Networked Authoritarianism in the Russian Federation: Domestic Internet Policy and the 2018 Election

Catherine Peterson

A thesis

submitted in partial fulfillment of the

requirements for the degree of

Master of Arts in International Studies: Russia, E Europe & C Asia

University of Washington

2021

Committee:

Scott Radnitz

Jessica Beyer

Program Authorized to Offer Degree:

Jackson School of International Studies

©Copyright 2021

Catherine Peterson

University of Washington

Abstract

Networked Authoritarianism in the Russian Federation:
Domestic Internet Policy and the 2018 Election

Catherine Peterson

Chair of the Supervisory Committee:

Scott Radnitz

Jackson School of International Studies

The Kremlin's strategy toward the internet has evolved markedly over the past decade, leading to the adoption of a variety of legislative and regulatory measures designed to exert increased control over the Russian internet. This paper analyzes the internet control strategies employed by the Kremlin to repress Alexey Navalny's 2018 presidential campaign and their impact. It first addresses how domestic internet policy has changed in recent years before turning to data from Agora and the Levada Center to assess specific mechanisms of internet control used by authorities over the course of the Navalny campaign. Findings indicate that the government relied largely on six main mechanisms of repression, most of them being legislative and non-tech specific. Data also indicate such efforts likely made attracting additional support difficult for the campaign. These findings are consistent with signs that the Russian government is making deliberate efforts to control information within its borders and raises questions regarding the future of internet policy both within Russia and across the globe.

Table of Contents

Introduction

Following the 2016 presidential election, the United States government released a series of reports detailing Russian efforts to interfere with the American electoral process. According to the Senate Intelligence Committee report *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election*, Russia-affiliated actors carried out a variety of cyberattacks against internet-connected election infrastructure and "used social media to sow disinformation and discord among the American electorate" (*Russian Interference*, 2019, p. 67). However, the Russian Federation's manipulation of digital tools is not merely a foreign policy strategy. Efforts to interfere with both international and domestic democratic practices using the internet and social networking sites reflect the larger issue of the Kremlin's embrace of networked authoritarianism, defined as the use of digital communications technologies to consolidate power (MacKinnon, 2010, p. 3). Indeed, the rise of networked authoritarianism within the Russian Federation merits a closer look: how the Kremlin has adapted domestic policies to the internet age will provide insight into how governments seek to erode democracy across the globe.

Democracies such as the United States have typically advocated for freedom of expression online and other digital rights, touting the internet as a free and open global network (Clinton, 2010; *Internet Freedom Section*, 2017). American policymakers initially hoped that expanding internet access would aid in democratization efforts across the globe (Kalathil & Boas, 2002, pp. 1–2) with the idea that increased internet access provides opportunities for broadening political space and promoting democratization (Tkacheva et al., 2013, pp. 204–210). However, the Russian elite have come to regard the internet as a tool of U.S. hegemony and domestic political disruption (Nocetti, 2015b). Fearing the subversive nature of networked technologies, the Kremlin seeks to control, and by extension, de-Americanize the internet

(Nocetti, 2015b). Domestically, this has led to increasingly stringent levels of legislation allowing the government to censor and surveil their citizens.

Previous literature has centered on the period surrounding the 2011-2013 civil unrest and has not addressed how reactions to more recent events have contributed to networked authoritarianism in the Russian Federation. As such, I focus on the period following Putin's 2012 return to the Kremlin by conducting a case study of the 2018 presidential election. More specifically, I examine how the government leveraged state control of the internet to repress Navalny's 2018 presidential campaign and subsequent impact on said campaign. Since most current scholarship focuses on the Kremlin's use of digital technologies prior to and during the 2012 elections, this study will provide insight into how methods of control may have impacted Russian citizens and opposition movements since Putin's return to office.

This research seeks to contribute to current conversations regarding ways in which authoritarian governments seek to erode democratic norms through interference in global information systems. I review the literature on issues of internet sovereignty, the Russian concept of information security (as opposed to the Western idea of cybersecurity) and how Russian citizens utilize digital technologies for social mobilization and political change. I then address my case selection of the 2018 election, including key moments of the Navalny campaign as well as more details on post-2012 internet policy. I follow with a description of the design and methodology of the case study. Building on data from Agora and the Levada Center, I find that the Russian government relied on non-technical legislative measures in addition to harassment of RuNet users to repress campaign activities, which contributed to difficulty in attracting additional Navalny supporters. Finally, I will address how legislation has evolved further since the 2018 election and issues related to global internet governance. Domestic internet control is

part of the larger effort to territorialize information flows and ensure the Russian Federation's sovereignty in cyberspace. This is reflective of a larger global trend, and this study will provide some elucidation regarding the effects of the digital sovereignty movement.

Literature Review

In the three decades since the establishment of the Russian Federation, the government has adopted a variety of controls to regulate the Russian internet (RuNet). While these are domestic policies, there are connections to be drawn to Russia's foreign policy as well: current President Vladimir Putin regards the internet as a geopolitical weapon of U.S. hegemony (Nocetti, 2015b). Indeed, according to Julien Nocetti, the Kremlin perceives the West as manipulating digital technologies to instigate social unrest in countries where opposition parties are otherwise unable to mobilize supporters themselves (Nocetti, 2015a, p. 114). In other words, Putin is keenly aware of the internet's potential for enabling regime change, as evidenced by the Arab Spring uprisings, and Putin's belief has led to the Duma passing a series of laws seeking to exert increased control of domestic internet use since Putin's return to power (Nocetti, 2015b, pp. 2–3).

The goal of this literature review is to understand the origins and evolution of domestic internet policy in the Russian Federation, particularly its role in the development of networked authoritarianism within Russia. Current scholarship focuses on the Kremlin's reframing of domestic internet policy as a national security issue, the Russian concept of information security, and Russian citizens' efforts to leverage the internet to mobilize and advocate for political change.

Internet Sovereignty

Digital technologies and the internet have ushered in an era of global interconnectivity and borderless information flows. However, Milton Mueller posits that nation-states increasingly perceive internet policy through the lens of national sovereignty and are seeking to partition cyberspace much like the physical world by passing legislation designed to align information flows with territorial boundaries (Mueller, 2017). The Russian Federation has largely adopted the aforenamed territorial approach when it comes to internet governance, and the government prioritizes national borders when it comes to creating policy regarding internet infrastructure and the online information space (Kovaleva, 2018, pp. 141–142). According to Mueller, such efforts to realign states and cyberspace rely in part on calls for national securitization (Mueller, 2017, p. 73). DeNardis explains that this shift of the political into the technical is tied to the governmental loss of control over information, whether classified national security materials or global media communications (DeNardis, 2014, p. 10).

As noted by Ermoshina and Musiani, the Russian government began utilizing such narratives as early as 1998 with the implementation of surveillance measures designated as System of Operative Investigative Measures (SORM) (pp. 43-44). SORM-I and later SORM-II (implemented in 2005) allow government services such as the Federal Security Services (FSB) to intercept communications via the telephone and internet. Per Nocetti, the Kremlin justifies such measures as necessary to combat “extremism” (Nocetti, 2015b). Authorities contend, through consistently fear-based language (Ognyanova, 2010, p. 9), that integrating into the global information space exposes Russia to foreign interference. Nocetti argues further that intelligence services openly underscore the potential for national security emergencies as a result of being connected to the Internet (Nocetti, 2018, p. 186).

The Information Threat

The American concept of cybersecurity focuses on the protection of networks and physical infrastructure to ensure the confidentiality, integrity and availability of information (*What Is Cybersecurity?*, 2019). Russian officials, however, view cyber and information as one, encompassed within the concept of information security (*informatsionnaya bezopasnost'*). According to Nocetti, while the Kremlin sees information as including the "thoughts in one's head and information in books and documents," cyber has become the *technical* representation of information (Nocetti, 2018, p. 184). He posits that the Russian "view of security of information includes therefore several dimensions: human, social, spiritual, and technical factors" (Nocetti, 2018, p. 184). Indeed, the Russian government views information security as defending both citizens and the State against both internal and external threats using a range of legal, investigative, intelligence and technological measures (*Doctrine of Information Security*, 2016)

Scholars overwhelmingly agree that two events in particular helped solidify this perspective. The 2011 Arab Spring protests—organized thanks to digital platforms such as Twitter—sparked Kremlin fears of possible domestic social unrest engineered from abroad (Nocetti, 2015b). While such events in the Arab world stoked Kremlin fears of the internet's potential to facilitate regime change, Edward Snowden's 2013 revelations on American electronic surveillance fanned the flames further. According to Nocetti, Snowden's leaks strengthened the Kremlin belief that domestic internet access and the accompanying information revolution had become one of "most pervasive components of U.S. expansionism in the post-Soviet sphere" (Nocetti, 2018, p. 188). Maréchal agrees that Putin associates the internet with the U.S. government and its "unique role in internet governance and [as] a major funder of the global digital rights movement" (Maréchal, 2017, p. 35).

Social Media and Social Mobilization

While the basic technology behind the Internet and the concepts around which it was conceived—connectivity and information sharing—lend themselves to the process of democratization and the development of an informed, participatory electorate, authoritarian regimes have also understood the internet's potential to censor and surveil citizens. Denisova posits that the government's focus on internet regulation both confirms the importance of the online protest movement as well as leads to the potential for additional oppression of digital activism (Denisova, 2017). The Kremlin has recognized that digital technologies can be used to intimidate activists, spread disinformation and otherwise disrupt opposition movements, ultimately precipitating their dissolution (Deibert & Rohozinski, 2010, p. 16). Therefore, the Russian government has sought to implement control strategies that manipulate how and when netizens receive information (Deibert & Rohozinski, 2010, p. 16). Authors White and McAllister add that authoritarian leaders have responded to social media challenges through information monitoring and information denial, e.g. shutting down the internet "at crucial times" (White & McAllister, 2014, p. 74). This in turn has led to what Ermoshina and Musiani refer to as an "infrastructural battle" between the Russian government who seeks to control internet infrastructure and users and providers who attempt to reconfigure infrastructure to evade government control (Ermoshina & Musiani, 2017, p. 52). They contend that the ways in which the Russian government co-opts internet infrastructure have encouraged individual mobilization, the results of which have in turn affected the geopolitics of the Russian internet.

