network” section below). Within the Ministry of Internal Affairs (MVD), a federal policing body known as the Center for Extremism (Center “E”) patrols the web looking for individual and collective abuses of federal Internet standards and referring perpetrators to the court system. Multiple agencies manage federal blacklists, creating confusion for ISPs who are responsible for blocking the sites included on the lists. The result of the overlapping responsibilities of these governing bodies is a general “incoherence” of a singular message or agenda of Internet governance. This phenomenon will be depicted in greater detail in the following sections through analysis of the inconsistency of prosecution outcomes and the conflict between regional courts and the executive over applications of federal laws, such as the recently decriminalized Article 282 of the Criminal Code.

### *Full Network Level Governance*



| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Full Network | Internet | Isolation, Regional Blackouts |

Russia has made considerable legal and technological changes to its full network infrastructure in the past few years. On November 1st 2019, Federal Law No. 90-FZ came into force, legally authorizing the government to isolate the Russian Internet from foreign information flow in the face of certain—initially unspecified—threats. Just months before the provision entered into force, the Russian Ministry of Justice released a statement framing the law as a protection against “aggressive actions from abroad,” such as affronts to the network’s “confidentiality, integrity, and accessibility” (Газета.ру 2019). Such external threats could trigger the complete isolation of Russian Internet traffic by Roskomnadzor, the Federal Service for Supervision of Communications, Information Technology and Mass Media, the government entity at the heart of Russian Internet governance in practice (RF 2019; Газета.ру 2019). This update, coupled with the proposed adoption of full network-level Deep Packet Inspection (DPI) technology by 2021, which enables more advanced means of locating, inspecting and filtering data on a detailed level, would enable the government to employ more sophisticated, centralized controls on the Internet (Seddon and Foy 2019).

However, the hardware and software necessary for the Internet isolation infrastructure is estimated to cost the government about 134 billion rubles (approx. $2.1 billion) per year (Moscow Times 2019). For now, only 30.8 billion rubles (approx. $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, 12). In addition to the steep cost of the technology, some observers questioned the feasibility of the project in practice, pointing to the potential need to overhaul of the entire network infrastructure in order to achieve true full-network isolation.

Although many remain unconvinced of the state’s capacity to isolate the entire network, state officials offer a more optimistic outlook. Alexei Sokolov, the head of the Ministry of Communications, confirmed that in December of 2019 a test of the isolated web was successfully conducted: “The results of the exercises showed that, in general, both the authorities and telecom operators are ready to effectively respond to emerging risks and threats, to ensure the stable functioning of both the Internet and the unified telecommunication network in the Russian Federation" (TACC 2019). Such isolation exercises are slated to take place once a year in the near future (Meduza 2019a). Although it is difficult to confirm the success of these tests in practice, subsequent developments in ISP cooptation and overall network control increase the likelihood of the state's capacity to more meaningfully control the flow of information on the Internet. For the meantime, while this project remains in development stages, it is impossible to determine the Russian state's efficacy in full-network control.

However, not only does the Russian state possess the legal authorization to isolate its domestic Internet, it has cut off regional service during periods of increased political demonstration or anti-state unrest. The first instances of state-mandated regional Internet outages in Russia are reminiscent of incidents in China and are legally authorized by Article 64 of the Law on Communications. In fall 2018 and spring 2019, cellular data service was blocked in Ingushetia in response to regional unrest and calls for separatism. According to Reuters, a document recovered from the Ingushetia office of Roskomnadzor confirmed that 3G and 4G mobile Internet services were cut off from October 4-17 "on the basis of the justified decision of the law enforcement authorities" (Kolomychenko 2018). In June, October, and November 2018, during mass protests over a border agreement with the Republic of Chechnya, three major mobile service providers staged a blackout of network servers in response to a request from state security agencies (FH 2018). It is suspected that similar measures were taken in summer 2019 during the protests in Moscow (Shabaz and Funk 2019).

Another recent change in Russian full network governance is the decision to increase critical infrastructure security by replacing foreign technologies with domestic alternatives, a move that bears striking resemblance to the Chinese Internet governance strategy. A 2015 federal decree

"On the establishment of a ban on the admission of software originating from foreign countries for the purposes of procurement for state and municipal needs" marked a concerted move towards greater domestic technological autonomy for official use (Stadnik 2019, 3-4). Although there are significant costs associated with this long-term plan, the intention is to eventually remove any opportunities for foreign intervention or malign activities in the domestic network infrastructure.

### *Sub-Network or Website Level Governance*

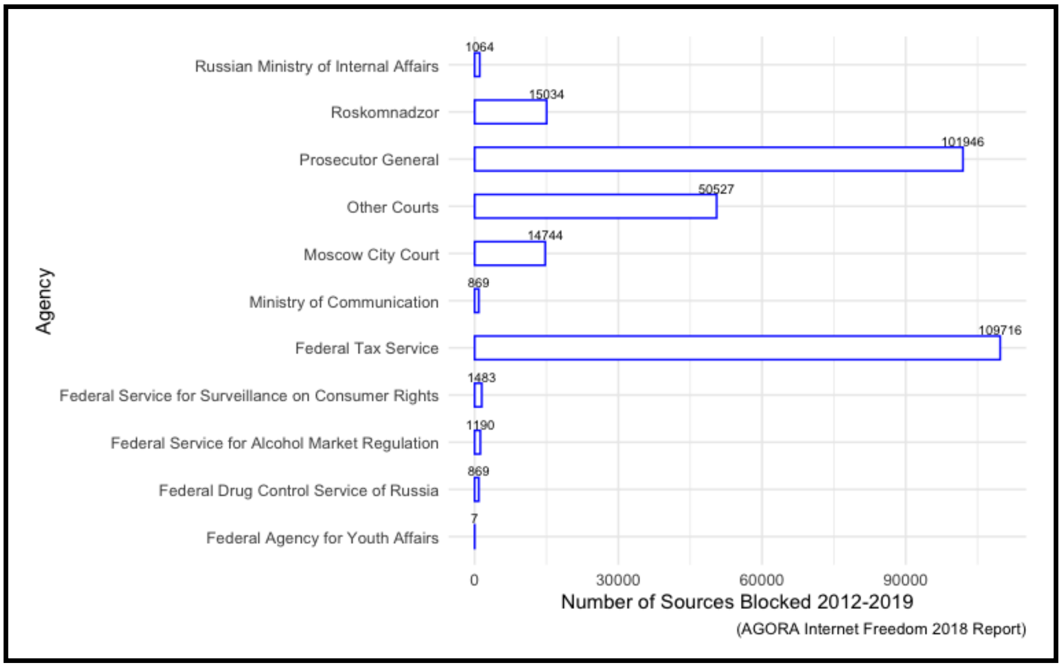
| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Sub-Networks | Websites<br>🗔 | Blacklisting, Blocking, Filtering |

In 2012, following the Bolotnaya Square protest, the 2006 federal law № 149-FZ "On Information, Information Technologies and Information Protection" was amended to include Article 15, a provision for a national blacklist of digital and non-digital materials with implications of suicide, drug use, child pornography, or other inappropriate content (Griffiths 2019, 267). A year later three additional federal blacklists were created for piracy websites, sources promoting extremism, and unauthorized protests (HRW 2017; Soldatov 2017, 40). Scholars often criticize states' creation and use of blacklists because they "undermine transparency and due process" (Mueller and Wilson 2010, 198). For that matter, the extremism list is the only blacklist that is publicly accessible, although it provides only minimal background information about blocked content.[14]

[14] To see a full list of administrators or for more information about the list itself, see https://reestr.rublacklist.net/visual/

The blacklists are each maintained by many disparate and overlapping government entities including the Federal Drug Control Service, Roskomnadzor, Prosecutor General's Office, Ministry of Internal Affairs, Ministry of Communications, Moscow City Court, Federal Service for Alcohol Market Regulation, Federal Agency for Youth Affairs, Federal Service for the Oversight of Consumer Protection and Welfare, and the Federal Tax Service. Each list is comprised of different content and compiled on the basis of different, opaque protocols determined by the various responsible governing bodies. As of May 2019, approximately 4.1 million Internet resources, or 96 percent of blocked content, were done so without any prosecution record or warrant (FH 2019b). According to statistics collected by Roskomsvoboda, between 2012 and 2019 the Federal Tax Service and the Prosecutor General's Office were the two most active contributors to the blacklists (see Figure 3 below). Although the Prosecutor General's Office is a logical body for blocking websites and content on the Russian Internet, it less obvious why the Federal Tax Service plays a disproportionately large role in these activities.

***Figure 3. Distribution of Digital Blocks 2012-2019 by Agency***



(AGORA Internet Freedom 2018 Report)

While federal government entities maintain these blacklists, several *ostensibly* non-governmental, “vigilante” organizations police the web in support of federal legislation, flagging posts for inclusion in the banned materials registries. In particular, two non-profits, *Molodezhnaia Sluzhba Bezopasnosti* (MSB- Youth Security Service) and *Liga Bezopasnogo Interneta* (LBI- Safe Internet League), have been patrolling the RuNet since the early 2000s and 2011, respectively (Daucé, et al. 2020, 48). Although technically unaffiliated with the government, these organizations are responsible for alerting authorities to posts, especially on VKontakte, that represent an affront to the cultural, political, or social standards enshrined in Russian legislation (Daucé, et al. 2020, 49).

MSB claims to specialize in preventing “drug trafficking, organized crime and corruption, terrorism and extremism (racial and ethnic hatred, religious radicalism), online economic crime, child pornography, pedophilia, incitement to suicide,” whereas LBI has focused on the “fight against pedophilia, homosexuality, extremism, prostitution,” but also animal cruelty (Daucé, et al. 2020, 50). LBI has recently extended the mandate of its digital vigilantism by establishing “Cossack cyber patrols” to more effectively “Defend the digital borders” (Daucé, et al. 2020, 59). In fall 2018, two deputies from Putin’s United Russia Party introduced a bill that would formally recognize digital vigilantes and lend government support to “combat Internet dissemination of information prohibited in Russia, particularly concerning war propaganda and incitement to national, racial, or religious hatred” (Daucé, et al. 2020, 47). This would mark a transition from the vigilantes’ non-profit “auxiliary” function to formal recognition and incorporation into Russia’s Internet governance regime.

Once a page has been blacklisted, the legal burden falls on ISPs and communications companies to individually block sites and content, according to a 2006 federal law (Maréchal

2017). In this respect, the system remains somewhat decentralized as the state relies on both public and private providers to carry out its orders. For the most part, content filtration is manually conducted by a large policing entity called the Anti-Extremism Center ("Center E"). The "Center E" was initially created in 2008 to serve as a federal police headquarters but, after the protests in 2012, expanded to include district-level police offices. The Center is vast and houses various departments, including one for general counterterrorist measures, religious extremism, nationalist extremism, and "suppressing extremism at public events" (Meduza 2019c). Center E employees, known as "eshniki," are embedded in protests to document demonstrators and identify the most active participants (Meduza 2019c). Some eshniki, like Alexey Okopny, are even publicly known and recognized (Meduza 2019c). For more information about the Center, see the "Network-Node or Individual Level Governance" section below.

One of the best insights into Russian blacklisting is the open-source data from the official federal "extremism list," which has been updated regularly since 2005.[15] As of October 2019, the blacklist consists of 4,959 entries, at least 215 of which have been labelled "excluded" (*isklyuchyon*) and do not have identifying information or date. It is unclear if this denotation is meant to signify that the entry is no longer considered extremist or if the material is too sensitive to publicize. Each entry has been added to the list in accordance with court proceedings in various regions of the Russian Federation.

A random sample (n=150) of the entire dataset from 2005-2019 reveals that 82% of entries were added to the extremism list in 2011 or later. Of this random sample, at least 63% of materials were digital in nature (websites, digital articles, social media video, audio clips, posts, or

[15] For updated extremism list data, see https://minjust.ru/ru/activity/extremism

comments) and 15% were non-digital materials (brochures, books, poems, songs, and newspaper articles).[16] Of the entries which could be definitively categorized, 54% of digital materials were found on social media sites, mostly of the domestic variety (90%) like VKontakte and Odnoklassniki. The remaining 46% of digital materials were websites themselves or their content.

A random sample (n=150) of all extremist materials included during or after 2011 reveals that at least 73% of materials are digital in nature. This finding denotes a significant recent trend towards stronger digital information regulation in Russia since 2011. Moreover, 70% of digital blacklisted materials were located on social media platforms, of which 87% were domestic platforms. Of the domestic social media entries, 87% were located on VKontakte. Less than 13% of the blacklisted materials were located on foreign social media platforms, perhaps suggesting that the state prioritizes digital control of the *Russian* social media sphere as opposed to international platforms. This bias could also be the result of technological limitations. The remaining 30% of digital materials were materials on websites or websites themselves.

The content of the extremism list closely mirrors the Russian white paper from 2016, which condemns subversion of national unity, violence motivated by ethnic or religious bias, and reinterpretations of important historical narratives. Materials labelled extremist on this public list often contained illusions to hatred of religious of ethnic identity, incitements of regional separatism or religious minority empowerment, revisions of state-approved history, and occasionally criticism of Putin and his administration. The vast majority of entries on the list indicated an affiliation with skinheads or Neo-Nazis and expressed hatred towards Jewish, Central Asian or Caucasian people. Another large subset of entries were related to Islam but no distinction was drawn between

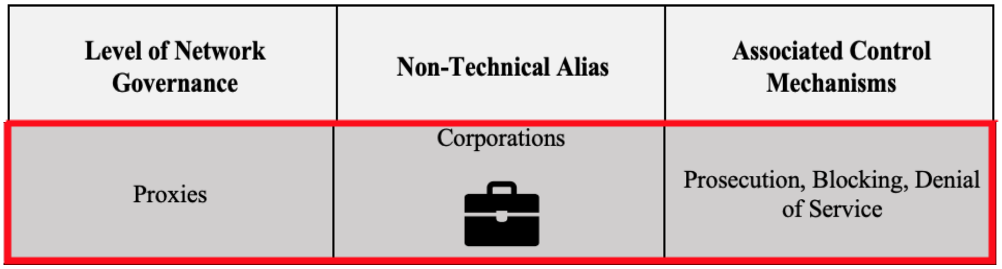
[16] The remaining 22% of entries in the sample could not be definitively categorized as digital or non-digital.

informational texts on the faith, pro-Islam calls for separatism in regions, and incitement of violence in the name of Jihad. Several materials about Soviet or more recent Russian history from the perspective of a minority group (such as the Jewish diaspora) were included on the list. A few entries stood out from the more predictable content themes. For example, it is unclear why a university lecture from 2016 on the history of human rights and law in Russia would be included on the extremism list. Similarly, "Zhuan Falun," the seminal text for the Falun Gong religious movement, and several books by L. Ron Hubbard, the founder of Scientology, also appear on the extremism list. Although considered extremely subversive in China where it is subject to strict censorship in print and online, it is unclear why the Falun Gong text would be considered extremist in the vastly different Russian cultural and political context.

The extremism list samples demonstrate a trend towards increased restriction of contentious digital materials in the Russian information environment. The disproportionate blacklisting of Russian social media content underscores the state's desire to govern its digital space as an extension of its territorial sovereignty. Although this extremism list provides some context for digital controls in Russia, it also raises further questions. Why are international social media platforms seemingly left off the list or targeted with less frequency? Why is some content on the blacklist seemingly unrelated to extremism? These findings may indicate that the Russian state faces resource constraints, operational challenges in deploying content flagging on non-Russian language pages, or that the state does not wish to anger international social media companies with large-scale blacklisting. It is likely that it is simply easier for the state to effectively govern domestic websites and social media platforms.