Despite government efforts to maintain control over political narratives, the internet and social networking sites have provided Russian citizens with unprecedented opportunity to change political agenda-setting. As noted by scholars Deibert and Rohozinski, the internet has surpassed

other types of mass media when it comes to boosting free speech and facilitating social mobilization (Deibert et al., 2010, p. 19). White and McAllister concur and explain that, while political elites have traditionally maintained significant control over traditional media, thereby conditioning the public to react to events in a foreseeable manner, social networking sites are more difficult for elites to regulate and allow dissidents to bypass official media and avoid censorship (White & McAllister, 2014, p. 73). Indeed, Russian opposition leader Alexey Navalny has gained in both notoriety and popularity thanks to his online presence and leveraging of social networking sites in spite of rarely being mentioned through state-run media (Kazun, 2019, p. 313). Further, the opposition's use of both Twitter and Facebook were integral in disseminating information on protests following the disputed 2011 Duma elections and Putin's 2012 re-election (Placek, 2019, p. 498).

Government attitudes toward the information space have evolved significantly beginning in 2012, and the Duma continues to pass legislation which further strengthens internet regulations and internet control. This review examined the origin and evolution of these policies and regulations as part of the digital sovereignty movement, the Russian concept of information security and the internet as a tool for social mobilization. The reviewed literature suggests that efforts to control the domestic digital space through surveillance and censorship reflect the Kremlin's view that the internet and information are dangerous weapons, representing both internal and external threats to the current regime. Domestic internet policy and its enforcement are, therefore, intimately tied to the Russian Federation's foreign policy, and understanding the development of networked authoritarianism within Russia will provide greater insight into the Russian Federation's interference in global information systems. Accordingly, this study seeks to understand how the Kremlin leveraged state control of the internet to repress Navalny's 2018

presidential campaign and the impact of said efforts. By exploring the impact that internet controls have had on opposition parties, we will gain a better understanding of how networked authoritarianism has developed within the Russian Federation.

Research Design

Case Selection

The question of how domestic internet policy and regulations have contributed to the development of networked authoritarianism within Russia can be answered by looking at the 2018 presidential election, specifically opposition politician Alexey Navalny's campaign starting in December 2016. As an electoral or hybrid regime, Russia is a combination of democratic and non-democratic components, meaning the state uses elections to disguise oppression and provide a sense of regime legitimacy while restricting freedoms, ignoring civil liberties and allowing corruption to flourish (Upadhyay, 2018, p. 273). To limit electoral challenges to the regime, the state relies on "targeted repression, surveillance, and selective prosecution against opposition activists" (Dollbaum et al., 2018, p. 619). Navalny's campaign is a pertinent case study given the opposition leader's involvement in the 2011-2012 protests that contributed the Kremlin's threat-oriented approach to information and the internet (Dollbaum et al., 2018, p. 619). Previous scholarship has focused on the 2011-2012 Duma and presidential elections, yet, considering the government's stance on internet policy has since changed, a case study looking at the ramifications of these transformations will provide additional insight into how the Kremlin is evolving in their use of digital technologies to exert control over Russian citizens.

Post-2012 Internet Governance

Prior to Putin's reelection, the RuNet remained largely unfettered by government control, in part due to low internet penetration rates as well as an underestimation of its political relevance (Alexanyan et al., 2012; Kazun & Semykina, 2020; Sivetc, 2019; Treisman, 2018). This allowed a "remarkably free," robust internet culture to establish itself (Alexanyan et al., 2012, p. 10). During this unregulated—though not unsurveilled—time, RuNet infrastructure became enmeshed with overall global internet infrastructure, and RuNet users became accustomed to forming online civic groups and accessing international content such as YouTube (Alexanyan et al., 2012).

In autumn 2012, 48.6 million Russians, or 40% of the population, were daily internet users (*Internet v Rossii 2012*, 2012), and by the end of the year there were 4.21 million .ru domains (*Domeny Rossii*, n.d.). The government seemingly wanted to facilitate citizens' internet access as in January of 2013, Prime Minister Medvedev initiated plans to lower the cost of connecting households to the internet ("Medvedev," 2013). During this time, human rights activists reported 1,197 internet freedom restrictions for the year, a fairly low number relatively speaking (Gaĭnutdinov & Chikov, 2013, p. 2). Despite such seemingly positive news of expanding internet access, internet regulations began occupying an increasingly more significant amount of legislative and political agenda setting.

A reliance on international infrastructure (Ermoshina et al., 2021, p. 12) and users' habituation to a free RuNet have made outright filtering and blocking technically and politically complicated. The RuNet currently depends on international Domain Name System (DNS) infrastructure as well as global cloud services such as Amazon Web Services, Google and Microsoft, which makes backward engineering internet architecture difficult (Jee, 2019). Corruption and lack of expertise also contribute to the complexity of introducing and enforcing

more technically restrictive internet controls (Ermoshina et al., 2021, p. 12). Authorities in the Russian Federation have, therefore, generally avoided direct censorship of content as seen in other countries: first generation internet controls focused on denying access to information by directly blocking resources via technical means, akin to Chinese-style filtering, remain largely unused (Deibert & Rohozinski, 2010, pp. 16–17). (The 2012 'internet blacklist law' seeking to ban content related to drug abuse, suicide and child pornography is perhaps the exception to this and a step toward more stringent internet-specific restrictions ("Russia Internet Blacklist Law Takes Effect," 2012).) Rather, second and third generation controls, involving legislative and regulatory measures meant to encourage self-censorship, are preferred (Deibert & Rohozinski, 2010, p. 17). Second generation controls rely on legal justifications for information access denial, generally involving the implementation of non-internet related laws to the online space, and are generally applied when the information in question has the most value, e.g. before an election (Deibert & Rohozinski, 2010, p. 24). Third generation controls focus on surveillance, data mining, and direct physical action to disrupt users (Deibert & Rohozinski, 2010, p. 28). Multiple types of controls can coexist, as seen in Russia (Deibert & Rohozinski, 2010, p. 23).

Comparable internet control measures are observed in other post-Soviet states as well. Belarus and Kazakhstan employ measures most similar to those seen in Russia, including the creation of a normative environment for information control, warrantless surveillance and taking direct action against users (Deibert & Rohozinski, 2010). Ukraine and Georgia have the fewest controls in place, relying solely on developing a legal and normative control system, while Uzbekistan and Turkmenistan rely on first generation controls like internet filtering in addition to measures similar to those seen in Russia (Deibert & Rohozinski, 2010).

Within Russia, surveillance measures originated in 1998 with the introduction of SORM, or System of Operative Investigative Measures, which allows law enforcement and intelligence agencies direct access to the information stored on commercial databases (Ermoshina & Musiani, 2017, p. 43). SORM-1 implementation required that telecommunications operators install hardware allowing the FSB access to telephone calls, and in 2005, SORM-2 extended these capabilities to email and web browsing traffic by compelling ISPs (internet service providers) to install devices allowing the FSB to intercept data. Finally, SORM-3, implemented in 2014, encompasses all telecommunications data, including "SMS, MMS, forums, blogs, and social networks" (Bourgelais, n.d., p. 8). While most Western countries require law enforcement agencies to seek warrants before being able to ask that an ISP lawfully intercept and deliver data, SORM architecture allows the FSB to bypass contacting ISPs. SORM control stations are located in regional FSB offices, and the hardware and software used to access data are able to do so remotely, meaning that ISPs may not realize what data is extracted and inspected (Ermoshina & Musiani, 2017, p. 44). Additionally, SORM-3 requires that ISPs and network providers store data for three years, and maintenance of SORM equipment remains the responsibility of the ISPs.

In February 2014, the "Lugovoy Law" was entered into force, allowing for the blocking of websites "if they contain "extremist" content, call for mass riots, or call for participation in unsanctioned public gatherings (*Russia,* 2014). Later that year, a data localization law was signed, compelling ISPs to store the personal data of Russian citizens on the territory of the Russian Federation. ISPs must guarantee the storage, modification and extraction of data using databases within Russia. Web services must also allow intelligence and security services high level, or 'backdoor,' user access to data (Ermoshina & Musiani, 2017, p. 46).

Efforts to increase control of the information space accelerated even more dramatically in 2016. “At least 97 legislative initiatives related to Internet regulation were announced and approved in Russia in 2016. There were only five in 2011” (*Russia’s Social Networks*, 2017). Allegedly in an effort to bolster public safety, the Yarovaya Law was signed and came into force over the course of 2016. Building on previous laws, it included new surveillance measures requiring telecom operators to save traffic and related meta data for three years (Ermoshina & Musiani, 2017, p. 45). Authorities claimed the law was designed to boost anti-terrorism measures and strengthen punishment for extremist activity (*The Yarovaya Law: One Year After*, 2017, p. 3). This explanation is in line with the government’s evolving policy towards the internet, which “has been in fact characterized by the words ‘attack’, ‘campaign’, ‘enemies’, and has practically turned into a military campaign against the free RuNet” (Gaĭnutdinov & Chikov, 2017, p. 19).

In light of this mentality, the government published an updated Doctrine of Information Security of the Russian Federation on December 5, 2016. The Doctrine represents the government’s “official views on ensuring the national security of the Russian Federation in the information sphere” (*Doctrine of Information Security*, 2016). It focuses on perceived internal and external threats such as

> the possibility for cross-border information exchange, the use by foreign intelligence services of the Internet to exert ‘informational-psychological influence’ aimed at the destabilization of the domestic and social situation, as well as an increase of materials in foreign media containing biased assessment of the State policies of the Russian Federation. (Gaĭnutdinov & Chikov, 2017, p. 19).

Such national security concerns are a pretense to exert ever more control over the information space and internet users.

Alexey Navalny and Social Media

Despite harsh criticism of the president, Alexey Navalny has become Russia's leading opposition politician and "one of only two individuals in Russia with substantive political autonomy – the other one being Putin" (Ferrari, 2018, p. 69). The creator of the Anti-Corruption Foundation (FBK), an organization that "investigates, reveals and prevents corruption among high-ranking Russian government officials" (*The Anti-Corruption Foundation*, n.d.), Navalny shares the results of his investigations—which include exposés on both former president Dmitry Medvedev and current president Vladimir Putin—on social media platforms, notably his YouTube channel. Thanks to this active social media presence, *Time Magazine* even named him as one of 2017's most influential people on the internet (*25 Most Influential People*, 2017). However, online fame doesn't necessarily translate to notoriety at large in Russia. Indeed, Navalny is considered a persona non grata by the state, and government officials and state-run media refuse to mention him by name on television (Kazun, 2019, p. 313).

In late 2011, "For Fair Elections" (FFE) protests erupted in Moscow and across Russia, prompted by rigged parliamentary elections, and social networking sites such as Facebook, Twitter and Russia-based VKontakte became essential in organizing and financing protests. Navalny himself participated in the demonstrations and was subsequently arrested. However, it was the 2013 Moscow mayoral elections, in which he received a surprising 27% of the vote, that established him "as the most credible threat to the political status quo" (Dollbaum et al., 2018, p. 620). Navalny's increasing popularity and such widescale social mobilization correspondingly rekindled Kremlin suspicion regarding the Internet and its role in facilitating civil unrest (Nocetti, 2018, p. 188), and in the ensuing years the Duma began enacting a series of increasingly restrictive internet regulations.

By 2016, internet penetration in Russia had increased to 57% or 66 million daily users (*Internet v Rossii 2016*, 2016), and, as of December that year, there were 5.42 million .ru domains (*Domeny Rossii*, n.d.). Despite RuNet growth, most Russians still preferred television to stay informed. According to 2016 Levada Center data, 86% of Russians preferred to receive their news via television, while only 23% relied on social media (*Channels of Information*, 2018). Additional 2016 data reveal that, although 44% of Russians used the internet either every day or almost every day, 27% never did (*The Number of Internet Users*, 2018). Nonetheless, somewhat miraculously, 47% of survey respondents knew who Navalny was as of February 2015 (data for 2016 not found) (*Aleksey Navalny*, 2017).

Timeline of the 2018 Election

In December 2016, Navalny announced his intention to run for president in 2018, and his campaign had a decidedly American spin with a country-wide network of volunteers, logo-emblazoned sweatshirts and uniformly designed pamphlets (Dollbaum et al., 2018, p. 622). As part of their street campaigning, volunteers were tasked with helping to gather the 300,000 votes needed for Navalny to register as an independent presidential candidate (Dollbaum et al., 2018, p. 620). Since state-run television prohibited any Navalny coverage on their platforms, his campaign relied on social media to get the message out. In March 2017, Navalny and the FBK posted a YouTube video—*On vam ne Dimon*—describing corruption of then-prime minister Dmitry Medvedev. According to a Levada poll, 30% of respondents had heard of the documentary, making it "an ideal anchor for what appeared to be a central part of the campaign's strategy: street protests" (Dollbaum et al., 2018, p. 620).

The first big rallies of the campaign occurred on March 26, 2017, and the Navalny campaign sought to attract large crowds in order to project an image of strength to both the

public as well as the Kremlin. Authorities arrested over 1,000 participants in addition to Navalny. In the fall he was again detained yet again—this time for thirty days—while on a cross-country electoral tour. Navalny's troubles culminated on December 25, 2017 when the central electoral commission announced that Navalny could not participate in the election due to an earlier criminal conviction. Notably, the European Court of Human rights had already determined this was an "arbitrary" ruling (*Human Rights Court Says Navalny Unfairly Convicted In "Yves Rocher Case,"* 2017). Navalny subsequently encouraged supporters to boycott the election, which would lower turnout and diminish any sense of electoral legitimacy.

Many of the campaign's 199,836 volunteers were teenagers and young adults (*Navalny's Campaign 2018. How It Was*, n.d.), which corresponds with higher internet and social media—platforms at Navalny's disposal—use among this population. Despite the campaign's extensive volunteer network and crowd-sourced funding, Navalny volunteers, supporters and activists had to deal with significant harassment including arrests, lack of premises for campaign activities, and raids on people's offices and homes (Dollbaum et al., 2018, p. 622).

Hypotheses

Russian internet penetration and digital media use—from social networking sites to blogs and independent news sites—have steadily increased over the past several years, during which time Navalny has become Russia's most prominent opposition leader, largely thanks to his active online presence. However, the Kremlin has also proved itself adept at media manipulation, and even digitally experienced RuNet users may engage with content confirming pre-existing views consistent with high approval ratings for and overall satisfaction with government officials

(Volkov & Goncharov, 2014). As such, I propose the following two hypotheses when it comes to assessing how government control of the internet may have impacted Navalny's campaign:

Hypothesis 1: Internet restrictions and repression efforts led to an extension of Navalny's follower base.

Protest activism during 2011-2012 affirmed the digital world's power in allowing citizens to circumvent censorship and promote dissent discourse in an otherwise restrictive media environment (Denisova, 2017). Moreover, Soviet history reveals that content restrictions can encourage creativity in exploring new means of communication and expression, meaning that government repression efforts may galvanize public participation in activism (Denisova, 2017). Indeed, research has shown that increasing censorship has encouraged RuNet users to explore a variety of resistance tactics, including petitions, reorientation towards products and services beyond government purview, subversive error messages on blocked sites and technical countermeasures like VPNs and the Tor network, i.e. software that enables anonymous communication (Ermoshina & Musiani, 2017). RuNet users also post content to multiple platforms, including Western ones, which allows for easier subversion of government control measures (Denisova, 2017).

Government attempts to silence opposition parties can also become a tool for activists, and Navalny's campaign shrewdly began integrating repression efforts into their campaign strategy (Dollbaum et al., 2018). That is to say, government repression provided his campaign with evidence to validate their overall message—that honest, everyday Russians were resisting systemic corruption coming from a callous, incompetent elite who rely entirely on intimidation and extensive power abuse to advance their own self-interests (Dollbaum et al., 2018). In

contrast, Navalny's campaign was run by capable, earnest people with fewer resources and for the benefit of Russian society at large.

Given the above, it could theoretically be expected that internet repression efforts would encourage solidarity, increase networking opportunities across societal boundaries, facilitate positive involvement in collective action and boost Navalny's popularity, leading to an increase in support for the opposition leader.

Hypothesis 2: Internet restrictions and repression efforts led to a contraction in Navalny's follower base.

While repression efforts confirm the internet's growing role in promoting dissent and may energize some supporters, activists need to be able to connect with a wide audience in order to spread their message (Denisova, 2017). Individual internet users also need some level of supplementary organization to overcome disengagement, misunderstandings and possible alienation from other users (Denisova, 2017). Repression efforts that reduce opportunities for opposition activists to disseminate their message and collaborate online may isolate individuals. If users fear coming into conflict with their social surroundings by expressing political dissent, this may in turn encourage a cycle of self-censorship and further isolation. Additionally, despite routine complaints about corruption and economic inequality, many Russians distrust politicians and perceive of politics as inherently 'dirty,' meaning that, for many, the risks associated with collective action exceed any possible benefits (Dollbaum et al., 2018). Government control of the information space may, therefore, minimize willingness to participate in campaign support activities, online or in-person, by increasing exposure and liability for those who do engage.

Considering the above, it could theoretically be expected that internet repression efforts would dilute online activist organization, cause activists and supporters to lose their motivation,

and discourage additional voters from participating in campaign activities or from seeking information from diverse or unconventional sources, thereby leading to a decrease in support for Navalny.

Data and Methods

Data was obtained from the Agora International Human Rights Group to assess both the specific internet control measures used by authorities as well as their frequency during Navalny's presidential campaign. Founded in 2005 by lawyer Pavel Chikov, Agora is a Russia-based human rights organization known for its pro-bono work defending activists, journalists and bloggers. Also a member of the International Network of Civil Liberties Organizations (INCLO), an international group of independent human rights organizations, Agora is currently defending 160 cases before the European Court of Human Rights (*International Human Rights Group Agora*, n.d.). Added to the government's blacklist of 'foreign agents,' or organizations receiving foreign funding and engaging in political activity, Agora was banned in early 2015 before re-organizing later the same year (Chikov, 2016; Smirnov, 2015). One of Russia's most well-known experts on human rights issues, Chikov is a former member of the Presidential Council on Civil Society Development and Human Rights, an advisory body established to inform the president on human and civil rights issues, serving from 2012 until 2019 (Kozenko, 2016; *Pavel Chikov*, n.d.). Notable Agora clients have included 2012 protestors, Pussy Riot and Alexsey Navalny himself (Kozenko, 2016). Indeed, Agora lawyers have worked with opposition activists for several years (Bushuev, 2020), representing a possible source of bias in Agora reporting. Agora has not specifically made note of any possible conflicts of interest when it comes to their reporting and opposition parties. Despite this, no evidence of explicit political support on the part

of Agora or Chikov for Navalny was identified. Further, Navalny has not been Agora's principal client as they have worked with a wide range of individuals (Kozenko, 2016).