Users can find still ways around the blacklisted and blocked sites. In 2013 the Deputy Head of Roskomnadzor admitted that technologically, the government entity had only seen mixed results when it came to preventing access to certain pages or content: “advanced users have, in most cases, the ability to bypass the blocking,” but that this was of little concern as the fraction of the population with requisite knowledge about bypassing blacklists was “negligible at present” (Soldatov 2017, 42). However, as time goes by and the population grows more technologically savvy, the state’s Internet governance measures could be flouted in higher numbers. Perhaps motivated by these very concerns, in July 2017 lawmakers passed restrictions on virtual private networks (VPNs) to prevent users from accessing banned sites that are hosted outside the country (FH 2018, 15). Even still, some users manage to find ways around the laws. Many websites, including one entitled “openrunet” provide step-by-step guides for users to skirt blacklisted content with VPNs.[17] While total VPN usage is low in Russia like in China, more than 20 percent of Russians between the ages of 18 and 24 are estimated to use this circumvention tool (FH 2019b).

### *Proxy or Corporation Level Governance*



| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Proxies | Corporations<br>💼 | Prosecution, Blocking, Denial of Service |

The state channels a great deal of attention and resources into the proxy level of network governance. Almost all Internet service or telecommunications providers in Russia are licensed by Roskomnadzor. Furthermore, of the four main private providers MTS, MegaFon, VEON, and Tele2, two have been taken over by Rostelekom (now the primary stakeholder), a state-owned

[17] To access this site, see link: https://openrunet.org/#select

and dominant force in the broadband market (FH 2019b). Due to limited competition in the ISP sector, the Russian state is able to exercise a significant amount of power over this type of "proxy" actor.

According to its website, Roskomnadzor requires ISPs to frequently check federally-maintained blacklists as new websites and content are added. The penalties of non-adherence are fines and denial of operation. Moreover, ISPs are required to both pay for and install hardware, such as the SORM black box, which intercepts communications traffic. This technology allows the FSB to present a warrant to the Ministry Justice for seizure of a private citizen's data without providing any information (or the warrant) to the ISP itself (Soldatov 2017, 55). The provider must comply or face legal consequences. Most recently, Roskomnadzor asked ISPs "to provide information about physical Internet exchange points that they and network operators use to exchange Internet traffic" before the November 2019 Internet isolation law came into force, suggesting a move towards greater centralization and cooptation of providers by the state (FH 2019b).

However, the other actors at the "proxy" level of network governance are the social media and communications platforms, many of which are international, posing a unique challenge to governance. Whereas the Chinese Firewall blocks its domestic users from accessing international sites like Google, Facebook, and Twitter, users in Russia can access all but a few of these services, including LinkedIn. Like China, a myriad of domestic Internet platforms and products exist, including Yandex (a company that began as a search engine but has since expanded to ridesharing, online food ordering and delivery, digital media streaming, among other services), VKontakte (an analog of Facebook), Odnoklassniki (another social media site), and several other media conglomerates and search engines such as Mail.ru, Rambler, and Sputnik. Generally speaking, Russian netizens use a combination of domestic and foreign Internet services;[18] for example, many Russians have both a Facebook and VKontakte account.

The Russian state has made several recent attempts to bring these more distant "proxies" directly under its sphere of influence. The July 2018 Yarovaya Laws compel corporations operating in Russia to store users' data, including text and voice messages, photos, and videos, and more, for up to six months. This modification of Article 10.1(3) of the Federal Law on Information, Information Technologies and Data Protection of 2006 (149-FZ) essentially provides the FSB with unrestricted access to user data. (FH 2018, 15; Gorodissky and Partners 2018). Russian security services have warrantless access to data stored in the territory of the Russian Federation. Therefore, it is in the state's interest to compel non-native social media and other companies to store data on Russian soil to ensure widespread surveillance (Maréchal 2017). The Ministry of Communications plans to localize 99% of all Internet data by 2020 (Polyakova and Meserole 2019, 8).

For many of the reasons mentioned above, foreign firms like LinkedIn, Twitter, Google, and Facebook have refused to comply with laws that essentially permit the Russian state access to their users' and internal company data. In 2016 LinkedIn became the first international platform to be blocked in Russia after refusing to comply with these laws. Twitter and Facebook were charged and fined in 2018 (FH 2019b). Meanwhile, the likes of Lenovo, Microsoft, Booking.com, Uber, Samsung, Aliexpress, eBay, and PayPal upgraded to cloud services for processing personal

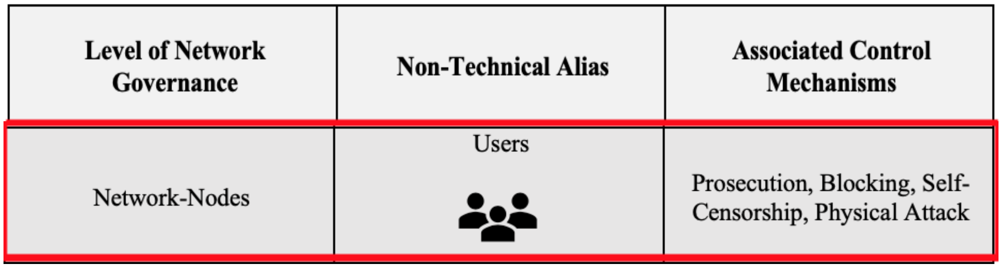
[18] One 2018 poll conducted by the Levada Center demonstrated that Russian citizens are increasingly likely to seek out domestic and world news from online social media sites and online publications than ever before, with a 22 and 28% increase, respectively, since 2009. In the same survey, respondents were 21% less likely to seek out TV news than survey respondents just nine years prior (Levada 2018). Nevertheless, TV remains the most sought out source for national and international news, representing approximately 73% of citizens' top choice. However, younger Russians (aged 18-24) are almost equally likely to seek out the news from Internet (49%) and TV sources (54%) (Levada 2018). This Russian generational shift poses a threat to the authoritarian system maintained by the Putin administration.

data in order to skirt the FZ-242 data localization law (Stadnik 2019, 7). In 2018 BlackBerry Messenger, imo, Line, Vchat, and Zello were blocked for not handing over encryption keys to Roskomnadzor (Shabaz and Funk 2019). In the same year, the state blocked Google IP addresses and fined the company 500,000 rubles (approximately $8,000 at the November 2019 exchange rate) for defying its data storage provisions (Seddon and Foy 2019). This paltry fine reveals the inability for Russian Internet governing bodies to firmly crack down on international firms such as Google (Stadnik 2019, 6). Other international companies, including Uber and Viber, have opted to comply with Russia's strict data laws (FH 2019b).

The CEO of Telegram (a native-Russian messaging service) was prosecuted by the state in 2018 for both refusing to both store company data on domestic servers and provide encryption keys to the state for state surveillance purposes (Griffiths 2019, 270). When Telegram initially attempted to skirt federal blocking, Roskomnadzor demanded that at least 18 million IP (Internet protocol) addresses be obstructed. Since 2018, access to Telegram has been mostly restored to users, including many of the government employees that relied on the messaging service for official purposes (2018, 15). As of May 2019, over one million IP addresses remained blocked in connection with the Telegram order, according to a monitoring bot (Shabaz and Funk 2019). Roskomnadzor was somewhat discredited by its inability to completely block Telegram and ensure the platform's adherence to federal laws (Stadnik 2019, 10).

One recent law, which came into force in January 2020, requires that Apple and other mobile phone companies selling to the domestic Russian population pre-install applications ranging from maps, payment platforms, and social media sites that Russia's Federal Anti-Monopoly Service (FAS) deems of "moral and spiritual" social significance (Кречетова, et al. 2020). Although little is known yet about the content or surveillance potential of the apps, one can't help but see a parallel with China's mandatory surveillance app in Xinjiang that enables the police force to track civilians' whereabouts and access their private messages. If the speculation about the Russian applications is confirmed, this could represent a step towards more large-scale surveillance of citizens in keeping with the Chinese model. Taken as a whole, the recent Russian legal provisions pressure "representatives of Internet businesses to behave more cautiously, to engage in self-censorship, and to run constantly to the Kremlin for consultation," an element of authoritarian resilience found in Chapter One (AGORA and Roskomsvoboda 2020; Soldatov 2017, 44).

### ***Network-Node or Individual Level Governance***



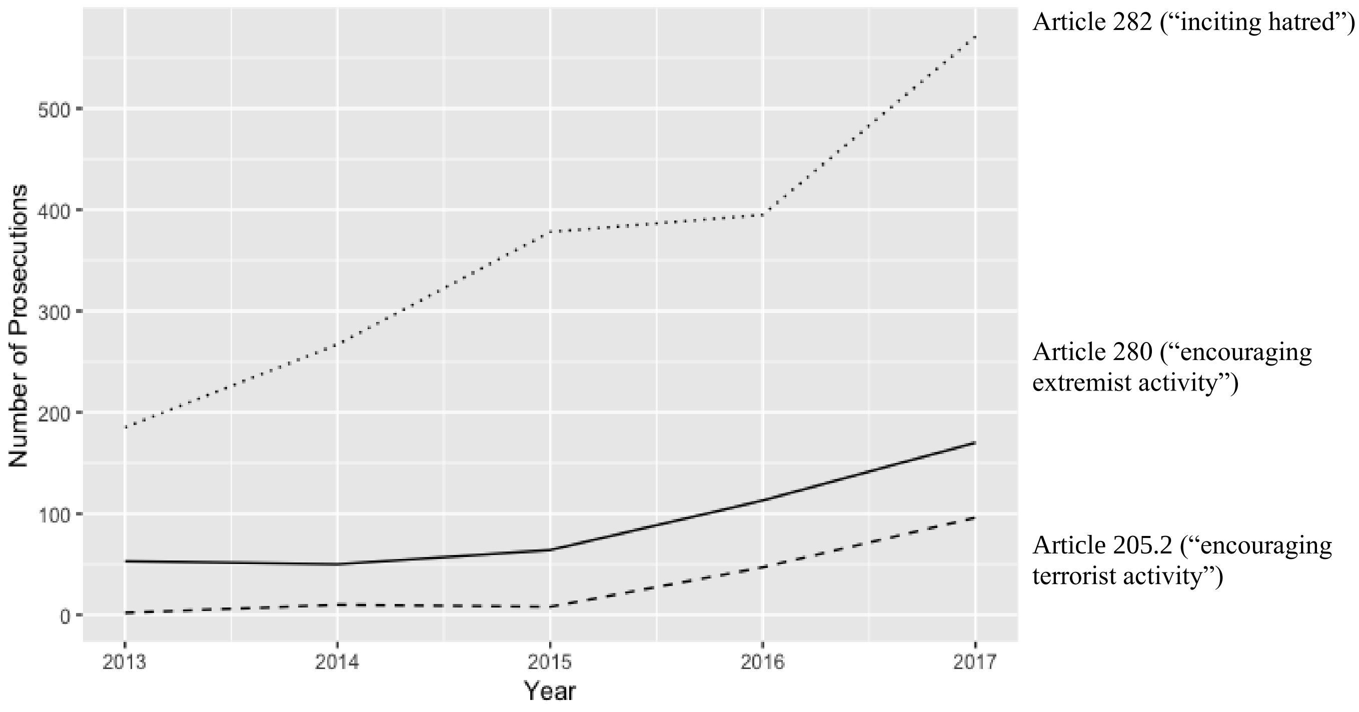
| Level of Network Governance | Non-Technical Alias | Associated Control Mechanisms |
|---|---|---|
| Network-Nodes | Users<br>👥 | Prosecution, Blocking, Self-Censorship, Physical Attack |

The last level of governance in the analytical framework considers restraints on individual Internet users, or netizens. With the advent of social media networks like Twitter, Facebook, Instagram, and similar Russian-language versions, it is becoming easier to express one's opinions to a large audience. If a post goes viral, it can reach millions of other users, thereby posing a considerable threat to authoritarian regimes attempting to stifle some voices (oppositional or not) and control narratives around specific topics. The threat that an individual Internet user, especially when in a position to reach thousands or millions of other users, is massive to an authoritarian regime that intends to control the distribution and access of information within and beyond its borders. The Russian state, like its Chinese neighbor, appears to punish some individuals—such as Oksana Pokhodun—who are perceived to pose a threat to their regime not just online, but in a physical political mobilization effort (King, et al. 2013). In this way, the state may intend to preempt unwanted political opposition and demonstrations by intercepting such oppositional figures and making prosecutions on the grounds of digital activity.

When it comes to governing the Internet user, the Russian legal system relies on a series of interconnected laws, most of which are amendments to the Russian Criminal Code and the Code of Administrative Offenses, that govern the information environment broadly, not just its digital realm. In recent years, legislation like the 2014 “Bloggers’ Law” (Federal Law № FZ-97) and amendments to the Russian Criminal Code have placed extraordinary pressure on the individual Internet user in Russia. According to the Bloggers’ law, Internet users whose posts are visited more than three thousand times per day are required to register their legal surname and provide other identifying information to Roskomnadzor (HRW 2017). The Russian Blogger law closely resembles China’s “microblogger” law which also denies users digital anonymity.

As Figure 4 depicts below, online behavior is mostly governed by Articles 280 (“encouraging extremist activity”), 282 (“inciting hatred”), 205.2 (“encouraging terrorist activity or public justification of terrorism”), and 148 (“insulting the feelings of believers”) of the Criminal Code. 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 remain in place to deter specific Internet behavior and usage deemed unsavory by the state (HRW 2017; Verkhovsky 2019).

***Figure 4. Number of Prosecutions 2013-2017 Per Article of the Russian Criminal Code***



Sources: AGORA Internet Freedom 2018 Report, AGORA 2019b

The legal climate in Putin's Russia is complex and is influenced by both directives from the top and varied conditions and inconsistent enforcement at the regional levels. The law invoked most often for prosecutions of individuals online, Article 282 governing hate speech (represented in Figure 4 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 (see Figure 5 below). AGORA also identifies Articles 280 on encouraging extremist activity (solid line) and 205.2 public justification of terrorism or encouraging terrorist activity (dashed line) as the next most common charges. Although Article 282 of the Russian Criminal Code was partially decriminalized in 2018, only two and a half months after this prosecutorial easing, more direct restrictions on freedom of speech were introduced in Russia. 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 (Sulim 2019; Verkhovsky 2019). Individuals may also be added to the extremism list maintained by the Federal Financial Monitoring Service (Rosfinmonitoring).[19] In the following section, examples of prosecutions will demonstrate the varied, extreme, and sometimes surprising instances of Internet governance on the individual Internet user level.

### *Sample Prosecution Cases of Internet Users*

Between 2014 and 2016, approximately 85% of convictions for “extremist expression” were made on the basis of online activities (HRW 2017). The sheer breadth of laws governing Internet activity provides prosecutors with a notable amount of autonomy in initiating and carrying out individual cases. However, courts are not the only government entities responsible for governing the individual level of the network. The Anti-Extremism Center is responsible for opening extremism cases before turning over individual prosecutions to the courts. Digital user content can be flagged by other social media users who bring concerns to the Center, officers who trawl the web themselves, or by orders from “above” in the case of high-profile individuals or “somebody who had become an inconvenience to the government” (Meduza 2019c). The origins of individual prosecutions usually remain obscure to the public.