Since 2011, Agora has published an annual report on internet freedom in the Russian Federation (Suleĭmanov, 2018). Reports consist of two main parts, the first of which provides an assessment of the overall internet landscape in Russia and the second which presents quantitative data on the number of identified instances of restrictions to internet freedom. This second section also provides qualitative data on some of the more flagrant acts of restriction. Reports for 2017 and 2018 also include, via an Excel file (Soshnikov et al., 2019; Suleĭmanov, 2018), "an annexed summary table with the date, source, region and type of restriction in each case about which information is available" (Gaĭnutdinov & Chikov, 2017). Because Roskomnadzor—the federal body supervising media and telecommunications—has not published official statistics regarding court cases, all information included in the summary tables was open-source, generally news articles and blog postings. Since Agora data originate from such open-source material, it may be incomplete as other instances of restriction or repression may have occurred but were not reported on in the media, whether independent or state-controlled. Despite extensive searching, the summary table for 2016 was not located. It should be noted here that all Agora reports referenced in this paper were found via third party news sites such as Meduza.io: for the duration of this project, the agora.legal and en.agora.legal sites were "temporarily closed for technical reasons."

This study relies primarily on reports from 2016, 2017 and 2018, since Navalny announced his campaign in December 2016, the campaign spanned 2017, and the election took place in March 2018. Summary tables for 2017 and 2018 were used to identify instances of restriction related to Navalny. Considering Navalny announced his campaign in December 2016

and the election took place in March 2018, no filtering of dates was needed for the 2017 summary table. The 2018 summary table was first filtered for dates through March 31, 2018 since the election took place on March 18, 2018. Then the Excel file was searched by the following key terms in Russian: Alexey Navalny (Alekseĭ Naval'nyĭ); opposition party (oppozi͡tsionnai͡a parti͡a); election (vybory); and voting/polling (golosovannie). Once these Navalny-related instances were identified, provided sources (i.e. links to news articles, blogs or social media posts) were then double-checked to confirm the instance was indeed related to Navalny. Those that were not relevant were discarded. After having been collected, articles and blog posts were read to identify methods of internet control and were accordingly categorized into thematic groups. Data from GoogleTrends and the Levada Center were used to assess the impact of government controls.

Results

Of the 1,018 instances of internet restrictions recorded by Agora between January 1, 2017 and March 31, 2018, 51 (5%) were identified as related to Navalny and his campaign. This is a significant percentage considering that no other person or entity was noted as having more than one or two instances of associated internet restriction during this period. Other instances of internet restrictions not related to the Navalny campaign were directed at individual journalists, bloggers, activists and member of the general public.

In conducting this analysis, six main mechanisms of repression were identified from the corpus of data. These categories included "protest events," "offensive or extremist material," "website content," "coercion/harassment," "campaign laws," and "other." These topics will be discussed in the following section.

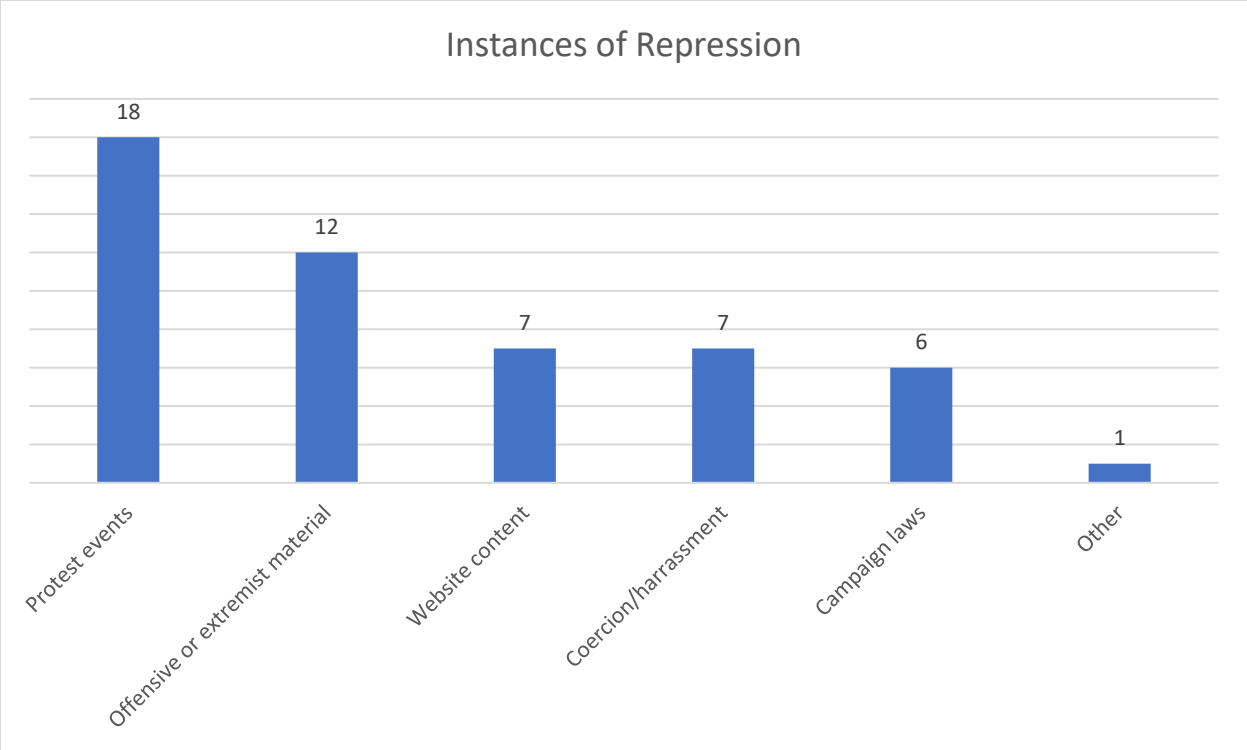


Figure 1: Instances of Repression by Mechanism Type

Further, each case of repression tied to Navalny's campaign fell into either second or third generation internet controls. Neither generation of controls is particularly high tech, relying instead on soft means of control. Second generation controls focus on creating a "legal and normative environment" that allows for the denial of access to information resources as needed (Deibert & Rohozinski, 2010, p. 24). Second generation controls do not require that regulations be specific to the internet. Indeed, means of control may instead rely on the arbitrary application of criminal, financial or other laws (Ognyanova, 2019, p. 1781). Third generation controls involve a more complex approach than either first- or second-generation controls. Rather than deny access to online information or resources, third generation controls seek to "to effect cognitive change" (Deibert & Rohozinski, 2010, p. 28). This generally involves encouraging self-censorship through verbal or physical harassment.

Five of the six themes identified in this study could be categorized under second-generation controls.

Protest events

Protests and rallies were characteristic of the Navalny campaign. Accordingly, one of the most common legal mechanisms for repression was the application of Article 20.2 of the Administrative Code ("Violating the Established Procedure for Arranging or Conducting a Meeting, Rally, Demonstration, Procession or Picket") (*Kodeks RF*, 2001). In one instance, a blogger was arrested for having organized a public event without submitting the proper notifications after simply posting a video online in support of a Navalny rally ("Blogera v Krasnodare," 2017).

Leonid Volkov, Navalny's campaign chief of staff, was also accused of calling for an unauthorized public event after tweeting the links to two blog posts on Navalny's website. In the first blog post, he encourages supporters to continue protesting despite Navalny's arrest, stating that "The election campaign must continue. Meetings with Navalny can be held without Navalny"[1] ("Navaln'nomu dali 20 sutok aresta," 2017). In the second, Volkov invokes supporters to put forth their political demands, both online and in-person:

> On October 7, write via any of your social networks, tell the media, or just call your grandmother to say that you personally put forward two main political demands:
>
> a) I demand political competition
>
> b) I demand the admission of Navalny and any other candidates who are able to collect the necessary 300,000 signatures.
>
> We say this on the Internet. And we say it in the streets.[2] ("Chto proiskhodit i chto delat'," 2017)

[1] Translation my own. Original text: "Избирательная кампания должна продолжиться. Встречи с Навальным можно проводить и без Навального."

[2] Translation my own. Original text: "7 октября напишите в любой своей социальной сети, скажите в СМИ, ну или просто по телефону своей бабушке, что лично вы выдвигаете два главных политических требования: а) я требую политической конкуренции б) я требую допуска на выборы Навального и любых других кандидатов, способных собрать необходимые 300 000 подписей. Мы говорим это в интернете. И говорим это на улицах."

Here, Volkov draws a direct connection between online activism and activism via street protests. The blog post continues with details on an organized protest in the coming days.

Campaign laws

Beyond protest related legislation, campaigning laws were another means of government control. Early in the campaign, the electronic payment service Yandex.Money disabled Volkov's account which had been used to collect campaign funds. Without specifying specific legal prohibitions, the service asserted that new rules prohibited individuals from using Yandex.Money to raise money for political purposes ("'I͡andeks.Den'gi,'" 2017). Map and navigation service 2GIS removed the addresses of Navalny's campaign headquarters from their maps, since Navalny was not a representative of the government and was therefore unable to have a registered headquarters (Ri͡abova, 2017).

Website content

Laws related to defamation and slander are other popular second generation controls. Over the course of his campaign, Navalny was involved, directly or indirectly, in civil lawsuits related to FBK investigations. Businessman Alisher Usmanov filed a claim against Navalny for "the protection of honor and dignity" related to an FBK investigation on luxury real estate and land transfer between Usmanov and Prime Minister Medvedev ("Alisher Usmanov," 2017). The court determined the FBK video contained defamatory material and ruled in Usmanov's favor, requiring Navalny and the FBK to remove the video and associated publications. They were later fined for non-compliance ("Pristavy oshtrafovali Naval'nogo," 2018).

In a second example, Navalny was impacted by another civil suit, despite not being a defendant in the case. Businessman Oleg Deripaska sued two other individuals for spreading

information about his private life. This information had been the basis for an FBK report, and other media outlets picked up the story. In association with the lawsuit, Roskomnadzor required that materials related to the FBK investigation be removed from media outlets, Instagram and YouTube. They also blocked Navalny's website ("Blokirovka saĭta Naval'nogo," 2018). It should be noted that Deripaska has close ties with Putin (Stone, 2019). Deripaska's civil suit, and associated information removal requests, was yet another way for the government to repress Navalny's campaign.

Offensive or extremist material

After protest events, the second largest category was offensive or extremist material. This echoes the Doctrine of Information Security in that said document cites the free flow of information as an opportunity for the spread of extremism (*Doctrine of Information Security*, 2016). Russian extremism legislation is ambiguous and loosely qualifies extremism as anything justifying terrorism, stirring up social or other discord, obstructing lawful activities and spreading propaganda, among other activities (Roudik, 2020). During the course of the campaign, authorities classified everything from rally photos published on VKontakte to videos in support of Navalny as extremist material ("Lidera PARNASa," 2017).

Laws related to the display of fascist symbols and the incitement to hatred were also enforced. In one incident, following an attack on Navalny during which he was doused with an antiseptic that stained his face green, a campaign volunteer posted an image to VKontakte of the statue "The Motherland Calls!" photoshopped with a green face and hand. Authorities subsequently searched his Volgograd campaign headquarters and ultimately submitted a case under Article 354.1 for the "dissemination of information about the days of military glory and memorable dates of Russia related to the defense of the Fatherland, as well as desecration of

symbols of military glory of Russia, insult to the memory of defenders of the Fatherland or humiliation of the honor and dignity of a veteran of the Great Patriotic War"[3] (*UK RF Stat'i͡a 354.1*, 2014).

Other

While most incidents of repression were related to the above, authorities also resorted to more unconventional legislation. A student from Tyumen was detained after being caught putting up FBK leaflets. Authorities initially attempted to charge the student with extremism but, after some confusion, preferred a regional code related to the violation of landscaping regulations (Sulim, 2017).

The remaining theme identified in this study, "coercion/harassment," is categorized under third-generation controls.

Coercion/harassment

On March 26th, students around the country attended Navalny rallies, often posting questions about and photos of rallies online. While social media permitted students to organize and share information, it also allowed authorities to track their activities. A Kazan Federal University student who attended a March 26th rally received a request from a university administrator that she avoid participating in any rallies or demonstrations (Sulim, 2017). This was after her mother received a call from another university employee threatening to have the student expelled for leading an active political life in support of Navalny. The same student relayed that classmates had been forced to remove rally-related comments from the university's VKontakte page.

[3] Translation my own. Original text: "Распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России, связанных с защитой Отечества, а равно осквернение символов воинской славы России, оскорбление памяти защитников Отечества либо унижение чести и достоинства ветерана Великой Отечественной войны."

In yet another example of youth activist harassment, the deputy director of a school in Vladimir threated to have students who posted such photos removed from their families for having attended Navalny rallies. According to the deputy director, the students' parents were failing to fulfill their duties by allowing their children to become members "of an extremist group"[4] ("Zamdirektora shkoly," 2017). In Cheboksary, a teacher attempted to dissuade students from joining social media groups in support of Navalny, warning that "an investigation almost always ends at the level of the FSB"[5] and that they should think twice before joining any VKontakte groups (*53 stol'ko raz*, 2017).

Journalists and bloggers faced pressure from those in positions of power, as well. The editor-in-chief of an online Novosibirsk magazine resigned in September 2017 after one of his articles covering a Navalny rally was removed from the site after its publication. According to him, "(The decision was made) that we do not write about the rally, and I'd had enough. I think, in general, it was decided to pretend that Navalny does not exist at all"[6] (T͡soĭ, 2017b). This effort to repress campaign information is perhaps not surprising, given Russian media traditions of censorship. Indeed, "Internet censorship mechanisms are often indistinguishable from the ones used in traditional media" (Ognyanova, 2010, p. 2).

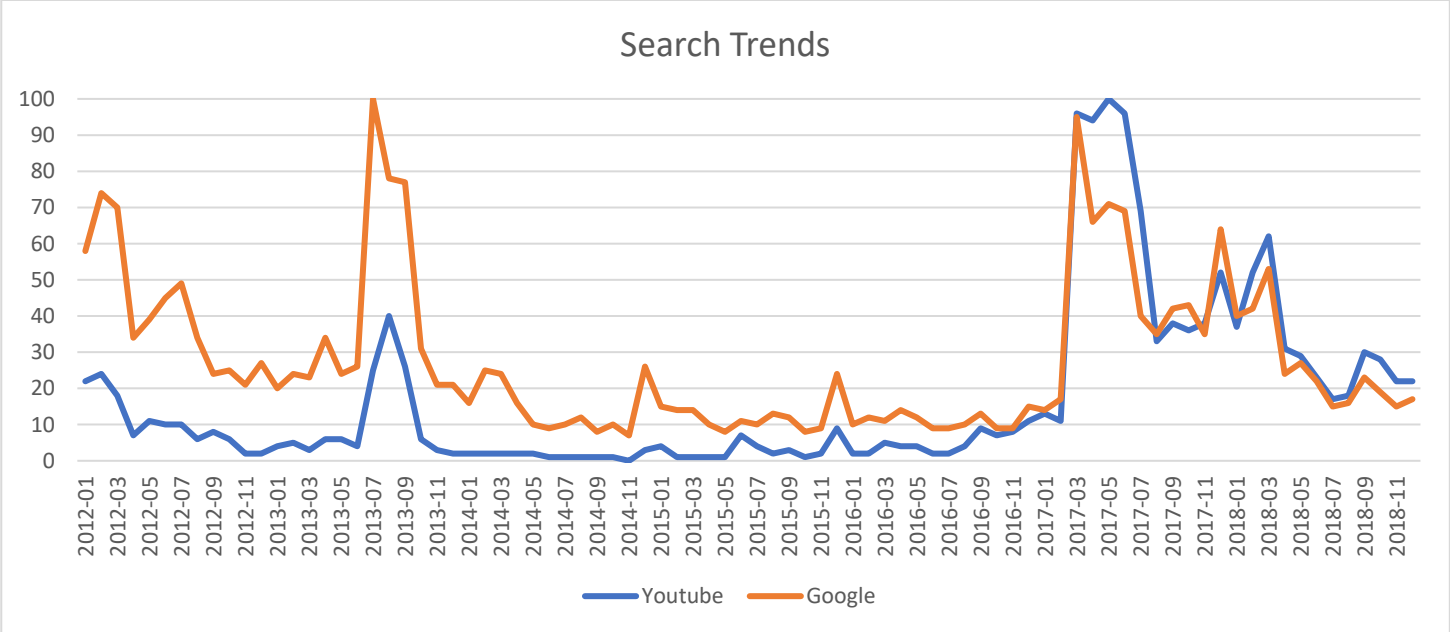
Even those not directly involved in campaign activities or protests were subject to harassment by authorities. A bystander filming a conversation between police officers and an activist distributing campaign leaflets was detained and questioned by police (T͡soĭ, 2017a).

Impact

[4] Translation my own. Original text: "группы экстремистской направленности."
[5] Translation my own. Original text: "разбирательство заканчивается чуть ли не на уровне ФСБ."
[6] Translation my own. Original text: "(Решение было) о том, что не пишем о митинге, и мне этого хватило. Думаю, вообще было решено сделать вид, что Навального не существует в природе."

This analysis identified six predominant categories related to internet controls utilized to repress opposition activity during the 2018 election. The instances detailed above highlight the government's use of second and third generation internet controls in their effort to stifle Navalny's campaign. What was the impact of these efforts? Government repression efforts seemed to have played a role in preventing him from gaining further support from the general public, though they did not seem to have caused him to lose supporters, an outcome which confirms neither an extension nor a contraction of his follower base as hypothesized. A closer look reveals that, despite an increase in RuNet users and an only selectively censored online ecosystem, the internet has been unable to compete with messaging from state media; internet repression efforts are tied to the broader efforts of the Putin regime to control the larger information space—both digital and analog—in order to secure and legitimize power.

GoogleTrends data reveal that from March through June 2017, there was a spike in both Google and YouTube searches for Navalny (*Google Trends*, n.d.-a; *Google Trends*, n.d.-b). This



was during the time of the campaign's initial protests and reflects a similar spike prior to the 2013 Moscow mayoral election in which Navalny ran. (See figure 2[7].)

According to Levada Center data, the 2013 search spike correlates with an increase in recognition. However, the increase in searches for Navalny in 2017 seems to be correlated to smaller increase in name recognition amongst those polled (See figure 3) (*Aleksey Navalny*, 2017). Indeed, ordinary voters know little about politicians who are not mentioned in state-run media (Volkov & Goncharov, 2014). Even then, state-promoted smear campaigns and otherwise hostile treatment by the mass media mean that greater recognition does not necessarily equate to greater electoral support (Dollbaum, 2020).