Past prosecution records offer a window onto the Russian government’s Internet governance priorities and the topics it attempts to discourage on the web. This review is not meant to suggest that all Internet user prosecutions are unjustifiable. Some cases such as those punishing xenophobic ideas and implications of violence, would be considered valid in most regime types

[19] See the Rosfinmonitoring website here: http://www.fedsfm.ru/documents/terrorists-catalog-portal-add

and Internet governance models. However, a thorough analysis of past prosecutions also reveals that the state especially disapproves of criticism of President Putin, political authorities, and the Orthodox Church, and references to certain groups, such as the Nazis. The regional variation in prosecution outcomes described in this section raises questions about the centralization and consistency of Russia's Internet governance model overall.

In late 2016 and early 2017 a 20 year old from Kurgan published xenophobic drawings and an audio recording containing calls for violence against Central Asian and Caucasian immigrants on social media. A case was filed against her under Articles 280.2 and 282.1 of the Russian Criminal Code for public calls for extremism and incitement to national hatred. The case was ultimately terminated in February 2018 when the girl paid a 50,000 ruble fine, made a full apology, and gave a lesson on tolerance at a local educational facility (SOVACenter 2018). This case shows that the Russian extremism laws can be invoked for a more deliberate social purpose than mere discouragement of opposition voices. In contrast, the examples to come demonstrate the breadth and inconsistency in application of some of the same laws that nominally serve to punish inappropriate or socially detrimental behavior on the web.

Criticism of Putin takes various shapes and forms in Russia. From public remarks and protests to social media posts, anti-Putin sentiment appears in various realms of the Russian information environment. Digital criticism of Putin himself, his administration, and his policies are punished by Russia's legal system. In fact, AGORA and Roskomsvoboda report that in the last year, Internet users paid roughly 1 million rubles ($15,900) in fines for insulting state officials, with Putin as the most common target (AGORA and Roskomsvoboda 2020).

When one Novgorod resident posted “Putin is an incredible f…wit” (dots included in original post) he was quick to defend his position, emphasizing “It’s my right to write” (Baumgartner 2019). However, in May 2019, Kartizhev became the first individual charged under the newly amended Article 20.1.3 of the Code of Administrative Offenses for insulting the government and was fined 30,000 rubles (approximately $500) (Baumgartner 2019).

Apart from explicit criticism of Putin as an individual, criticism of his senior level administrators has resulted in prosecutions under the same legal clause. When journalist Fyodor Krashennikov posted the link to an article about the renewed detention of his activist friend on Telegram and remarked “These Putinist judges are such whores,” he was charged under the same law as Kartizhev in October 2019 for insulting authorities who represent the Putin administration (Meduza 2019b).

The prosecution of anti-Putin sentiment in Russia is not limited to criticism of government representatives. Internet users, like Oksana Pokhodun, are also punished for posting dissenting opinions of state policies, in an interesting counter-point to the findings from China in King, et al. Yekaterina Vologzheninova fell victim to the repressive legal regime on Internet use when she shared a cartoon on VKontakte that depicted President Vladimir Putin bending over a map of war-torn Eastern Ukraine with a knife in his hand. She was ultimately charged under Article 282 for “inciting hatred” and sentenced to 320 hours of community service (Litvinova 2016).

In some ways, it appears criticism of the Russian Orthodox Church is tantamount to condemnation of the state itself. In recent years, political pundits and scholars alike have followed Putin’s growing affinity for the Russian Orthodox Church. His repeated reference to “the destruction of traditional values from the top” and the controversial “re-Christianization” of Russia in the past two decades has demonstrated the mutually-beneficial relationship between Putin's administration and the Church (Fish 2018; Kaylan 2014). Some speculate that Putin's alliance with the Orthodox Church and its leaders, including Patriarch Kirill, is an element of his government's legitimation strategy (Fish 2018; Rivkin-Fish 2013). As the cases below demonstrate, protecting the Orthodox church and its believers from online criticism appears to be a priority of the Putin administration's Internet governance model.

In 2014 Viktor Krasnov expressed his atheist views on VKontakte, posting "God doesn't exist" and calling the Bible a "collection of Jewish fairytales." Two other VK users alerted authorities to the posts, claiming to be "insulted" by his words (Litvinova 2016). The prosecution first brought charges under Article 282 for "inciting hatred toward religion," later modifying the charges to Article 148 for "insulting religious believers" (Litvinova 2016). Although the case was dropped after the two petitioners were found lacking evidence and refused to be part of the trial (Kommersant 2017), the case profoundly altered Krasnov's life; he lost his business, became unemployable elsewhere, and suffered from both the social and political repercussions of his public trial. Not to mention, the judge sentenced Krasnov to 30 days in a mental hospital, asserting that nobody "in sound mind would doubt or criticize the Orthodox church" (Litvinova 2016). Krasnov has not received any restitution for what appeared to be a gross violation of his rights.

In a similar case, then 20 year old Maria Motuznaya was the peculiar target of legal action on the grounds of religious-themed memes she had posted on VKontakte (Robinson 2018). One meme included an image of nuns smoking cigarettes and urging each other to be quick "while God isn't looking" (Robinson 2018). Although the humoristic style of Motuznaya's post may not appeal to all viewers, it may surprise some to learn that she was charged under Articles 282 and 148 and condemned to community service in exchange for a full confession just on the basis of posting these memes. In July 2019 Motuznaya successfully brought a counter suit to clear her name and received 100,000 rubles and an apology directly from prosecutor's office for the “moral harm” she sustained in the case (AGORA 2019a). Especially in comparison to Krasnov’s, Motuznaya’s case serves to demonstrate the unpredictable application of law in Russia.

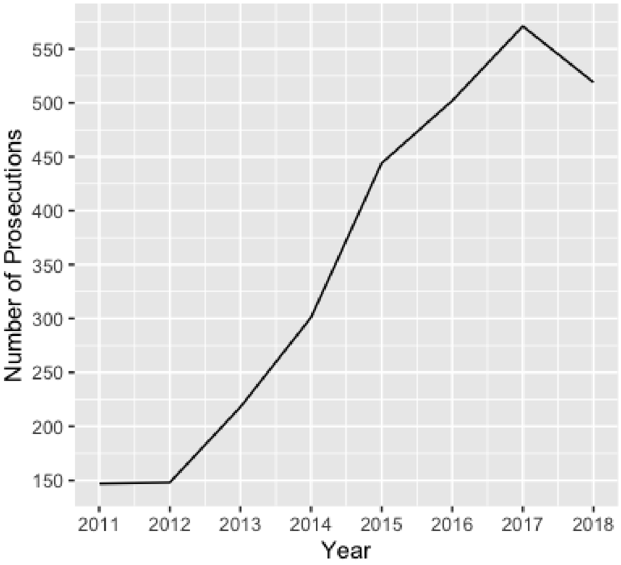
One point of sensitivity that appears both in the Russian and Chinese cases which is highlighted by the repressive legal regimes is the subversion of a singular, state-directed historical narrative. Russia’s disapproval of reinterpretations of history is explicitly mentioned in its white paper on Internet governance and deeply enshrined in laws. Some political scientists refer to this phenomenon in Russia as the “notion of content as threat,” which Nocetti argues is a product of the state’s “nebulous unease about the vulnerability of Russia’s national culture to outside influences” (Nocetti 2015, 116). The Russian state’s desire to create a unified interpretation of history heavily influences its Internet governance regime. 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, including aimed at undermining the historical foundations and patriotic traditions associated with the defense of the Fatherland.” (RF 2016). Interestingly, the term “fatherland” invokes the defense of the fatherland in the second world war.

Perhaps the most unique Russian law applicable to Internet activity is one punishing “the rehabilitation of Nazism” in speech or image. Although Russia is not alone in its legal provision banning Nazi flags and imagery—others include Germany, Austria, Hungary Latvia, Lithuania, Poland and Ukraine—its law is rare in that it does not, like the aforementioned countries, distinguish between the educational, historical, or artistic use of the flag and more problematic usages. The application of this law in practice is inconsistent and at times surprising. For example, when Ilya Varlamov reposted a photo from a World War II museum in Gdansk in 2018, his post was flagged and he was detained by the Ministry of Internal Affairs’ Center "E" because one of the photos contained a flag bearing a swastika (AGORA 2019b). Varlamov claimed that he neither supported nor intended to promote Nazi values but rather had wished to make a blog post about his experiences at the museum. While detained, Varlamov claimed he was questioned about whether he was involved with opposition figure Alexei Navalny or attended any protests in the recent past. Varlamov was ultimately found guilty of violating Part 1 of Art. 20.3 Administrative Code (public demonstration of Nazi paraphernalia or symbols) (AGORA 2019b).

In a similarly befuddling prosecution under Article 20.3 of the Administrative Code, Vladimir Luzgin was convicted of “falsifying history” after reposting an article on VK that suggested the Soviet Union bore some responsibility for the outbreak of WWII by invading Poland (AGORA 2019b; HRW 2017). This legal decision appears to be motivated not by the intention to prevent violence or hatred but rather by the agenda to promote a uniform and state-approved interpretation of Soviet history, especially when it comes to the “Great Patriotic War.” It is widely understood that in the “Putin-Medvedev memory regime” representations of World War II are “central to the Russian national self-image” to the extent that “professional historians…are not presently able to keep its elaboration within scholarly canons” (Vihalemm and Jakobson 2011). Regional courts bolster the administration’s desire for a uniform historical narrative by prosecuting individuals for ostensible breaches. Scholars such as Vihalemm and Jakobson consider the “Nazi Rehabilitation Law” as one of several tools utilized explicitly to homogenize historical memory according to the state-approved version. Although discouraging violence in the name of Neo-Nazism is reasonable in theory, some prosecutions, like those above, demonstrate a demonstrate a more authoritarian agenda in practice.

Given the extensive mandate of federal laws in place for governing individuals' use of the Internet, Russia appears on paper to be one of the world's most extreme digital authoritarians. However, the governance on an individual level is notably inconsistent. For example, in December 2018 when Putin ordered a partial decriminalization of Article 282 (inciting hatred law), ordering first-time offenses to be treated as an administrative misdemeanor rather than as a federal crime, regional courts heeded the warning (Verkhovsky 2019). This executive order by the President is considered an attempt to rein in unruly regional prosecutors, indicating that variation in the law's enforcement across the Russian Federation was significant enough to attract the attention of the president. In a meeting about the partial decriminalization, Putin underscored that the police's job was to "stop pulling criminal cases out of thin air and start focusing on preventing extremism" (Sulim 2019).

***FIGURE 5. NUMBER OF PROSECUTIONS UNDER ARTICLE 282 OF THE RUSSIAN CRIMINAL CODE 2011-2018***



Sources: AGORA Internet Freedom 2018 Report

The notable decline in prosecutions under Article 282 leading up to and after Putin's executive order (depicted above in Figure 5) underscores the power of the executive branch to direct certain interpretations of the law and suggests the desire for top officials to set an agenda for such prosecutions. Whereas in 2017, about 127 extremism cases were brought forward per month, in 2018 this number decreased to 105 per month, and an average of 41 in the first two months of 2019 (Verkhovsky 2019). This partial decriminalization is a result of wide variations in regional Internet governance and demonstrates a notably more decentralized approach in Russia than in China. Furthermore, the origins, outcomes, and degrees of punishments of each prosecution case highlighted above are unpredictable at best. Prosecutions are determined heavily by regional interpretations of the law, but also by executive orders. The Russian state's inconsistency of individual-level Internet governance could also be a tool for encouraging self-censorship. By identifying and punishing a number of unpredictable and regionally disparate Internet users, the state intentionally or unknowingly scares many netizens into submission to certain state- approved digital behavior.

**Conclusions from the Russia Case:**

The Russian Internet governance model is newer and undergoing recent and rapid change in comparison to the Chinese model. Russia's institutional oversight of its digital information environment is less coordinated and centralized than China's. Not to mention, the Russian state does not utilize centralized points with which to control Internet service provision but instead contains decentralized points which ISPs and other proxies much police for themselves, in adherence to government mandates. For many of these reasons, the Russian Internet governance model appears somewhat inconsistent in application of both technical (digital) and traditional (non-digital) mechanisms.

As Russia's governance model becomes more sophisticated and its restriction capacity grows, there could be significant repercussions. Perhaps due to the relative freedom of access that Russian Internet users have enjoyed for decades, Russian citizens have been expressed strong opposition to censorship. According to Pew Research Center's Spring 2015 Global Attitudes 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 restrictions while maintaining regime legitimacy and stability.

## HOW AND WHY DO THE RUSSIAN AND CHINESE MODELS DIFFER?

The cases of Russia and China demonstrate the increasing ability of different states to govern the Internet according to similar authoritarian standards despite varying resources, political structures, and other institutional differences. In many ways, an exploration of Chinese and Russian Internet governance has demonstrated the similarities of the two models—for example in justification or legitimation of Internet control, reliance on common authoritarian resilience mechanisms, and mutual promotion of international Internet sovereignty norms. A more thorough consideration of the models' similarities will precede an analysis of the traits that set the Chinese and Russian Internet governance models apart, namely differences in infrastructural centralization, and extent and pace of change in digital governance. The final section of this chapter identifies possible explanations for such differences in digital authoritarianism, building upon approaches that anticipate persistent differences on the grounds of digital development trajectories and varieties of authoritarianism.

### Similarities of Russian and Chinese Internet Governance:

Before expanding on the differences between the Chinese and Russian Internet governance models, it is important to acknowledge their points of similarity. An examination of the Russian and Chinese Internet governance models in previous sections has yielded the finding that both systems govern at all four levels of the digital network and employ a wide range of similar governance mechanisms, such as regional blackouts, legislation, prosecution, blacklisting or blocking, as well as promoting self-censorship. Moreover, both Internet governance models rely on similar authoritarian control mechanisms, and advance a global Internet sovereignty agenda.

### *1. Common (Digital) Authoritarian Mechanisms for Regime Survival*

Perhaps unsurprisingly, both the Russian and Chinese states employ more modern and technologically advanced versions of the authoritarian survival mechanisms described in Chapter One. More specifically, Russia and China practice "strategic repression and co-optation" by passing legislation to prohibit digital anonymity, extracting revenue and data from corporations, and allowing some contention on the web to ensure social stability (Geddes 1999; Slater and Fenner 2011, 15).

One shared strategy of strategic repression comes in the form denying users the ability to remain anonymous online. The 2005 Chinese blogger law, expanded in 2012, punishes social media users or "micro-bloggers" who post or comment online under a nickname or alias. A similar blogger registration law was passed in Russia in 2014 (HRW 2017). These anti-anonymity laws encourage greater self-censorship on public discussion boards and in private messages and signal to civilians that the state can track their content and bring charges for violations.

The Russian and Chinese Internet governance systems also rely on the cooptation of Internet service providers and other corporations. By passing legislation requiring companies to register with the state, store data on domestic servers, and provide encryption assistance to the state, Russia and China force corporations to abide by domestic laws and hand over proprietary and user data to state security apparatuses. In both Russia and China, Google, Facebook, and Twitter have been prosecuted, fined, and in several instances, blocked altogether from domestic service due to violations of data localization and encryption laws. By mandating that private sector entities, especially digital service providers, adhere to specific domestic legislation, Russia and China have encouraged ISP reliance on the state, coopting organizations that could otherwise pose a threat to regime survival.

Lastly, as many scholars on authoritarian resilience observe, both Russia and China permit some contention in the digital realm of the information environment (Brancati 2014, 314; MacKinnon 2011, 33). In order to maintain an accurate reading of public opinion, Russia and China must permit some opposition voices, thereby identifying possible threats to regime security. Providing limited forms of participation and debate is also a powerful tool for authoritarian durability because it convinces most users that censorship is conducted sparingly. In their study of Internet traffic censorship in China, King et al. observed that content condemning authority or policies is less likely to be censored by the Firewall than implications of collective action. They state, "Contrary to previous understandings, posts with negative, even vitriolic, criticism of the state, its leaders, and its policies are *not* more likely to be censored. Instead…Censorship is oriented toward attempting to forestall collective activities that are occurring now or may occur in the future" (King, et al. 2013). This study found that "when the Chinese people write scathing criticisms of their government and its leaders, the probability that their post will be censored does not increase" but rather, the Chinese system is said to employ a "paternalistic strategy to avoid chaos and disorder" that more rigorously polices content supporting or calling for political mobilization (King, et al. 2013, 3).[20]

[20] For an example of a post not censored despite its clear criticism of authorities, see the following: "'This is a city government [Yulin City, Shaanxi] that treats life with contempt, this is government officials run amuck, a city government without justice, a city government that delights in that which is vulgar, a place where officials all have mistresses, a city government that is shameless with greed, a government that trades dignity for power, a government without humanity, a government that has no limits on immorality, a government that goes back on its word, a government that treats kindness with ingratitude, a government that cares nothing for posterity....'" (King, et al. 2013 13).

While no similar study has been conducted to analyze the Russian censorship apparatus, a thorough analysis of Russian prosecution records reveals that some critical citizens are prosecuted for their statements, while others go unpunished. Although condemnation of many kinds, including direct denigration of President Putin, his administration, and the Orthodox Church, are not tolerated, especially on domestic social media platforms like VKontakte and Odnoklassniki, government-approved protests still occur and censors do not forestall all opposition voices, especially on international social media sites. This underscores that authoritarian vulnerability resides not merely in opposition perspectives or information, but in the collective action which said information may elicit.

### 2. *A Shared Domestic and International Objective: Cyber Sovereignty and Isolation*

In the company of a few other digital authoritarians, China and Russia lead the charge for the international recognition of physical and digital sovereignty. For example, controversial claims over territories like Crimea and the South China Sea are accompanied by assertions of sovereignty in cyberspace. In the context of global Internet governance, Russia and China share an agenda to place their domestic digital information environments under the umbrella of state sovereignty in both an infrastructural and normative legal sense. In addition to advocating for the norm of digital sovereignty in various international organizations or governing bodies (Nocetti 2015, 112), Russia and China construct domestic laws around the sovereignty of their digital space.

For a few decades, Russia and China have challenged U.S. and E.U. dominance in the global Internet domain both internationally and with domestic legislation. In its 2010 white paper on “Internet Administration,” China justifies the “sovereignization” of the Internet on grounds of cultural self-determination: “National situations and cultural traditions differ among countries, and so concern about Internet security also differs. Concerns about Internet security of different countries should be fully respected. We should seek common ground and reserve differences, promote development through exchanges, and jointly protect international Internet security" ("White Paper: The Internet in China"  2010).

In a similar vein, the Russian model of Internet governance strives for the sovereignty of the RuNet. According to the 2016 federal decree, one of the main goals of Russian information security is the "protection of the sovereignty of the Russian Federation in the information space through the implementation of independent policies aimed at realizing national interests in the information sphere," or in other words, "the development of a national system for managing the Russian segment of the Internet" (RF 2016). The isolation of domestic information, digital and non-digital, is a boon for authoritarian regimes. The ability to maintain dominance over a political narrative is only amplified when information is contained and isolated from potential foreign threats to governance.

Russia and China promote the norm of cyberspace sovereignty and seek legal recognition for this standard in both international and regional governing bodies. In order to challenge the status quo dominance of U.S.-created international Internet governing entities such as ICANN and the Internet Engineering Taskforce (IETF), Russia prefers working with other organizations it perceives as more sympathetic to its interests, including "the Shanghai Cooperation Organization (SCO), the Collective Security Treaty Organization (CSTO), and the BRICS grouping of Brazil, Russia, India, China and South Africa" (Nocetti 2015, 120). The SCO, whose member states consist of Russia, China, and all but one Central Asian Republic, highlights the growing importance of Sino-Russian cooperation in the sphere of information and communications technologies as well as Internet governance. Russia and China, along with a larger contingent of countries, have promoted documents that permit a more state-centric model of Internet governance. For example, in 2011 Russia, China, Tajikistan, and Uzbekistan introduced the International Code of Conduct for Information to the UN General Assembly, calling for UN involvement in the international Internet governance dialogue, with no mention of a multi-stakeholder approach that would check government powers (Nocetti 2015, 123). Nocetti calls Russia's international posturing an attempt at "de-Americanizing the Internet" (Nocetti 2015, 120). Russia and China both advocate vocally for more protectionist Internet policies in the main Internet forums, the International Telecommunications Union (ITU), ICANN, and the Internet Governance Forum (IGF) (Nocetti 2015, 121).

With the help of private surveillance technology companies, China in particular has skillfully engaged in a hard and soft power strategy to increase the global adoption of protectionist Internet policies.[21] One firm, Xiamen Meiya Pico, works alongside the federal cybersecurity agency, the Ministry of Public Security (MPS) to distribute Chinese digital security technologies to regional partners as part of the Belt and Road Initiative (Weber 2019). On its website, Xiamen Meiya Pico describes itself as "the expert in digital forensics and cybersecurity in China, mainly provides solutions and services for law-enforcement and government organizations all over the world" and for the last 12 years has been approved as a 'National Cyber Police Training Center' by the MPS. Representatives from the U.K., CIS countries, Saudi Arabia, Russia, and as many as 45 others have attended these trainings in digital forensics and other cybersecurity techniques (Weber 2019).[22] Some observers view China's attempt to export its digital management

[21] Joseph Nye defines soft power as an alternative to traditional, coercive hard power. Soft power "tends to be associated with intangible power resources such as culture, ideology, and institutions" (Nye 1990).

[22] For a complete list of countries, see the map on Meiya Pico's website (https://www.meiyapico.com/about-us_d14), or Weber 2019 p. 19.

technologies as an extension of digital authoritarianism in direct opposition to the Western-skewed international Internet governance order.

### Points of Divergence:

As the paramount and perhaps most extreme example of authoritarian interference in the Internet, China has come to represent most observers' understanding of digital authoritarianism, despite the fact that authoritarian Internet control is not monolithic. The Russian and Chinese Internet governance models differ most notably in degree of infrastructural centralization as well as extent and pace of change in governance.

#### 1. *Degree of Network-Infrastructural Centralization*

One of the most significant differences between the Chinese and Russian models is the degree of technological centralization of each system. Whereas the Chinese model 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). On the one hand, the Chinese network includes centralized "chokepoints" for more widespread Internet control (Ramesh, et al. 2020, 1). These chokepoints are physical sections of the network infrastructure in which the state restricts data flow and can centrally enforce access prohibitions. In contrast, Russia lacks these chokepoints and relies more on ISPs to block or filter content, sites, or users based on federally-maintained blocklists that must be frequently updated by the state and carried out by ISPs. In Russia, the state's governance of the Internet relies on the successful cooptation of ISPs and other digital media platforms, whereas in China, the state itself possesses a greater degree of control over network infrastructure through central chokepoints and ownership of ISPs and other digital service proxies like domestic social media companies. In other words, the more centralized the network infrastructure of the country, the more concentrated the state's power over the digital realm, as it need not rely as heavily on mandatory ISP or proxy adherence to its regulations.

The degree of network infrastructure centralization in each country also determines the perceived 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). Due to the country-wide scope of censorship tools, it is unsurprising to know that Internet governance is standard across China's regions. While there is some evidence of inconsistency in the Chinese governance model, it much less apparent to an outside observer because "the effort the government puts into its censorship program is large, and highly professional" (King, et al. 2013, 5). In their study, King, et al. do note "some evidence" but indicate that such phenomena are difficult to study (King, et al. 2013, 5).

In contrast, the Russian model shows some stark points of inconsistency, such as in the application of legislation and the types of content filtered and blacklisted. Examples of inconsistent application of law in prosecutions, tension between regional judiciaries and executive, controls employed by different ISPs, and changes in mechanisms applied over time may indicate a lack of internal consensus or clear mandate. Putin's federal decree for the decriminalization of Article 282 of the Russian Criminal Code exemplifies the discord between the executive and regional levels of governance in Russia. Although there was a stark decrease in regional prosecutions under

Article 282 after the federal decree indicating a concentration of power in the executive, regional differences in application of the law and extremity of punishment still varies widely, for example when it comes to the prosecution of individuals like Victor Krasnov accused of “offending religious believers”. It remains unclear how and why some individuals are prosecuted for digital content deemed illegal while others are spared. The outcomes of trials also vary depending on the regional court bringing the case and the perceived threat that the specific individual poses to the state’s status quo. Whereas the detainment and prosecution of Oksana Pokhodun—a perceived affiliate of a radical opposition group—under the incitement of extremism article (Art. 282) can be understood as a straightforward attempt to neutralize activism, the legal actions taken against the unaffiliated citizen Maria Montuznaya under the same Article is more difficult to comprehend. This inconsistent prosecution record could also be a tool to intimate Internet users into tailoring digital behavior to state-approved standards. Inconsistency also arises in the types and frequencies of content removals. An analysis of the federal extremism blacklist yields a somewhat opaque picture of blacklisting standards. The decentralized nature of the system, in which content removal or filtering must occur at the ISP level, also contributes to inconsistencies in governance, as each ISP ultimately employs different blocking software and hardware tools which produce different censorship results depending on the location.

Although decentralized Internet governance models were long considered less powerful or effective than centralized systems such as in China or Iran, recent scholarship undermines this conventional wisdom. Through an investigation of Russian Internet traffic, Ramesh et al. explain that “large-scale censorship can be achieved in decentralized networks through inexpensive commodity equipment.” (Ramesh, et al. 2020, 1). While neither China nor Russia publish total expenditure figures for their Internet governance systems, it is widely understood that Russia’s model allows the state to offset surveillance and filtration software and hardware costs onto proxies, including ISPs. The less centralized or predictable model provides Russia with the notable advantage of more flexible, albeit somewhat less extensive, governance of the Internet and a lower cost of infrastructure maintenance as other actors, like ISPs, bear many of the costs of surveillance and information technologies (Polyakova and Meserole 2019). In fact, Russia's decentralized infrastructure may even serve to deter evasion of digital governance. As Ramesh et al. note, "in countries like Russia, decentralized information control adds another layer of complexity: a circumvention tool that works for one user may not work for others" (Ramesh, et al. 2020, 2). In other words, because each ISP uses difference blocking tools, such as TCP-layer blocking, application-layer blocking facilitated by deep packet inspection, and DNS manipulation to block the same federally-mandated content, there is a level of inconsistency and randomness in the Russian model that makes it hard to circumvent in a straightforward and consistent way. For these reasons, many CIS countries have adopted the Russian model of digital governance.

While the Russian model is currently decentralized in nature, it may not remain this way forever; the passage of the 2019 Internet isolation (sovereignty) law marks a preliminary yet considerable step towards a more centralized and significantly more costly model. The full realization of a sovereign RuNet would require an overhaul of Russia's present digital infrastructure, which some doubt is feasible or practical given the extent of Russia's pre-existing network infrastructure.

### 2. *Extent and Pace of Change in Governance*

In addition to degree of network centralization, the Russian and Chinese Internet governance models vary considerably in extent and pace of governance. In the absence of reliable, directly comparable statistics such as the number of blacklisted or filtered sites in China versus Russia, Freedom House International's Freedom on the Net (FOTN) rankings, tabulated by rating each state's "obstacles to access," "limits on content," and "violations of user rights," offer an insight into the different degrees of Internet governance by country. According to the 2019 report, Russia's Freedom on the Net score of 31 is still significantly less extreme than China's 10 (0=not free, 100= free) (Shabaz and Funk 2019). In addition, whereas China was the world's worst abuser of Internet freedoms in 2019, Russia ranks at number 11 (with 13 other countries in between, some tied) (Shabaz and Funk 2019).

Although Russia remains a less extreme digital authoritarian than China according to Freedom House's calculations and conventional wisdom, the pace with which its Internet governance model has evolved and expanded in recent years, especially since the Bolotnaya protests in 2011, is noteworthy. A compilation of Freedom House's Freedom on the Net Reports from 2009-2018[23] shows that since 2009 Russia's Internet governance has become significantly more authoritarian. Russia's "freedom" score increased by 19 points out of 100 (from 49 "partly free" to 67 "not free") in ten years, compared to China's more modest 9 point rise (from 79 to 88 "not free") (Shabaz and Funk 2019).

Another way we can observe Russia's more recent, rapid Internet governance pace is by comparing legislation adopted at each level of network governance in both Russia and China. In the table below, one type of law is chosen to represent each level of network governance in order to compare the timing of implementation in Russia versus China. Internet isolation is the best representation of governance at the network level, because it allows states to use an Internet "kill

[23] From 2009-2018 the FOTN scoring scale was 0= more democratic, 100= less democratic. The scale inverted in 2019 where high scores reflected more democratic systems and low scores the opposite.

switch" which is technologically advanced and highly centralized when fully realized. Blacklist creation is a good indicator of sub-network governance. The registration and legal liability placed on ISPs as well as blogger registration laws serve as the comparative legal standards across countries at the proxy and individual levels of governance. These laws are by no means exhaustive and merely represent a common standard by which to compare the Internet governance timelines of Russia and China. Some of these laws have since been updated, amended, or replaced in both the Russian and Chinese legislative systems.

***Table 1. Comparative Timeline of Internet Laws in Russia and China***

| **Level of Network Governance** | **Full-Network** | **Sub-Network** | **Proxies** | **Network-Nodes** |
|---|---|---|---|---|
| Type of Law | Internet isolation | Blacklist creation | Official ISP registration/liability | Blogger registration |
| China | 1996 | 1996 | 2000 | 2005 |
| Russia | 2019* | 2012 | 2006 | 2014 |

*Full Russian network isolation has not yet been realized.

(Sources: RSF 2005, HRW 2017, King, et al. 2013, Creemers 2016)

Table 1 demonstrates that at each level of Internet governance, China implemented its own version of the laws in question earlier than Russia. 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. Perhaps of particular importance is the fact that Russia's attempts to govern the upper levels of the Internet came decades later than China's, but its proxy laws were not as delayed. While China introduced legislation to govern the full network in 1996, analogous legislation was only introduced in Russia with the 2019 Internet Isolation Law.