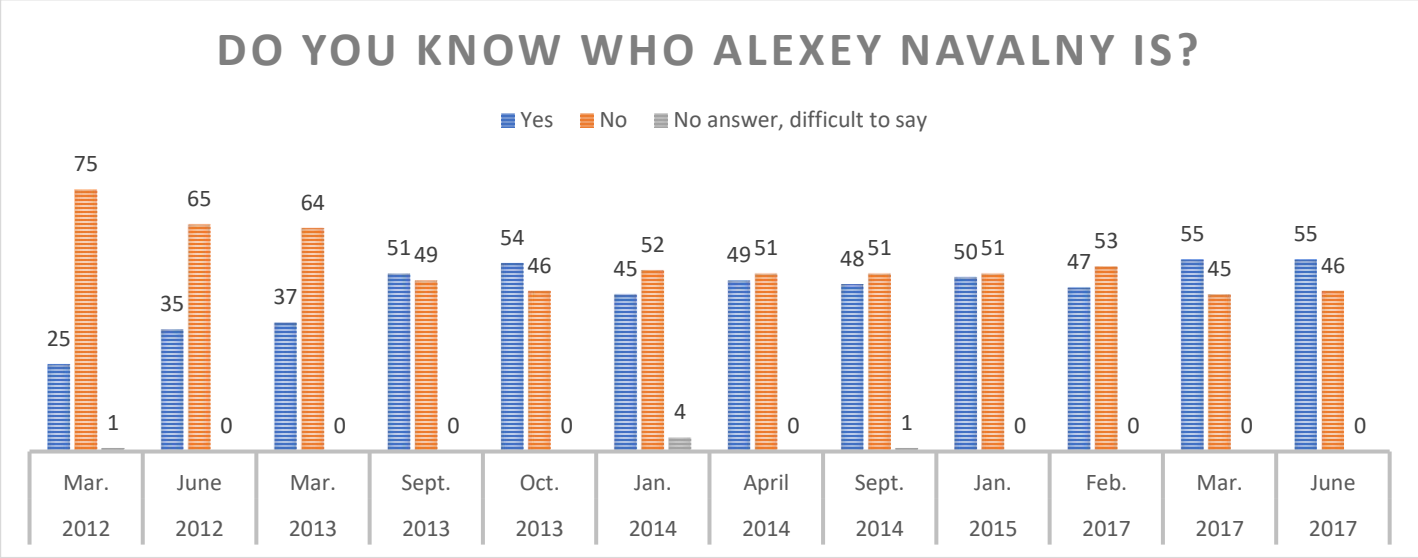


Figure 3: Navalny name recognition from the Levada Center

Authorities applied broad interpretations of laws from the Administrative and Criminal Codes in an attempt to stifle campaign rallies and messages. The second largest category of

[7] "Numbers represent search interest relative to the highest point on the chart for the given region and time. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means there was not enough data for this term" (*Google Trends*, n.d.-a)

repressive actions overall was related to offensive and extremist material (12 of 51 instances). Prior to October 2017, most legal mechanisms used to stifle campaign activities were related to offensive and extremist materials or campaign laws in addition to coercion and harassment of supporters. Articles 280 and 282 of the Criminal Code (Public Appeals for the Performance of Extremist Activity and Incitement of Hatred or Enmity, as Well as Abasement of Human Dignity) were two popular ways to repress campaign related activity. Authorities also cited Articles 20.29 and 20.3 (Production and Dissemination of Extremist Materials and Displaying Fascist Attributes and Symbols) as further reasons to punish Navalny volunteers and supporters. Again, the Doctrine of Information Security classifies the internet as a means of spreading extremist or unlawful material detrimental to national security (*Doctrine of Information Security*, 2016).

Of 11 instances of repression between March and June 2017, five were related to extremism or offensive material, and, during this time, public opinion also seems to be preoccupied with national security related concerns. In March and June 2017, 28% and 30% of Levada survey respondents believed that Navalny was publishing FBK investigations in the interest of the West while only 12% believed he did so in the interest of Russia (*Protesty i Naval'nyĭ*, 2017). In December of that year, a month which also saw authorities use extremism laws as a method of electoral repression, 2% of Levada respondents affirmed that Russia's enemies included "the political opposition/the fifth column/Navalny" (*Enemies*, 2018). This is the first year Navalny was mentioned by respondents, who were asked this question only if they believed Russia had enemies and provided names without prompting. It is largely reflective of the Kremlin's ability to manipulate public opinion in the broader information space. Throughout his campaign, Navalny presented himself as modern and Westernized, a position in direct

contrast with the Kremlin's anti-American media strategy (Cottiero et al., 2015; Dollbaum & Semenov, 2021; Pomerantsev, 2015).

18 instances of repression were related to protest activity, with half being specifically tied to Article 20.2 of the Administrative Code (Violating the Established Procedure for Arranging or Conducting a Meeting, Rally, Demonstration, Procession or Picket). Article 19.3. (Failure to Follow a Lawful Order of a Police Officer) was another frequent charge. Other instances referenced activity that had not been formally coordinated with officials without naming specific laws or articles of the Administrative Code. The majority of these instances occurred from October 2017 onward, corresponding with Navalny's October arrest and call for an election boycott in January. In November of that year, 10% of Levada survey respondents stated they did not trust Navalny, while 2% did (*Political Trust*, 2019). In May 2016, August 2017 and January 2018—dates for which there is available data—voters willing to cast a ballot for Navalny hovered around 1% (*Russian Presidential Elections*, 2019).

Despite an overall upward trend beginning in 2013 of Russians getting their news from either internet publications or social networking sites, from July 2016 to March 2018, there was a slight decrease in survey respondents claiming to stay informed via these sources (*Istochniki*

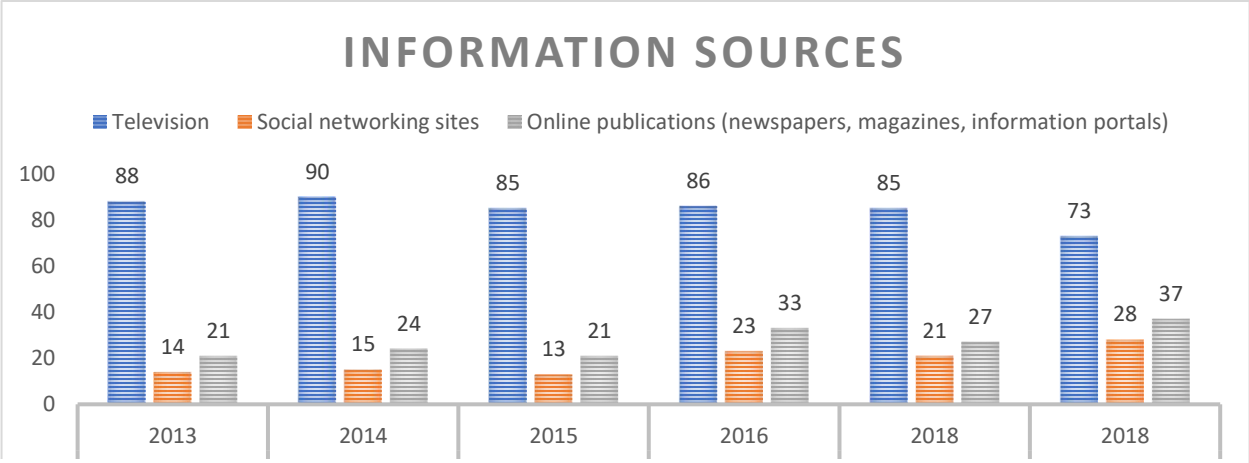


Figure 4: Information Sources from the Levada Center

informat͡sii, 2020). This is problematic since mainstream media shun Navalny and his support originates from online campaigning.

Overall, Navalny's name recognition increased by eight percentage points early in his campaign but was still within ranges seen in previous years. At one point, around 30% of survey respondents believed Navalny was acting in the interests of the West, and, for the first time, survey takers listed Navalny as an enemy of Russia.10% of voters distrusted Navalny, and, per polling data, the percentage of voters willing to vote for him remained stable throughout the campaign. Over the course of his campaign, the number of Russians getting news from online sources—the media platform most accessible to him—decreased. Given this data, it seems that there is an association between government internet controls used to repress his campaign and his ability to attract more supporters.

These findings seem to indicate that networked authoritarianism in Russia is part of a larger, overall information control policy needed to consolidate power, and Russian citizens themselves are complicit in the Kremlin's efforts. Rather than resort to outright violent repression, Putin has sought to persuade Russian voters that it is external forces at the root of social and economic problems versus regime corruption and ineptitude (Treisman, 2018, p. 14). As noted by scholars Guriev and Treisman, "competent dictators do not need to use repressions," as doing so publicly exposes the dictator's incompetence and brings into question his regime legitimacy (Guriev & Treisman, 2015, p. 33; Treisman, 2018, p. 14). Putin has instead sought to shape public perception through control of political information flows (Treisman, 2018, pp. 13–14). By limiting negative press rather than the supply of information itself (Morgus, 2018, p. 90), the Putin regime is able to cultivate an environment ostensibly free of restrictions in which it is possible to access a range of content, including that which may be critical of the government,

while at the same time promoting government narratives (Kerr, 2018). Russia is adept at pro-regime content production and narrative manipulation (Kerr, 2018, pp. 67–68), which seems to have had positive effects regarding Putin's approval ratings (Lipman et al., 2018, p. 185).

By reclaiming control over the internet, the state is able to limit alternative agendas and benefit from greater opportunities to manipulate public opinion (Kazun & Semykina, 2020). Although the information space remains less controlled than traditional media, coverage of current events is strikingly similar both online and in the press, and Vladimir Putin maintains a greater online presence than Navalny, the former being mentioned nearly four times as often as the latter (Kazun & Semykina, 2020). Despite more people turning to the internet to inform themselves, alternatives to state media have far lower readership, and users aren't necessarily turning to sources with views differing from state-sponsored ones (Denisova, 2017; Kazun & Semykina, 2020).