Russia's recent emphasis on governance of the upper levels of the network also marks an alarming trend towards less visible, more technical control mechanisms. The table below is aggregated from yearly reports by AGORA International Rights Group and Roskomsvoboda and depicts the complex changes in Russian Internet governance mechanisms between 2015 and 2019 (AGORA and Roskomsvoboda 2020). Some of the shifts in regulation mechanisms utilized in the last four years are striking, pointing to the lack of consistent governance; the number of "regulatory proposals," including legal amendments or new bills has varied from year to year with a high of 114 in 2017. Whereas total non-digital mechanisms have oscillated over time, digital restrictions have increased exponentially since 2015. The number of "Internet access restrictions" and "prohibitions of information by government entities" surged by over 9,000 and 3,000%, respectively since 2016. Meanwhile, after an increase in 2015, instances of "administrative pressure" and "civil suits" decreased by over 1,200 and 53%, respectively since 2016.

***Table 2. Digital and Non-Digital Internet Controls in Russia 2015-2019***

| Restriction Category | Restriction Mechanism | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|
| **Non-Digital (legislative, judicial, extra-judicial)** | Regulatory proposals (Legislative) | 48 | 97 | 114 | 82 | 62 |
| | Criminal investigation/ deprivation of freedom | 202/18 | 298/32 | 411/48 | 384/45 | 200/38 |
| | Pressures on IT-companies | N/A | N/A | N/A | N/A | 12 |
| | Administrative pressure | 5,073 | 53,004 | 22,523 | 4,402 | 3,917 |
| | Civil suits | 49 | 170 | 39 | 58 | 79 |
| | ***Total Non-Digital Restrictions*** | ***5,418*** | ***53,651*** | ***23,201*** | ***5,030*** | ***4,365*** |
| **Digital** | Internet access restriction | 1,721 | 35,019 | 88,832 | 488,609 | 161,490 |
| | Blacklisting by government entities | 7,300 | 24,000 | 2,196 | 161,171 | 272,785 |
| | Cyberattacks | 30 | 122 | 15 | 20 | 32 |
| | Government shutdowns | N/A | N/A | N/A | N/A | 8 |
| | ***Total Digital Restrictions*** | ***9,051*** | ***59,141*** | ***91,043*** | ***649,800*** | ***434,315*** |
| ***ALL*** | ***TOTAL*** | ***14,469*** | ***112,792*** | ***114,244*** | ***654,830*** | ***438,680*** |

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

The data indicates a trend towards greater emphasis on 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. Whereas the number of non-digital mechanisms decreased by 19% from 2015 to 2019, the number of digital mechanisms of Internet control increased by just shy of 4,700% in the same period. Furthermore, the total number of restrictions (digital and non-digital) to the cyber information environment increased by almost 3,000% from 2015 to 2019. In the explanatory section below I provide two hypotheses for the trend towards more high level, technologically advanced and less visible mechanisms: the transition of Russia into a more advanced stage of digital governance development or as a response to inherent political constraints to publicly visible Internet governance.

### What Explains these Differences in Internet Governance?

Analysis of the differences between Russian and Chinese Internet governance expands the study of digital authoritarianism by accounting for the variations within this broad designation of regimes. This section enumerates two theories to explain the differences in Internet governance models. First, differences in Internet governance models may result from unique digital development trajectories. Second, differences between models may arise from variations in each regime's political and legal institutions. These theories are not mutually exclusive; both hypotheses can be used to underscore that differences in the Russian and Chinese Internet governance models will persist. On the other hand, the developmental path theory could also be used to argue that present differences in Internet governance models could diminish over time if Russia, like China, were to increase its technological capacity and pay high monetary and political costs. There has been some speculation about future Russian convergence on the Chinese model (Deibert and Rohozinski 2010; Roberts 2018a). However, I will use both the digital development trajectory and varieties of authoritarianism theory to demonstrate that there is more empirical evidence in support of the persistent differences argument.

#### 1. *Distinct Development Trajectories*

For decades, the People's Republic of China (PRC) and the Soviet Union (USSR) shared Marxist-Leninism as the ideological pretext for political rule. Although the official relationship between the PRC and USSR was marked by oscillations between non-aggression pacts and invasions, the two share both a Communist past and extensive transition from socialist to capitalist economies in the last few decades of the twenty-first century. The development trajectories of the PRC and USSR are not coterminous but rather differ in a few significant ways which shaped their unique Internet governance regimes. First, legal oversight of the Internet began significantly earlier in China than in Russia. Second, early domestic technological innovation was more influential in forming the domestic cyberspace infrastructure and user experience in China than in Russia. However, despite these differences in governance timelines, the recent Russian Internet governance focus on higher level, more technologically advanced mechanisms suggests a trend towards more similar strategies of governance.

During the Soviet Union, the state curtailed some technological advances, fearing their potentially destabilizing and democratizing effects. However, this is not to say that Russia lacked the technological capability to surveil and police the Internet. Although the USSR possessed the state-of-the-art SORM surveillance technology since the 1980s, its broader Internet governance model evolved rather slowly until 2011, when political mobilization against Putin's reelection raised the importance of more aggressive digital governance.

Russia's foray into the worldwide web came later than the U.S. due to the KGB's tight grip over the penetration of cutting-edge technology, most of which was emerging from the West. Fear of the ostensible democratizing effect of some technological advances like personal computers motivated the security service's reticence to embrace such technologies. The tide began to turn when in 1990 a KGB research institute exchanged emails with a University in Helsinki, Finland and registered the first Soviet domain ".su" the same year (Soldatov and Borogan 2017, 30). Perhaps a more groundbreaking change came not from within the state apparatus, but from two colleagues, one American and one Russian academic. By creating a shell company, "Computerland USSR," friends Ed Fredkin and Yevgeny Velikhov gifted the first personal computers for civilian use to the Russian Academy of Sciences, hoping to "jailbreak the prison of information" that the USSR represented to so many technology advocates and critics (Soldatov and Borogan 2017, 23). However, by its dissolution in 1991, the Soviet Union still had the "lowest teledensity of any industrialized country," (Deibert and Rohozinski 2010, 18). The policies of *glasnost, perestroika* and *demokratizatsiya* (openness, economic restructuring, and democratization) appeared to promise more democratic institutions, including digital user freedoms as more technology was permitted in the territories of the former Soviet Union. In addition to Western technology, foreign Internet services and social media platforms became a part of many Russians' lives Internet penetration spread across the country.

In comparison to the Russia case, top PRC officials like Premier Zhao Zhiyang recognized the potential political boon of the Internet and related digital technologies. As early as 1983, Premier Zhao posited that "The new technological revolution or information revolution… may help China skip over some of the stages of which have been experienced by other developing countries" (Polyakova and Meserole 2019). While China was beginning to establish the framework for the "Great Firewall," in the mid to late 1990s, Russia's leadership under Putin was said to have little understanding of the Internet and only a nascent interest in governing it (Soldatov 2017). By the time Putin convened one of the first meetings of digital platform executives and other Internet and RuNet- specific specialists in 1999, then-President of China Jiang Zemin had already passed the first Internet governance legislation to establish the now infamous Firewall (Лошак 2019).[24]

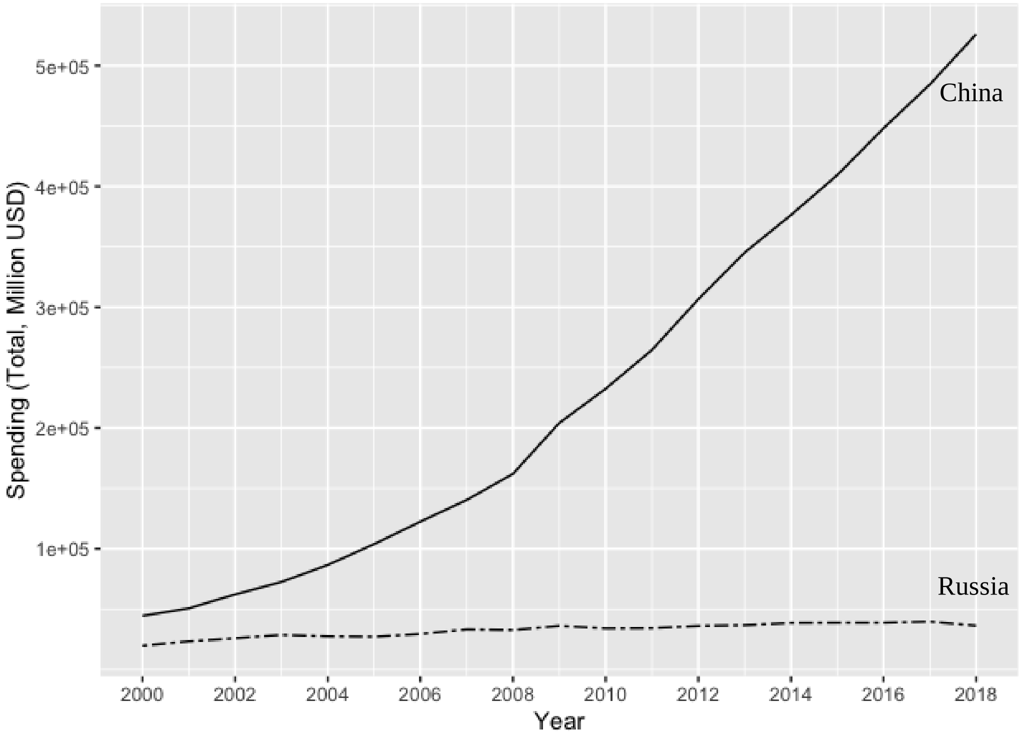
Under Premier Zhao and his successors, China established itself as one of the leaders in the Information and Communications Technology (ICT) sector. Since then, China has positioned itself as a front-runner in 5G technologies, artificial intelligence (AI), and machine learning (ML) (Henry-Nickie, et al. 2019). Even today, China's global ICT exports greatly outstrip Russia's. According to the OECD, Russia's ICT goods exports totaled $1.634 billion compared to China's approximately $550 billion (OECD 2020b). In keeping with China's soft power strategy highlighted in the sovereignty section above, several Chinese companies—Hikvision, ZTE, Huawei, and Dahua—provide 63 countries with AI surveillance technology, 36 of which are signatories to China's Belt and Road Initiative (Feldstein 2019).

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 total GDP—on R&D, Russia spent just shy of 1% or $36.4 billion (OECD 2020a). Perhaps of greater note is the upward trend in Chinese R&D since 2000 compared to the relative flat line of Russian investment. China's early dominance in the ICT sector gave rise to domestic surveillance technologies, Internet services, and social media platforms, ensuring the state's ability to corner the digital information environment. It has been posited that Chinese policymakers believe that "to be truly secure, China must achieve technological self-sufficiency," an attainable goal with such an extensive R&D budget (Segal 2018). It is important to note,

[24] For more information about the formation and evolution of RuNet in the 1990s to present, see Russian language documentary series, "Холивар. История Рунета" on Настоящее Время. Available on YouTube for free. https://www.currenttime.tv/a/runet/30107847.html

however, that the Chinese government faces a long-term dilemma of striking a balance between encouraging economic and technological innovation while still remaining in control of these tools and the information environment. In comparison, Russia neither fostered a cutting-edge domestic technology sector nor create a more insular, state-aligned domestic digital environment in the early days of Internet development. Although Russia has lagged behind China in domestic ICT manufacturing and exports, a recent shift has taken place in response to global sanctions and growing fears of dependence on foreign critical software and hardware technologies. The 2015 federal decree to establish greater domestic technological autonomy suggests that, although Russia has historically invested less in its domestic ICT sector, it may be beginning to trend in the same governance direction as China (Stadnik 2019, 3-4).

***Figure 6. Gross Domestic Spending on R&D in Russia and China 2000-2018***



(OECD, Gross domestic spending on R&D (indicator). doi: 10.1787/d8b068b4-en)

For many of the reasons highlighted above, Russia has been widely perceived as playing catch up to China and other technologically advanced nations in legislation and military control over the cyber realm (Deibert and Rohozinski 2010; Soldatov and Borogan 2017). In fact, the Russian Internet was considered by many domestic and foreign interlocutors as fairly free in the late 1990s through the 2000s. The Russian inventor of VKontakte, Pavel Durov, once recalled, “The best thing about Russia during that time was the Internet sphere was completely not regulated. In some ways, it was more liberal than the United States” (Griffiths 2019, 262). However, after the rise of protests in the Russian Federation, in the ‘color revolutions’ of its near-abroad, and in the more distant Middle East, in 2011, the Russian state made a considerable effort to place the Internet under its control. Soldatov argues that Russia’s relatively late arrival to Internet governance changed the way it could evolve 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 2017, 56).

The Chinese digital space has been occupied by countless domestic alternatives to Western social media platforms and information providers for decades. Some citizens admit that they do not yearn for access to Western alternatives because they have long relied on Chinese analogs (Yuan 2018). In contrast, Russian netizens have enjoyed decades of access to more varied and international Internet resources and services. In other words, the Russian system of Internet governance did not evolve with the development and increased usership of the Internet, as did China’s, but rather in response to its proliferation and the ever-increasing threat it posed decades later. I argue that because Russia’s Internet governance model flourished much later hence in conjunction with international Internet services and platforms that are less accountable to the state, eventual convergence with the Chinese model is unlikely.

Currently, the Russian Internet governance model can be described as more reactive and ad hoc than China's (Polyakova and Meserole 2019). However, Russia's alarming trend from publicly visible to more technologically advanced mechanisms of Internet governance represents an important evolution of the model. The increased prioritization of less visible mechanisms of governance (where legislation is more publicly visible than, say, complex deep packet inspection systems) allows the state to increase Internet restrictions covertly, so as to avoid spark criticism from its domestic netizens who are accustomed to a greater degree of online freedom (MacKinnon 2011). In the varieties of authoritarianism section to come I will argue that, although this Russian trend mirrors some Chinese Internet governance strategies, the differences between Russian and Chinese political systems entail persistent differences in constraints to Internet governance which prevent eventual convergence of the two models. For regimes with more democratic checks and balances like Russia, public opinion, civil disobedience, and circumvention of digital governance could prevent eventual convergence with the more centralized one-party Chinese state model.

### 2. *Varieties of Authoritarianism*

A state's regime type can shape its Internet governance strategy in crucial ways. Authoritarian regimes all struggle to encourage innovation while still presiding over the domestic information environment and ensuring political stability, but these challenges are manifested differently depending on the unique political institutions and constraints of each system. Decades of scholarship have contributed to a more nuanced view of authoritarian regimes in which political systems are considered in light of their unique restraints and institutions (Chang and Golden 2010;

Diamond 2002; Levitsky and Way 2002; Ottaway 2003; Schedler 2002). It is also crucial to consider how legitimation strategies differ across regimes. An analysis of the Russian and Chinese political systems through the lens of varieties of authoritarianism is one essential component of accounting for differences in their Internet governance models. Russia and China have unique constraints and opportunities for concentration of political power broadly and in relation to Internet governance. Whereas Russia's regime is more institutionally decentralized and faces greater checks and balances, power in centrally concentrated in China's one-party state and as such the party and state face fewer institutional and public constraints to Internet governance. The persistent differences in regime structure and accountability prevent the eventual convergence of the Russian and Chinese Internet governance models.

According to its 1993 constitution, the Russian Federation functions as a democratic, federal regime with three separate branches of government (legislative, executive, and judiciary). Its bicameral, multi-party parliamentary system includes president Vladimir Putin's dominant United Russia Party in addition to several others including the Communist Party, the Liberal Democratic Party, and A Just Russia. The dual-executive includes a president and prime minister who possess a great degree of power in the government. Although the president is elected, elections have been consistently found by international and domestic Russian NGOs to breach democratic standards (Dewan and Gigova 2018). In the 2018 presidential election, Golos documented instances of "carousel" voting, voter intimidation, ballot-stuffing and an overall lack of transparency (DFRLab 2018). The disproportionate concentration of political power in the executive became readily apparent when from 2008-2012 Putin and his prime minister operated a "tandemocracy" in which they swapped positions, thereby allowing Putin to run again for president in 2012 and make constitutional changes to the presidential term limit. Another more recent example of executive power was Putin's unilateral decree in January 2020 to overhaul the government, appoint a new prime minister, and increase the power of the State Council (Tétrault-Farber 2020).

In many ways and for several decades the Russian system has been organized around Putin as an individual leader for the past twenty years (Brechenmacher 2017; Levada 2017). It is possible to characterize President Vladimir Vladimirovich Putin's rule as "personalistic," as he is in many ways "the source of authority" and power within the Russian system may sometimes "depend on access to, closeness to, dependence on, and support from the leader" (Huntington 2009, 33). The "cult of personality" that Putin has constructed by posing for various, widely-circulated pictures which highlight his athleticism, masculinity, vigor, sobriety, and Orthodox faith is evidence of this phenomenon. When asked in 2019 whether they would vote for Putin to remain in office after his term expires in 2024, as many as 54% of Russians answered in the affirmative, with 43% of respondents indicating that "People don't see who else they could rely on"— better the devil you know than the devil you don't (Levada 2019).  Given that Putin's public image is a crucial source of regime legitimacy in Russia, the protection of the public narrative is a top priority in the Russian legal environment. The political personalism of the Russian system explains the legislative and prosecutorial emphasis on punishing direct criticism of Putin and his administration.

Despite some authoritarian hallmarks, the Russian political system does also possess inherent checks and balances. The degree of freedom enjoyed in civil society in the 1990s, although somewhat curtailed in recent years, included access to varied media sources beyond state television. Within the political hierarchy of the Russian Federation system, there is some regional and local-level autonomy, including gubernatorial elections. The local autonomy that regional representatives and courts have as well as the existence of some independent media sources (most located outside Russia but available to Russian citizens online) implies a greater amount of accountability and competition in the Russian system, and by the same token places unique restraints on Internet governance.

The Russian system can be best understood as "competitive authoritarianism," in which "formal democratic institutions are widely viewed as the principal means of obtaining and exercising political authority." However, Levitsky and Way emphasize that these regimes "violate those rules so often and to such an extent, however, that the regime fails to meet conventional minimum standards for democracy" and faces a greater degree of regime instability than more consolidated authoritarian regimes (Levitsky and Way 2002, 52).[25] In more competitive authoritarian political systems like Russia's one may wonder whether inconsistency, such as can be seen in Russia's Internet governance model, is a result of the greater transparency and internal discord that is characteristic of more democratic or pluralistic institutions.

Given the more competitive nature of the Russian regime, Russian Internet users have enjoyed access to a wider variety of information and Internet services, including the New York Times, Google, and social media platforms that have been notoriously blocked in China for decades. Not to mention, overall Internet penetration is significantly higher in Russia than in China, indicating a heightened digital governance challenge for the former. In the Russian model, citizens can threaten the state through acts of social defiance, thereby placing constraints on the

[25] Levitsky and Way define "modern democratic regimes" as those which meet the following minimum criteria: "1) Executives and legislatures are chosen through elections that are open, free, and fair; 2) virtually all adults possess the right to vote; 3) political rights and civil liberties, including freedom of the press, freedom of association, and freedom to criticize the government without reprisal, are broadly protected; and 4) elected authorities possess real authority to govern, in that they are not subject to the tutelary control of military or clerical leaders. Although even fully democratic regimes may at times violate one or more of these criteria, such violations are not broad or systematic enough to seriously impede democratic challenges to incumbent governments. In other words, they do not fundamentally alter the playing field between government and opposition" (Levitsky and Way 2002 53).

degree of state-sponsored digital censorship. As Roberts puts it, “The constraints political entities face, the goals of the government, and the technological environment affect the capability of authorities to use each mechanism of censorship and the ways in which citizens will react to censorship” (Roberts 2018b). Perhaps the trend in Russia towards less visible mechanisms of governance, namely technologically advanced tools of surveillance and blocking, reflects the constraints on the state’s Internet governance model. By relying on more covert tools of governance, the Russian state could avoid the dissent from watchdogs and the general public which visible censorship often elicits. A state like Russia may impose stricter penalties for criticism of the government, its policies, and state-approved interpretation of history out of a greater fear of losing regime durability. For states with more concentrated power in the executive or one-party system, the likelihood of insurrection and regime change is lower. The complex and overlapping structure of Internet governance institutions in the Russian system is a reflection of a more competitive political system as compared to China’s one-party, more politically centralized model.

China’s political structure is notably less democratic and therefore faces fewer constraints in the realm of Internet governance. The one-party system in the People’s Republic of China (PRC) is “premised on unitary leadership” in which the party remains in power by promoting a single ideology (Shangli and Fewsmith 2014, 158). In other words, in one-party states, “the ideology of the party define[s] the identity of the state” (Huntington 2009, 38). Huntington argues that by likening “democratic opposition to communism” to treason against the state, China exemplifies the one-party state model (Huntington 2009, 38). The “unitary leadership” which Shangli and Fewsmith ascribe to the PRC’s political system as a whole is also applicable to the Internet governance bodies; the political messaging and governance activities appear, at least publicly, to promote a singular agenda.

Whereas one of the Russian state's sources of legitimacy is the personalism of Putin's leadership, the Chinese state relies on ideology as a source of legitimacy. It could be argued that the Chinese state has enjoyed a renewed emphasis on ideology—a mixture of communism, Leninism, Maoism and nationalism—in recent years under President Xi Jinping (Zhao 2016, 1171). On numerous occasions and, notably, in 2013, Xi has underscored the importance of ideology to the Communist Party's survival and influence within China, characterizing this emphasis on ideology as "the life and death of the party, the long-term stability of the country, and the cohesion of the nation" (Zhao 2016, 1172). His "national strategic goal" to safeguard the "Chinese Dream," a "revival of prosperity, unity, and strength," are underscored in Internet governance strategies (Kolton 2017, 126). According to Pei, the CCP's survival stems from three additional factors: "refined repression, economic statism, and political cooptation," the same strategic underpinnings of China's Internet governance regime (Pei 2012, 32).

The President of the PRC is elected not by popular vote but by a vote in the National People's Congress, comprised of the elite members of the Chinese Communist Party (CCP). While there is a degree of regional autonomy, originating first in the mid 1980s, the CCP is the dominant force in the entire political system and exists in a position of power above all other governing bodies (Fukuyama 2016, 384; Guangbin and White 2014; Keping 2014, 53). As several scholars put it, "the CCP has a leading position in China's decision-making system. It does not parallel, but rather leads, all other decision-making bodies. Every state organ performs its duties under the CCP's direct leadership, which is accomplished mainly by drawing up legislation, itineraries, guidelines, and policies" (Guanghui and Lampton 2014, 345).

As a more extreme example of authoritarian governance, the Chinese political system lacks "institutions of restraint," which provide a check on executive or top-down power (Fukuyama

2016, 385). For example, the recent "clean-government system," intended to decrease the amount of corruption in the CCP, lacks accountability measures for those in positions of heightened leadership (Zengke and Manion 2014, 374). Moreover, there exists no independent judiciary to hold the CCP to account. The Party's Disciplinary Committee, while nominally responsible for monitoring CCP transgressions and abuses of power, does no such thing in practice (Fukuyama 2016, 386).

This is not to say that the PRC faces no constraints to its digital governance regime. Like all authoritarian regimes, China is subject to threats to its survival (Pei 2012, 33). However, since the early days of the worldwide web, the Chinese state has made a concerted effort to govern the digital information environment, inherently shaping the experiences and expectations of its citizens according to its own standards. Because there is less competition in the Chinese political system than in its Russian counterpart, "information gaps," in which the state controls what information its citizens can access, are more common, a hallmark of more extreme, state-dominated governance of the digital information environment (MacKinnon 2011, 33; Zhao 2016, 1192). One example of this growing information gap is the coming of age of a generation of young adults in China with little to no understanding of Facebook, Twitter, Instagram, and other non-domestic social media platforms (Yuan 2018).

Mackinnon argues that China's Internet governance system can be best understood as "networked authoritarianism," in which "the single ruling party remains in control while a wide range of conversations about the country's problems nonetheless occurs on websites and social-networking services," providing some opportunities for criticism but with serious penalties imposed for online behavior deemed threatening (MacKinnon 2011, 33). Moreover, in the networked authoritarian state "there is no guarantee of individual rights and freedoms. Those whom the rulers see as threats are jailed; truly competitive, free, and fair elections are not held; and the courts and the legal system are tools of the ruling party" (MacKinnon 2011, 33).

Given that the Russian political system is more competitive than its Chinese counterpart, I argue that there will always be more constraints placed on the Russian government's governance of the Internet as compared to China's. For example, in the future it would be extremely difficult for the Russian state to pursue a China-inspired policy of blocking international search engines like Google and social media platforms such as Facebook. A policy such as this would require prior consultation with a variety of domestic governance institutions, and even if it passed through the necessary legislative bodies, could very well elicit negative reactions from Russian citizens who are accustomed to these international Internet services. Whereas the Chinese state is in a position to propose and rubber-stamp a new cybersecurity policy, the Russian system is considerably more decentralized in its political administration, making such a sweeping change near impossible in current conditions. In addition to persistent differences in political structures and institutional constraints, I argue that the varied digital development trajectories of Russia and China in the early days of the Internet prevent eventual convergence of the two Internet governance models.

# CONCLUSION

Digital authoritarianism poses a threat not just to domestic citizens but to the global Internet infrastructure and users around the world. To thoroughly assess digital governance mechanisms at authoritarian and other states' disposal, I proposed a new analytical framework which conceptualizes Internet governance as a series of mechanisms utilized at descending levels, from the full-network to individual-level of Internet governance. This approach 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 also those which are more technologically advanced and surreptitious (such as a variety of blacklisting and filtration tools and full isolation). Analysis of China and Russia using this analytical framework reveals several notable differences in the models: the relative degree of centralization in network infrastructure and the extent and pace of change in governance over time.

Despite the fact that Internet governance is a growing global phenomenon, scholarship on digital authoritarianism and Internet governance has not fully considered how varieties of authoritarianism and development trajectories impact a state's constraints and opportunities for management of its digital information environment. I argue that in the case of Russia and China, persistent differences in both the development of their digital information environments and political structures prevent the eventual convergence of the two Internet governance models. The trend towards more invisible, technologically advanced mechanisms of Internet governance in Russia is emblematic of a global phenomenon that endangers domestic citizens' access and contribution to the digital IE. The expansion of Chinese Internet governance is tempered mainly by the goal of encouraging economic supremacy in the ICT and other sectors. Domestic Internet users in Russia, China, and other digital authoritarian states are facing increasing legal and social penalties as well as restrictions on digital behavior. The list of targeted netizens highlighted in this paper will only increase as states become emboldened to govern their "sovereign" digital territories.

Moreover, the sovereignty or balkanization of domestic Internet segments threatens the inter-connectivity that the worldwide web is meant to provide. International demands by Russia and China for recognition of the digital realm as an extension of a state's territory threatens the U.S. and Western-centric status quo of the Internet as a space for global interconnectedness. Russian and Chinese co-led efforts to create a new global cybercrime treaty at the U.N. is one of the most recent manifestations of this geopolitical contest (Nakashima 2019). Rising digital authoritarian challengers seek to demonstrate the perceived hypocrisy of many Western states like the U.S. whose legal frameworks and surveillance systems make them anything but paragons of Internet or digital freedom (Nocetti 2015). Many scholars fear that Russian and Chinese efforts will lead to the eventual balkanization or fragmentation of the Internet.

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 U.S. incorporated social media companies to store data in local servers under domestic surveillance potentially jeopardizes the privacy of millions of Internet users. Most Internet users are not even aware that their data is stored in other localities and could be subject to surveillance by foreign governments.

Lastly, studies have found that the Russian and Chinese Internet governance models have been exported to several other authoritarian systems. King et al. argue that "China, as a relatively rich and resilient authoritarian regime, with a sophisticated and effective censorship apparatus, is probably being watched closely by autocrats from around the world" (King, et al. 2013, 15). Polyakova and Meserole posit that "at least 18 countries currently use Chinese surveillance and monitoring systems, and at least 36 government have held Chinese-led trainings and seminars on 'new media' or 'information management'" (Deibert and Rohozinski 2010; Polyakova and Meserole 2019, 6). The Belt and Road Initiative, an extension of China's grand strategy, serves as a conduit through which its model is exported to regional partners (Polyakova and Meserole 2019, 5-6). Chinese companies like Meiya Pico, directly supported by the Ministry of Public Service (MPS) cybersecurity agency, have instructed over 50 seminars in surveillance technologies and methodology, including to audiences in the U.K., Russia, Iran, Pakistan, and most of the CIS countries (Weber 2019).

The Russian model, including SORM surveillance technologies and other mechanisms, has been exported to the likes of Belarus, Kazakhstan, and Kyrgyzstan. As Polyakova and Meserole underscore, all CIS countries besides Armenia have instituted aspects of the Russian Internet governance model (Deibert and Rohozinski 2010; Polyakova and Meserole 2019, 10). One scholar warns that "Russia's censorship architecture is a blueprint, and perhaps a forewarning of what and how national censorship policies could be implemented in many other countries that have similarly diverse ISP ecosystems to Russia's" (Ramesh, et al. 2020, 1). The Russian model poses an even greater threat to the global Internet because its decentralized control methods are more cost-effective and ad hoc and therefore can be instituted in various types of governance regimes in other locations. As Russian and Chinese digital governance models become more fine-tuned and successful, the "export risk" only increases.

As technology has become increasingly intertwined with human interaction and organization in the 21st century, many authoritarian states have adapted to neutralize the digital threat to regime durability. Another disturbing trend is that the distinction between democratic and authoritarian Internet governance has become blurred, as democracies and authoritarian regimes alike strive to govern their domestic Internet spaces (Roberts 2018c). Therefore, it is crucial for political scientists to continue studying Internet governance to study the implications of an increasingly surveilled and controlled digital world. In this vein, it is vital to study the infrastructures and risks associated with digital authoritarianism as the likes of Russia and China exports surveillance technologies and practices around the world. The global proliferation of surveillance technologies will provide states with a trove of data on netizens' opinions, fears, and motivations, enabling even more customized and clandestine censorship. Comparative studies of disparate regime types' Internet governance models have the potential to propel the interdisciplinary research field forward and raise public understanding of the increasing digital controls around the globe. Lastly, as Internet users, we should all strive to learn about the ways in which our rights and data are manipulated in the cyber domains of other, distant regimes in addition to our own.

# REFERENCES

Abbate, Janet. 2001. "Government, Business, and the Making of the Internet." *The Business History Review*. http://www.jstor.org/stable/3116559.

Arendt, Hannah. 1953. "The Origins of Totalitarianism: A Reply." *The Review of Politics* 15: 76-84.