Furthermore, Russian citizens play an integral role in this effort to expand information control. Through their media choices, Russians help "to legitimize and normalize authoritarian power" (Robertson & Greene, 2017). Citizens' media choices are often determined by what are considered socially acceptable media consumption habits and political attitudes, which ultimately reinforce support for Putin (Robertson & Greene, 2017).

Government control of the information space and the reluctance of ordinary Russians to change their media consumption habits make attracting larger numbers of the general public to digital politics more difficult for opposition leaders and activists (Denisova, 2017). Navalny has been an outlier in that he was able to gain a stalwart online following despite a state-media ban and pro-government framing online and in the press. Yet, for digital resistance to connect with more people and truly take hold, opposition activists need greater media resources and

opportunities in addition to a societal shift in the majority's disinclination to seek out alternative points of view.

Limitations

Here it must be recognized that there are limitations to this study. First, data collection was conducted using open-source material. Only 51 instances of internet repression tied to the Navalny campaign were identified, but it is possible that others occurred and were never publicly reported. It is also conceivable that, given the types of repressive actions taken, some instances related to the Navalny campaign were not identified as such. The nature of second and third generation controls make their impact difficult to judge, considering their more abstract nature. Another limitation regarding the use of open-source data is that controlling for other factors that may have influenced voters was not possible. Additional factors swaying voters may have included disinterest in or dislike of Navalny's platform or a general increase in voter apathy. Moreover, when it comes to survey data, there is the issue of nonresponse bias and social desirability bias: it is impossible to know if Levada survey respondents answered sincerely. Moreover, under an authoritarian regime, some may have wished to respond differently but feared reprisals or other potential risks associated with giving a non-regime conforming answer.

Conclusion

This research aimed to identify how the Russian government leveraged state control of the internet to repress Navalny's 2018 presidential campaign as well as the impact of such control on said campaign. Based on open-source information collected from news articles and blogs as well as public opinion data, it can be concluded that the government relied on second and third generation internet controls, which likely contributed to Navalny's inability to attract

additional supporters from the general public. Here I identified five legal mechanisms used by authorities to stifle campaign activities in addition to the harassment of RuNet users. Most legal justification for repressing campaign activity was tied to protest activity and the dissemination of extremist or offensive material. The government was also able to "outsource" repression efforts via civil litigation. Navalny received a slight uptick in recognition in the early part of his campaign, but the percentage of citizens willing to vote for him remained steady throughout the course of the campaign. While this study was able to identify the major mechanisms of internet control used by the government, it was unable to control for certain factors such as overall voter apathy and opinions regarding Navalny's platform.

The Russian model of networked authoritarianism, part of the state's overall information control policy, continues to lean heavily on non-technical measures such as legislation, intimidation, and self-censorship norms to hinder opposition movements and limit dissent. The government's creation of a legal environment in which access to information can be restricted has been more subtle than outright filtering and aims to legitimize information control. Authorities also seek to discredit or demoralize opponents through coercion and harassment, ultimately leading to an overall climate of self-censorship. This confirms previous literature regarding government control of the RuNet (Deibert & Rohozinski, 2010; Maréchal, 2017; Morgus, 2018) and indicates that effective internet control does not require sophisticated technology. Further, exerting authority over the digital space is yet another way for the Putin regime to manipulate public opinion, control information flows and bolster regime legitimacy.

Since the 2018 election, the Russian government continues such attempts to exert control over the RuNet, and in some ways seems to be moving toward more first-generation style bans through blacklists (Maréchal, 2017, p. 36). In April 2018, authorities moved to block the popular

messaging app Telegram after the app refused to cooperate with the FSB by providing encryption keys needed to access user data, thereby violating anti-terrorism laws. Despite the ban, the app remained popular in Russia, and authorities were unable to block it fully for technical reasons (Lyons, 2020). The ban was lifted in 2020. However, this is indicative of the government's more serious tone regarding information control and a strengthening of Russian networked authoritarianism. Indeed, Russian authorities are seeking to create a political environment in which the Internet is carefully regulated so that citizens have the impression of being able to express themselves in limited ways without allowing dissent to take hold (Maréchal, 2017, p. 36).

Through the end of 2018, control of the internet in Russia followed a largely decentralized model, with a variety of political bodies promoting their own agendas and enforcing regulations (Nocetti, 2015, p. 118). Entities involved in internet governance include the presidential administration, the Ministry of Internal Affairs, Roskomnadzor, intelligence services, and local governments. In many ways, this has allowed for more flexible application of laws and other repressive measures, while also rendering user resistance and circumvention more difficult (Ramesh et al., 2020, p. 13). Inconsistency in the application of laws may contribute to the development of self-censorship norms as methods of safely bypassing regulations become unclear.

Nevertheless, this decentralized approach may be changing. At the end of 2018, Putin signed legislation reforming Article 282 of the Criminal Code ("Putin Signs Law," 2018). A significant increase in Article 282 prosecutions raised questions within civil society regarding legal procedures and free speech, while simultaneously making authorities seem overly paranoid instead of capable and decisive (Pomeranz & Smith, 2018, p. 7). Reforms demonstrate that Putin

maintains far-reaching influence over legislative processes, while other references to extremism in Russian law still allow for significant flexibility in criminalizing online activity.

Additionally, in 2019, the Russian government passed several amendments to existing federal laws that ostensibly aim to protect the RuNet from external threats. These amendments require telecom operators to install state-owned equipment for traffic analysis and filtering within Russia, allow for Roskomnadzor to take over centralized control of telecommunications networks and lay the legal foundation for the creation of a separate Domain Name System (DNS), which would necessitate its own infrastructure. While authorities claim such measures are needed to protect Russian users and infrastructure from foreign, especially American, cyberattacks, they facilitate mass surveillance and censorship ("Struktura FSB predupredila ob ugroze," 2021). If attempts to create a "sovereign" RuNet are successful, perhaps this will be the fourth generation of internet controls.

Navalny himself continues to be a target of the government's repression efforts. In January 2021, Navalny returned to Russia after spending five months in Germany for medical treatment related to a nerve-agent poisoning. He was arrested upon his arrival, and protests began soon after. On January 21st, the Prosecutor General's Office of the Russian Federation released a statement regarding the upcoming protests, indicating that access to illegal information would be restricted. NetBlocks, a global internet monitor, subsequently reported a six-hour disruption in internet connectivity on January 23rd, the first day of the protests ("Internet Disrupted in Russia," 2021). Since then, Navalny's political network has been blacklisted for terrorist or extremist activity (*Perechen' Organizat͡siĭ i Fizicheskikh Lit͡s*, n.d.; Sauer, 2021).

While this study centers on the development of networked authoritarianism in the Russian Federation, this research also contributes to broader conversations about internet policies

across the globe. Unlike other networked authoritarian states, the expanding RuNet was long unaccompanied by strict online censorship and technical control measures (Tkacheva et al., 2013). This is in contrast to China, where early anticipation of online activism prompted the government to leverage more technical control much sooner (MacKinnon, 2012). Authorities are able to block sites directly thanks to the limited number of gateways where the global internet and the Chinese internet connect, and routers are configured to filter out politically sensitive terms or specific websites; Western online platforms such as search engines or social media sites are either unavailable or highly monitored (MacKinnon, 2012). Contrary to the RuNet, the Chinese internet has developed enough that there is little objection when it comes to restricting access to the global internet (MacKinnon, 2012). While Freedom House ranks both countries as "Not Free" in their Freedom on the Net 2020 report, China ranks 20 points below Russia (*China: Freedom on the Net*, 2020; *Russia: Freedom on the Net*, 2020). Both countries have seen decreasing levels of internet freedom since 2016, but Russia has seen a yearly point-by-point drop from 35 to 30 (out of 100), while China has fluctuated between 10 and 13. This indicates that, while more forward-thinking authoritarian governments, such as China's, have been able to maintain tighter control over the digital space for longer, it is possible for countries with wider internet freedoms to backslide into networked authoritarianism. Indeed, Russia's non-technical methods of internet control are more easily adoptable than more technical ones.

Although surveillance is often associated with authoritarian or hybrid regimes, democratic governments also seek to maintain some control over their citizenry, often in the name of national security. The French government has recently sought the authority to force telecommunications companies to monitor telephone and internet traffic to aid in anti-terrorist measures (Meichtry & Schechner, 2021). In the United States, the 2001 Patriot Act expanded

government authority to monitor telecommunications data, and the Biden administration has recently indicated it may partner with private companies to gather information from private messaging apps to monitor extremist groups (Cohen & Williams, 2021).

While not within the scope of this paper, such developments offer additional avenues for future research on networked authoritarianism and global internet policies at large. Government efforts to control the online space are reflective of the internet's far-reaching role in facilitating information exchange and promoting resistance. Although efforts to restrict internet freedoms may dissuade some RuNet users, others may feel more motivated to mobilize and advocate for political change. At the government level, Russian policy may influence the policies of other authoritarian governments, whether former Soviet republics or not. Finally, in what ways may the policies of democratic governments mirror those of authoritarian regimes and what does this mean for the future of free speech or other civil liberties?