"Artpodgotovka: Six Days to Destroy a Movement." *OpenDemocracy*. OVD-Info. 2017. https://www.opendemocracy.net/en/odr/six-days-to-destroy-movement/. (7 September, 2019).

"Authorities Declare War on Unregistered Websites and Blogs." *Reporters Without Borders Reports/Reporters Sans Frontièrs. 2005.*. https://rsf.org/en/news/authorities-declare-war-unregistered-websites-and-blogs. (5 April, 2020).

Barme, Geremie, and Sang Ye. "The Great Firewall of China." https://www.wired.com/1997/06/china-3/.

Baumgartner, Pete. 2019. "Curb Your Criticism? First Russian Fined for 'Disrespecting' Putin Doubles Down on Critique of President." *RFE/RL*. https://www.rferl.org/a/first-russian-fined-for-disrespecting-putin-doubles-down-on-critique-of-president/29903929.html. (25 April 2019).

Bissell, Benjamin. 2015. "What China's Anti-Terrorism Legislation Actually Says." Lawfare: 30 December. https://www.lawfareblog.com/what-chinas-anti-terrorism-legislation-actually-says. 2020.

Brancati, Dawn. 2014. "Democratic Authoritarianism: Origins and Effects." *Annual Review of Political Science*. https://doi.org/10.1146/annurev-polisci-052013-115248. (2014/05/11).

Brandom, Russell. "Samsung's Device Care App Is Sending Data Back to China — but It's Less Scary Than It Sounds." https://www.theverge.com/2020/1/8/21056629/samsung-galaxy-china-device-care-scanner-qihoo-360-privacy.

Brechenmacher, Saskia. 2017. "Delegitimization and Division in Russia." In *Civil Society Under Assault: Repression and Responses in Russia, Egypt, and Ethiopia*. Carnegie Endowment for International Peace: Carnegie Endowment for International Peace. 1-19.

Capoccia, Giovanni, and R. Daniel Kelemen. 2011. "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism." *World Politics*. https://www.cambridge.org/core/article/study-of-critical-junctures-theory-narrative-and-counterfactuals-in-historical-institutionalism/BAAE0860F1F641357C29C9AC72A54758. (2 September, 2019).

Chang, Eric, and Miriam A. Golden. 2010. "Sources of Corruption in Authoritarian Regimes." *Social Science Quarterly*. www.jstor.org/stable/42956520.

"Channels of Information." *Levada Center*. 2018. https://www.levada.ru/en/2018/10/12/channels-of-information/. (September 10, 2019).

Chen, Stephen. 2018. "China Takes Surveillance to New Heights with Flock of Robotic Doves, but Do They Come in Peace?" *South China Morning Post*. https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they. (20 April, 2020).

Cheung, Anne, and Zhao Yun. 2013. "An Overview of Internet Regulation in China." *University of Hong Kong Faculty of Law Research Papers*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2358247. (22 February, 2020).

Chi, Eunju. 2012. "The Chinese Government's Responses to Use of the Internet." *Asian Perspective*. http://www.jstor.org/stable/42704798. (2 February, 2020).

"China Blocks Websites, Internet Accounts in New Cleanup Campaign." *Reuters*. https://www.reuters.com/article/china-censorship/china-blocks-websites-Internet-accounts-in-new-cleanup-campaign-idUSL4N23J1RW. (27 March, 2020).

"China: Draconian Legal Interpretation Threatens Online Freedom." *Human Rights Watch*. 2013. https://www.hrw.org/news/2013/09/13/china-draconian-legal-interpretation-threatens-online-freedom. (15 April, 2020).

Cockerell, Isobell. 2019. "Inside China's Massive Surveillance Operation." *Wired*. https://www.wired.com/story/inside-chinas-massive-surveillance-operation/. (May 9).

Collier, David. 1979. *The New Authoritarianism in Latin America*: Princeton University Press.

Creemers, Rogier. 2016. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century." *Journal of Contemporary China*. (09/05).

Daucé, Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. 2020. "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia." *Laboratorium: Russian Review of Social Research*. http://www.soclabo.org/index.php/laboratorium/article/view/962. (01/13/20).

Deibert, Ronald J., and Masashi Crete-Nishihata. 2012. "Global Governance and the Spread of Cyberspace Controls." *Global Governance*. www.jstor.org/stable/23269961. (11 March, 2020).

Deibert, Ronald, and Rafal Rohozinski. 2010. "Control and Subversion in Russian Cyberspace." In *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, eds. John Palfrey and Jonathan Zittrain: The MIT Press.

"Department of Defense Strategy for Operations in the Information Environment." *Department of Defense*. 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf. (September 13, 2019).

Dewan, Angela, and Radina Gigova. 2018. "International Monitors Slam Russian Election as 'Overly Controlled'." *CNN*. https://www.cnn.com/2018/03/19/europe/russia-election-reaction-intl/index.html. (19 March, 2018).

Diamond, Larry. 2002. "Thinking About Hybrid Regimes." *Journal of Democracy* 13: 21-35.

"#Electionwatch: Voter Fraud in Russia." *Medium*. DFRLab. 2018. https://medium.com/dfrlab/electionwatch-voter-fraud-in-russia-4a0dc75c4fa8. (21 February, 2020).

Esarey, Ashley, and Xiao Qiang. 2011. "Digital Communication and Political Change in China." *International Journal of Communication*. https://www.semanticscholar.org/paper/Digital-Communication-and-Political-Change-in-China-Esarey-Xiao/32da4bb67c9825a3aa35e4ed417a265c3e7f5c5d. (29 April, 2020).

Faulconbridge, Guy. 2014. "Father of Web Tells Russia's Putin: Internet Is Not a 'Cia Project'." *Reuters*. https://www.reuters.com/article/us-web-russia-putin/father-of-web-tells-russias-putin-Internet-is-not-a-cia-project-idUSKBN0JP1E420141211. (29 December 2019).

Feldstein, Steven. 2019. "The Global Expansion of Ai Surveillance." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847. (September 17).

Fish, Steven M. 2018. "What Has Russia Become?" *Comparative Politics*. www.jstor.org/stable/26532689. (13 January, 2020).

"Freedom on the Net 2015." *Freedom on the Net Annual Reports*. Freedom House. 2014. https://freedomhouse.org/report/freedom-net/2015/russia. (10 March, 2020).

"Freedom on the Net 2018." *Freedom on the Net Annual Reports*. Freedom House. 2018. https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf. (February 4, 2020).

"Freedom on the Net 2019: China Country Report." *Freedom on the Net Annual Reports*. Freedom House. 2019a. https://www.freedomonthenet.org/explore-the-map?country=CHN&status[free]=free. (27 January, 2020).

"Freedom on the Net 2019: Russia Country Report." *Freedom on the Net Annual Reports*. Freedom House. 2019b. https://www.freedomonthenet.org/country/russia/freedom-on-the-net/2019. (6 January, 2020).

Fukuyama, Francis. 2016. "Reflections on Chinese Governance." *Journal of Chinese Governance* 1: 379-91.

Gandhi, Jennifer, and Adam Przeworski. 2007. "Authoritarian Institutions and the Survival of Autocrats." *Comparative Political Studies*. https://doi.org/10.1177/0010414007305817. (24 November, 2019).

Geddes, Barbara. 1999. "What Do We Know About Democratization after Twenty Years?" *Annual Review of Political Science*. https://www.annualreviews.org/doi/pdf/10.1146/annurev.polisci.2.1.115. (24 November, 2019).

Gerschewski, Johannes. 2013. "The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes." *Democratization*. https://doi.org/10.1080/13510347.2013.738860. (20 March, 2020).

Gorodissky and Partners. 2018. "Yarovaya Law and New Data Storage Requirements for Online Data Distributors." *Lexology Law Library*. https://www.lexology.com/library/detail.aspx?g=8029c37f-5a1c-4025-ac3f-8b3ede9c42e8. (29 December 2019).

Griffiths, James. 2019. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed Books.

Groot, Gerry. 2017. "Making the World Safe (for China)." In *Control,* eds. Jane Golley, Linda Jaivin and Luigi Tomba: ANU Press. 277-94.

"Gross Domestic Spending on R&D." ed. Organisation for Economic Co-operation and Development: 2020a. Organisation for Economic Co-operation and Development (OECD). https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

Guangbin, Yang, and Lynn White. 2014. "Decentralization and Central-Local Relations in Reform-Era China." In *China's Political Development*, eds. Kenneth Lieberthal, Cheng Li and Yu Keping, Chinese and American Perspectives: Brookings Institution Press. 254-81.

Guanghui, Zhou, and David M. Lampton. 2014. "Contemporary China's Decisionmaking System." In *China's Political Development*, eds. Kenneth Lieberthal, Cheng Li and Yu Keping, Chinese and American Perspectives: Brookings Institution Press. 340-65.

Haas, Benjamin. 2017. "Chinese Authorities Collecting DNA from All Residents of Xinjiang." *The Guardian*. https://www.theguardian.com/world/2017/dec/13/chinese-authorities-collecting-dna-residents-xinjiang. (20 April, 2020).

Henry-Nickie, Makada, Kwadwo Frimpong, and Hao Sun. 2019. "Trends in the Information Technology Sector." *Brookings Institution*. https://www.brookings.edu/research/trends-in-the-information-technology-sector/. (12 April, 2020).

Herold, David Kurt, and Peter Marolt. 2011. "Online Society in China : Creating, Celebrating, and Instrumentalising the Online Carnival." In *Taylor and Francis*. Hoboken: Taylor and Francis. http://grail.eblib.com.au/patron/FullRecord.aspx?p=683940. Accessed.

Howard, Philip N., Sheetal D. Agarwal, and Muzammil M.Hussain. 2011. "The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?" *Issues in Technology Innovation*. https://www.brookings.edu/wp-content/uploads/2016/06/10_dictators_digital_network.pdf. (October 11, 2019).

Huntington, Samuel P. 2009. "How Countries Democratize." *Political Science Quarterly*. www.jstor.org/stable/25655609. (24 March, 2020).

Iasiello, Emilio. 2017. "China's Cyber Initiatives Counter International Pressure." *Journal of Strategic Security*. http://www.jstor.org/stable/26466891. (20 September, 2019).

"ICT Goods Exports." ed. Organisation for Economic Co-operation and Development: 2020b. Organisation for Economic Co-operation and Development (OECD). https://data.oecd.org/ict/ict-goods-exports.htm#indicator-chart

"Internet Isolation Exercises to Take Place in Russia at Least Once Every Year." *Meduza*. 2019a. https://meduza.io/en/news/2019/10/21/Internet-isolation-exercises-to-take-place-in-russia-at-least-once-every-year. (29 December, 2019).

Jerit, Jennifer, Jason Barabas, and Toby Bolsen. 2006. "Citizens, Knowledge, and the Information Environment." *American Journal of Political Science*. http://www.jstor.org/stable/3694272. (9 September, 2019).

Kaylan, Melik. 2014. "Kremlin Values: Putin's Strategic Conservatism." *World Affairs*. www.jstor.org/stable/43555061. (13 January, 2020).

Kedzie, Christopher. 1997. "Communication and Democracy: Coincident Revolutions and the Emergent Dictators." https://www.rand.org/pubs/rgs_dissertations/RGSD127/sec2.html.

Keping, Y. U. 2014. "The People's Republic of China's Sixty Years of Political Development." *China's Political Development*. www.jstor.org/stable/10.7864/j.ctt6wpcbw.6. (26 February, 2020).

Kharpal, Arjun. 2019. "Everything You Need to Know About Wechat — China's Billion-User Messaging App." *CNBC*. https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html. (26 April, 2020).

King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *The American Political Science Review*. www.jstor.org/stable/43654017. (27 January, 2020).

Kolomychenko, Maria. 2018. "Russia Stifled Mobile Network During Protests: Document." *Reuters*. https://www.reuters.com/article/us-russia-protests-Internet/russia-stifled-mobile-network-during-protests-document-idUSKCN1NL1I6. (29 December 2019).

Kolton, Michael. 2017. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2: 119-54.

Kozkina, Anna. 2018. "«Сначала Картинки, А Потом Метро Взрывают». Медсестра-Активистка, Мемы И Статья 282 Ук." *Медиазона*. https://zona.media/article/2018/04/06/pokhodun. (September 11, 2019).

Krönke, Christoph, Michael W. Müller, Wenguang Yu, and Wei Tian. 2018a. "Introduction: Paradigms of Internet Regulation in the European Union and China." In *Paradigms of Internet Regulation in the European Union and China*, ed. Michael W. Müller Christoph Krönke, Wenguang Yu, Wei Tian. Baden-Baden: Nomos Verlagsgesellschaft. 15-31.

———. 2018b. *Paradigms of Internet Regulation in the European Union and China*. Vol. 13. Baden-Baden: Nomos Verlagsgesellschaft.

Lam, Willy Wo-Lap. 2013. "China: State Power Versus the Internet." In *Losing Control*, eds. Louise Williams and Roland Rich, Freedom of the Press in Asia: ANU Press. 37-57.

Laprad, Tatyana. 2017. "Ко Мне Вломились Шесть Человек." *Сибирь.Реалии*. https://www.sibreal.org/a/28800495.html. (10 September, 2019).

Laskai, Lorand. 2017. "'Nailing Jello to a Wall'." In *Control*, eds. Jane Golley, Linda Jaivin and Luigi Tomba: ANU Press. 191-208.

Lee, Melanie, Sabrina Mao, and Chris Buckley. 2012. "China Moves to Tame Microbloggers Amid Censorship Claims." https://www.reuters.com/article/us-china-microblogging/china-moves-to-tame-microbloggers-amid-censorship-claims-idUSBRE84S03T20120529. (10 March, 2020).

"Legal Provisions on Fighting Extremism: Russia." *Library of Congress*. https://www.loc.gov/law/help/fighting-extremism/russia.php. (September 23, 2019).

Levitsky, Steven, and Lucan Way. 2002. "The Rise of Competitive Authoritarianism." *Journal of Democracy* 13: 51-65.

Litvinova, Daria. 2016. "Like, Share, Convict: Russian Authorities Target Social Media Users." *The Moscow Times*. https://www.themoscowtimes.com/2016/03/10/like-share-convict-russian-authorities-target-social-media-users-a52114. (6 January, 2020).

Lu, Jiayin, and Yupei Zhao. 2018a. "Implicit and Explicit Control: Modeling the Effect of Internet Censorship on Political Protest in China." *International Journal of Communication* 12: 3294-316.

———. 2018b. "Implicit and Explicit Control: Modeling the Effect of Internet Censorship on Political Protest in China." *International journal of communication (Online)*: 3294+.

MacKinnon, Rebecca. 2011. "China's "Networked Authoritarianism"." *Journal of Democracy*. (15 February, 2020).

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald J. Deibert, and Vern Paxson. 2015. "An Analysis of China's "Great Cannon"." https://www.semanticscholar.org/paper/An-Analysis-of-China's-%22Great-Cannon%22-Marczak-Weaver/327803e2006777a1a914b5b4919c04c881fa3a4a. (22 February, 2020).

Maréchal, Nathalie. 2017. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *2017*. https://www.cogitatiopress.com/mediaandcommunication/article/view/808/808. (10 February, 2020).

Marsden, Christopher T. 2011. "Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace." Cambridge: Cambridge University Press. https://www.cambridge.org/core/books/Internet-coregulation/7179CDF556745BA2313666AEE0A60E70. Accessed.

McHale, John. 1973. "The Changing Information Environment: A Selective Topography." *Ekistics* 35: 321-28.

Miao, Weishan, Hongjun Zhu, and Zhangmin Chen. 2018. "Who's in Charge of Regulating the Internet in China: The History and Evolution of China's Internet Regulatory Agencies." *China Media Research*. https://go.gale.com/ps/anonymous id=GALE%7CA549658139&sid=googleScholar&v=2.1&it=r&linkaccess=fulltext&issn=1556889X&p=AONE&sw=w. (13 April, 2020).

Moscow Times. 2019. "Russia Moves to Grant Government the Power to Shut Down the Internet, Explained." *The Moscow Times*. https://www.themoscowtimes.com/2019/02/12/russia-moves-grant-government-power-shut-down-Internet-explained-a64470. (10 May, 2019).

Mueller, Milton L., and Ernest J. Wilson, III. 2010. "Information Revolution and Global Politics : Networks and States - the Global Politics of Internet Governance." Cambridge, UNITED STATES: MIT Press. http://ebookcentral.proquest.com/lib/bowdoin-ebooks/detail.action?docID=3339169. Accessed.

Müller, Michael W. 2018. "Mapping Paradigms of European Internet Regulation." In *Paradigms of Internet Regulation in the European Union and China*, ed. Michael W. Müller Christoph Krönke, Wenguang Yu, Wei Tian. Baden-Baden: Nomos Verlagsgesellschaft. 31-49.

Münkler, Laura. 2018. "Space as a Paradigm of Internet Regulation." In *Paradigms of Internet Regulation in the European Union and China*, ed. Michael W. Müller Christoph Krönke, Wenguang Yu, Wei Tian. Vol. 13. Baden-Baden: Nomos Verlagsgesellschaft. 139-58.

Nakashima, Ellen. 2019. "The U.S. Is Urging a No Vote on a Russian-Led U.N. Resolution Calling for a Global Cybercrime Treaty." *The Washington Post*. https://www.washingtonpost.com/national-security/the-us-is-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/b4895e76-075e-11ea-818c-fcc65139e8c2_story.html. (2 March, 2020).

Nathan, Andrew. 2003. "China's Changing of the Guard: Authoritarian Resilience." *Journal of Democracy*. (5 April, 2020).

Nocetti, Julien. 2015. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs*. https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2346.12189. (25 April, 2020).

Nye, Joseph S. 1990. "Soft Power." *Foreign Policy*. www.jstor.org/stable/1148580. (2 March, 2020).

"Online and on All Fronts: Russia’s Assault on Freedom of Expression." *Human Rights Watch*. 2017. https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression#e91d8a.

Ottaway, Marina. 2003. "Democracy Challenged: The Rise of Semi-Authoritarianism." Carnegie Endowment for International Peace. www.jstor.org/stable/j.ctt1mtz6c5. Accessed 28 February, 2020.

Pei, Minxin. 2012. "Is Ccp Rule Fragile or Resilient?" *Journal of Democracy*. (8 March, 2020).

Polumbaum, Judy. 2012. "Changing Media, Changing China." *Chinese Journal of Communication* 5: 355-59.

Polyakova, Alina, and Chris Meserole. 2019. "Exporting Digital Authoritarianism." https://www.brookings.edu/research/exporting-digital-authoritarianism/. (10 January, 2020).

Pommeranz, Will, and Kathleen Smith. 2018. "Kennan Cable No. 39: A Traditional State and a Modern Problem: Russia Rewrites Its Internet Extremism Laws." *Kennan Cables*. https://www.wilsoncenter.org/publication/kennan-cable-no-39-traditional-state-and-modern-problem-russia-rewrites-its-Internet#_edn11. (25 October, 2019).

Postman, Neil. 1979. "The Information Environment." *ETC: A Review of General Semantics*. http://www.jstor.org/stable/42575416. (3 September, 2019).

Ramesh, Reethika, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. 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 2020.

Remmer, Karen L., and Gilbert W. Merkx. 1982. "Bureaucratic-Authoritarianism Revisited." *Latin American Research Review*. www.jstor.org/stable/2503143. (7 February, 2020).

Repnikova, Maria. 2017. "Media Openings and Political Transitions: Glasnost Versus Yulun Jiandu." *Problems of Post-Communism*. https://doi.org/10.1080/10758216.2017.1307118. (26 March, 2020).

Rivkin-Fish, Michele. 2013. "Conceptualizing Feminist Strategies for Russian Reproductive Politics: Abortion, Surrogate Motherhood, and Family Support after Socialism." *Signs: Journal of Women in Culture & Society*. https://login.ezproxy.bowdoin.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=fmh&AN=85707939&site=ehost-live. (15 April, 2020).

Roberts, Margaret E. 2018a. *Censored: Distraction and Diversion inside China's Great Firewall*: Princeton University Press.

———. 2018b. "Censorship in China." In *Censored*, Distraction and Diversion inside China's Great Firewall: Princeton University Press. 93-112.

———. 2018c. "Implications for a Digital World." In *Censored*, Distraction and Diversion inside China's Great Firewall: Princeton University Press. 223-36.

Robinson, Olga. 2018. "The Memes That Might Get You Jailed in Russia." *BBC* https://www.bbc.com/news/blogs-trending-45247879. (4 January, 2020).

Roudik, Peter. 2016. "Russia: Strengthening of Punishment for Extremism." *Library of Congress Global Legal Monitor*. http://loc.gov/law/foreign-news/article/russia-strengthening-of-punishment-for-extremism/. (15 April, 2020).

Russian Federation. 2016. "Federal Decree: Information Security Doctrine of the Russian Federation." ed. Office of the President of the Russian Federation.

———. 2019. "Об Утверждении Порядка Централизованного Управления Сетью Связи Общего Пользования." ed. ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ.

"Russian Journalist Charged with ‘Insulting the Government’ for a Single Sentence Posted on Telegram." *Meduza*. 2019b. https://meduza.io/en/feature/2019/10/28/russian-journalist-charged-with-insulting-the-government-for-a-single-sentence-posted-on-telegram?utm_source=email&utm_medium=briefly&utm_campaign=2019-10-28. (13 January 2020).

"Russian Public Opinion 2017." *Levada Center*. 2017. (14 June 2018).

Schedler, Andreas. 2002. "The Menu of Manipulation." *Journal of Democracy*. DOI: 10.1353/jod.2002.0031. (28 March, 2020).

Schorske, Carl E., and Zbigniew K. Brzezinski. 1958. "Totalitarian Dictatorship and Autocracy." *The American Historical Review*. https://doi.org/10.1086/ahr/63.2.367. (25 November, 2019).

Seddon, Max, and Henry Foy. 2019. "Russian Technology: Can the Kremlin Control the Internet?" *Financial Times*. https://www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2. (8 January, 2020).

Segal, Adam. 2018. "When China Rules the Web." *Foreign Affairs*. https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web. (4 March, 2020).

Shabaz, Adrian, and Allie Funk. 2019. "Freedom on the Net 2019." *Freedom on the Net Annual Reports*. https://www.freedomonthenet.org/country/russia/freedom-on-the-net/2019. (20 April, 2020).

Shangli, L. I. N., and Joseph Fewsmith. 2014. "Political Consultation and Consultative Politics in China." In *China's Political Development*, eds. Kenneth Lieberthal, Cheng Li and Yu Keping, Chinese and American Perspectives: Brookings Institution Press. 136-64.

Slater, Dan, and Sofia Fenner. 2011. "State Power and Staying Power: Infrastructural Mechanisms and Authoritarian Durability." *Journal of International Affairs*. http://www.jstor.org/stable/24388179. (1 November, 2019).

Soldatov, Andrei. 2017. "The Taming of the Internet." *Russian Social Science Review*. https://doi.org/10.1080/10611428.2017.1275024. (24 February, 2020).

Soldatov, Andrei, and Irina Borogan. 2017. *The Red Web: The Kremlin's War on the Internet* 2 ed. New York, NY: Hachette Book Group. Reprint, 1.

Sondrol, Paul C. 1991. "Totalitarian and Authoritarian Dictators: A Comparison of Fidel Castro and Alfredo Stroessner." *Journal of Latin American Studies*. www.jstor.org/stable/157386. (20 November, 2019).

Stadnik, Ilona. 2019. "Internet Governance in Russia – Sovereign Basics for Independent Runet." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421984#. (13 April, 2020).

Statista. https://www.statista.com/statistics/941456/china-number-of-sina-weibo-users/.

Sulim, Sasha. 2019. "'Online Is Three Times as Dangerous as Offline' a Human Rights Advocate Explains Russia's New Limits on Free Speech." *Meduza*. https://meduza.io/en/feature/2019/03/21/online-is-three-times-as-dangerous-as-offline. (13 January, 2020).

Tétrault-Farber, Gabrielle. 2020. "Explainer: How Putin's Shake-up of Russian Politics Could Pan Out." *Reuters*. https://www.reuters.com/article/us-russia-politics-explainer/explainer-how-putins-shake-up-of-russian-politics-could-pan-out-idUSKBN1ZF1PW. (21 February, 2020).

Tkacheva, Olesya, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, and Caroline Baxter. 2013. "The Internet in China: Threatened Tool of Expression and Mobilization." In *Internet Freedom and Political Space*: RAND Corporation. 93-118.

"Twitter User Numbers Overtaken by China's Sina Weibo." *BBC*. 2017. https://www.bbc.com/news/technology-39947442.

Verkhovsky, Alexander. 2019. "A New Turn of the Kremlin's Anti-Extremist Policy." *PONARS Policy Memos*. http://www.ponarseurasia.org/point-counter/article/new-turn-kremlins-anti-extremist-policy. (5 January, 2020).

Vihalemm, Triin, and Valeria Jakobson. 2011. "Representations of the Past in the Estonian Russian-Language Press: "Own" or Diaspora Memory?" *Nationalities Papers*. https://www.researchgate.net/publication/233230983_Representations_of_the_past_in_the_Estonian_Russian-language_press_Own_or_diaspora_memory. (19 March, 2020).

Weber, Valentin. 2019. "The Worldwide Web of Chinese and Russian Information Controls." *Oxford University Press*. https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf. (9 April, 2020).

"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." *Meduza*. 2019c. https://meduza.io/en/feature/2019/08/29/what-is-center-e. (5 April, 2020).

"White Paper: The Internet in China." Information Office of the State Council, http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207983.htm.

Wike, Richard. 2016. "Broad Support for Internet Freedom around the World." *Pew Research Center Reports*. https://www.pewresearch.org/fact-tank/2016/02/23/broad-support-for-Internet-freedom-around-the-world/. (6 January, 2020).

Williams, Louise. 2013. "Censors at Work, Censors out of Work." In *Losing Control*, eds. Louise Williams and Roland Rich, Freedom of the Press in Asia: ANU Press. 1-15.

Wong, Edward. 2017. "Western China Region Aims to Track People by Requiring Car Navigation." *The New York Times*. https://www.nytimes.com/2017/02/24/world/asia/china-xinjiang-gps-vehicles.html. (20 April, 2020).

Xinhua. 2019. "China to Lead Global Cybersecurity Market Growth in Next 5 Years." *Xinhua*. http://www.china.org.cn/business/2019-09/09/content_75186972.htm. (20 April, 2020).

Xuan, Chen. 2018. "Boundary of Criminal Responsibility of Internet Service Providers." In *Paradigms of Internet Regulation in the European Union and China*, ed. Michael W. Müller Christoph Krönke, Wenguang Yu, Wei Tian. Vol. 13. Baden-Baden: Nomos Verlagsgesellschaft. 192.

Yang, Feng, and Milton L. Mueller. 2019. "Internet Governance in China: A Content Analysis." In *The Palgrave Handbook of Local Governance in Contemporary China*, eds. Jianxing Yu and Sujian Guo. Singapore: Springer Singapore. 441-63.

Yuan, Li. 2018. "A Generation Grows up in China without Google, Facebook or Twitter." *The New York Times*. https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-Internet.html. (4 March, 2020).

Zengke, H. E., and Melanie Manion. 2014. "Building a Modern National Integrity System: Anticorruption and Checks and Balance of Power in China." In *China's Political Development*, eds. Kenneth Lieberthal, Cheng Li and Yu Keping, Chinese and American Perspectives: Brookings Institution Press. 366-96.

Zhao, Suisheng. 2016. "The Ideological Campaign in Xi's China Rebuilding Regime Legitimacy." *Asian Survey* 56: 1168-93. www.jstor.org/stable/26364408. (28 February, 2020).

Кречетова, Ангелина, Петр Харатьян, and Екатерина Кинякина. 2020. "Духовно-Нравственные Ценности Станут Обязательными Для Предустановки На Гаджеты." *Ведомости*. https://www.vedomosti.ru/technology/articles/2020/01/23/821333-duhovno-nravstvennie-tsennosti. (5 February, 2020).

"Курган: Вина Заглажена, Штраф Назначен, Дело По Ст. 282 И Ст. 280 Прекращено." *Документы*. SOVA Center 2018. https://www.sova-center.ru/racism-xenophobia/news/counteraction/2018/02/d38798/. (13 January, 2020).

Лошак, Андрей. *Холивар. История Рунета*, 2019.

"Минкомсвязь: Госорганы И Операторы Связи Готовы Обеспечивать Устойчивую Работу Рунета." 2019 *ТАСС*. https://tass.ru/ekonomika/7407631. (13 January, 2020).

"Мария Мотузная Отсудила 100 Тысяч Рублей За Уголовное Преследование По Делу О Мемах Во «Вконтакте»." *AGORA International Human Rights Group*. 2019a. https://www.agora.legal/news/2019.07.22/Mariya-Motuznaya-otsudila-100-tysyach-rublei-za-ugolovnoe-presledovanie/956. (22 July 2019).

"Президент: Доверие И Голосование." *Levada Center*. 2019. https://www.levada.ru/2019/07/30/prezident-doverie-i-golosovanie/?fromtg=1. (23 April, 2020).

"Прокурор Просит Полтора Года Колонии-Поселения Для Обвиняемой В Экстремизме Из-За Мемов." *OVD-Info*. 2018. https://ovdinfo.org/express-news/2018/04/03/prokuror-prosit-poltora-goda-kolonii-poseleniya-dlya-obvinyaemoy-v?utm_source=tw&utm_medium=social. (10 September, 2019).

"Свобода Интернета 2018: Делегирование Репрессий." *AGORA International Human Rights Group*. 2019b. https://agora.legal/articles/Doklad-Mezhdunarodnoi-Agory-%C2%ABSvoboda-Interneta-2018-delegirovanie-repressiy%C2%BB/18. (5 February 2019).

"Свобода Интернета 2019: План “Крепость”." *Документы*. 2020. https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf. (4 February 2020).

"Список Экстремистов." 2019. ed. Министерство юстиции Российской Федерации. http://data.gov.ru/opendata/7707211418-spisokekstremistov

"Суд Прекратил Дело Об Оскорблении Чувств Верующих Во «Вконтакте»." *Kommersant*. 2017. https://www.kommersant.ru/doc/3219528. (6 January, 2020).

"Финишная Прямая: Совфед Одобрил Закон О Надежном Рунете." *Газета.ру*. 2019. https://www.gazeta.ru/tech/2019/04/22/12315799/sovfed_runet.shtml?updated. (22 April, 2019).