References

53 stol'ko raz, po mneniiu zavucha gimnazii №46 v Cheboksarakh, nado podumat', prezhde chem vstupat' v gruppy Naval'nogo v cotsetiakh. (2017, December 1). Mediazona. https://zona.media/number/2017/12/01/cheboksary-1937

Aleksey Navalny. (2017, March 20). [Polling Results]. Levada Center. https://www.levada.ru/en/2017/03/20/aleksey-navalny/

Alexanyan, K., Barash, V., Etling, B., Faris, R., Gasser, U., Kelly, J., Palfrey, J. G., & Roberts, H. (2012). Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere (SSRN Scholarly Paper ID 2014998). Social Science Research Network. https://papers.ssrn.com/abstract=2014998

Blogera v Krasnodare prigovorili k 10 sutkam aresta za rolik c prizyvom byĭti na miting. (2017, October 5). OVD-Info. https://ovdinfo.org/express-news/2017/10/05/blogera-v-krasnodare-prigovorili-k-10-sutkam-aresta-za-rolik-s-prizyvom

Blokirovka saĭta Naval'nogo. (2018, February 15). Mediazona. https://zona.media/chronicle/navalny-block

Bourgelais, P. (n.d.). Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia. Access, 14.

Bushuev, M. (2020, July 22). Delo protiv FBK Naval'nogo—Mest' za protesty v Moskve? Deutsche Welle. https://www.dw.com/ru/delo-protiv-fbk-navalnogo-mest-za-protesty-v-moskve/a-54257335

Channels of information. (2018, October 12). [Polling Results]. Levada Center. https://www.levada.ru/en/2018/10/12/channels-of-information/

Chikov, P. (2016, February 10). K reshcniiu suda o likvidatsii "Agory." SPCH. http://president-sovet.ru/members/blogs/post/1953/

China: Freedom on the Net 2020 Country Report. (2020). Freedom House. https://freedomhouse.org/country/china/freedom-net/2020

Chto proiskhodit i chto delat'. (2017, October 4). Naval'nyĭ. https://navalny.com/p/5576/

Clinton, H. R. (2010, January 21). Remarks on Internet Freedom. //2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Cohen, Z., & Williams, K. B. (2021, May 3). Biden team may partner with private firms to monitor extremist chatter online. CNN. https://www.cnn.com/2021/05/03/politics/dhs-partner-private-firms-surveil-suspected-domestic-terrorists/index.html

Cottiero, C., Kucharski, K., Olimpieva, E., & Orttung, R. W. (2015). War of words: The impact of Russian state television on the Russian Internet. Nationalities Papers, 43(4), 533–555. https://doi.org/10.1080/00905992.2015.1013527

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & OpenNet Initiative. (2010). Access controlled: The shaping of power, rights, and rule in cyberspace. MIT Press.

Deibert, R., & Rohozinski, R. (2010). Control and Subversion in Russian Cyberspace. In Access controlled: The shaping of power, rights, and rule in cyberspace. MIT Press.

DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press. https://ebookcentral-proquest-com.offcampus.lib.washington.edu/lib/washington/detail.action?docID=3421344

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

Doctrine of Information Security of the Russian Federation. (2016, December 5). https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Dollbaum, J. M. (2020). Protest trajectories in electoral authoritarianism: From Russia's "For Fair Elections" movement to Alexei Navalny's presidential campaign. Post-Soviet Affairs, 36(3), 192–210. https://doi.org/10.1080/1060586X.2020.1750275

Dollbaum, J. M., & Semenov, A. (2021). Navalny's Digital Dissidents: A New Dataset on a Russian Opposition Movement. Problems of Post-Communism, 1–10. https://doi.org/10.1080/10758216.2021.1893123

Dollbaum, J. M., Semenov, A., & Sirotkina, E. (2018). A top-down movement with grass-roots effects? Alexei Navalny's electoral campaign. Social Movement Studies, 17(5), 618–625. https://doi.org/10.1080/14742837.2018.1483228

Domeny Rossii. (n.d.). [Website Data]. Tekhnicheskiĭ T͡sentr internet. Retrieved April 18, 2021, from https://statdom.ru/

Enemies. (2018, February 2). [Polling Results]. Levada Center. https://www.levada.ru/en/2018/02/02/enemies/

Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. Journal of Information Technology & Politics, 1–16. https://doi.org/10.1080/19331681.2021.1905972

Ermoshina, K., & Musiani, F. (2017). Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. Media and Communication, 5(1), 42–53. https://doi.org/10.17645/mac.v5i1.816

Ferrari, A. (2018). Russia 2018. Predictable elections, uncertain future. Ledizioni. https://doi.org/10.14672/67057054

Gaĭnutdinov, D., & Chikov, P. (2013). Rossi͡a kak global'naya svobodnomu Internetu. Agora. http://www.ihahr-nis.org/sites/default/files/files/agora_internet_2012.pdf

Gaĭnutdinov, D., & Chikov, P. (2017). Rossi͡a. Svoboda interneta 2016: Na voehhom polozhenii. Agora.

Google Trends. (n.d.-a). [Web Search Trends]. Google Trends. Retrieved May 6, 2021, from https://trends.google.com/trends/explore?date=2012-01-01%202018-12-31&geo=RU&q=%D0%9D%D0%B0%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9

Google Trends. (n.d.-b). [YouTube Search Results]. Google Trends. Retrieved May 6, 2021, from https://trends.google.com/trends/explore?date=2012-01-01%202018-12-31&geo=RU&gprop=youtube&q=%D0%9D%D0%B0%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9

Guriev, S., & Treisman, D. (2015). How Modern Dictators Survive: An Informational Theory of the New Authoritarianism (No. w21136; p. w21136). National Bureau of Economic Research. https://doi.org/10.3386/w21136

Human Rights Court Says Navalny Unfairly Convicted In "Yves Rocher Case." (2017, October 17). RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/aleksei-oleg-navalny-yves-rocher-case-echr-unfairly-convicted/28799784.html

"I͡andeks.Den'gi" otkli͡uchili koshelek dli͡a sbora sredctv na kampanii͡u Naval'nogo. (2017, February 6). Meduza. https://meduza.io/news/2017/02/07/yandeks-dengi-otklyuchili-koshelek-dlya-sbora-sredstv-na-kampaniyu-navalnogo

International Human Rights Group Agora. (n.d.). International Network of Civil Liberties Organizations. Retrieved June 3, 2021, from https://www.inclo.net/members/agora/

Internet disrupted in Russia amid opposition protests. (2021, January 23). NetBlocks. https://netblocks.org/reports/internet-disrupted-in-russia-amid-opposition-protests-98aRXQAo

Internet Freedom and Business and Human Rights Section. (2017, November 27). [Government Website]. United States Department of State. https://2017-2021.state.gov/internet-freedom-and-business-and-human-rights-section/

Internet v Rossii: Dinamika proniknoveni͡a. Leto 2016. (2016, October 18). https://fom.ru/SMI-i-internet/13021

Internet v Rossii: Dinamika proniknoveni͡a. Osen' 2012. (2012, December 18). FOM. https://fom.ru/Proniknovenie-interneta/10738

Istochniki informat͡sii. (2020, September 28). [Polling Results]. Levada Center. https://www.levada.ru/2020/09/28/ggh/

Jee, C. (2019, March 21). Russia wants to cut itself off from the global internet. Here's what that really means. MIT Technology Review. https://www.technologyreview.com/2019/03/21/65940/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/

Kalathil, S., & Boas, T. C. (2002). Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule. Brookings Institution Press. http://ebookcentral.proquest.com/lib/washington/detail.action?docID=1123675

Kazun, A. (2019). To cover or not to cover Alexei Navalny in Russian media. International Area Studies Review, Vol. 22(4), 312–326. https://doi.org/10.1177/2233865919846727

Kazun, A., & Semykina, K. (2020). Presidential Elections 2018: The Struggle of Putin and Navalny for a Media Agenda. Problems of Post-Communism, 67(6), 455–466. https://doi.org/10.1080/10758216.2019.1685893

Kerr, J. (2018). The Russian Model of Digital Control and Its Significance. In N. D. Wright (Ed.), Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives (pp. 62–74). Air University Press. https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0161_WRIGHT_ARTIFICIAL_INTELLIGENCE_CHINA_RUSSIA_AND_THE_GLOBAL_ORDER.PDF

Kodeks RF ob administrativnykh pravonarusheniiakh. (2001, December 30). Konsul'tantPli͡us. https://www.consultant.ru/document/cons_doc_LAW_34661/

Kovaleva, N. (2018). Russian Information Space, Russian Scholarship, and Kremlin Controls. Defence Strategic Communications, 4(1), 133–171. https://doi.org/10.30966/2018.RIGA.4.5.

Kozenko, A. (2016, February 16). First blacklisted and now banned: Meet 'Agora,' the first of Russia's 'foreign agents' to be liquidated. Meduza. https://meduza.io/en/feature/2016/02/17/first-blacklisted-and-now-banned

Lidera PARNASa v Arkhangel'ske oshtafovali za rolik Naval'nogo. (2017, April 11). Kasparov.ru. http://www.kasparov.ru/material.php?id=58EBCD1EE35DD&utm_source=feedburner&utm_medium=twitter&utm_campaign=Feed%3A+kasparov%2FLoFO+%28%D0%9A%D0%B0%D1%81%D0%BF%D0%B0%D1%80%D0%BE%D0%B2.Ru%29

Lipman, M., Kachkaeva, A., & Poyker, M. (2018). Media in Russia: Between Modernization and Monopoly. In D. Treisman (Ed.), The New Autocracy: Information, Politics, and Policy in Putin's Russia (pp. 159–190). Brookings Institution Press.

Lyons, K. (2020, June 18). Russia lifts its ban on the Telegram messenger app. The Verge. https://www.theverge.com/2020/6/18/21295535/russia-telegram-ban-lifted-security

MacKinnon, R. (2012). Consent of the Networked: The Worldwide Struggle For Internet Freedom. Basic Books. http://ebookcentral.proquest.com/lib/washington/detail.action?docID=868682

MacKinnon, R. (2010). Networked Authoritarianism in China and Beyond: Implications for global Internet freedom. 31.

Maréchal, N. (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. Media and Communication, 5(1), 29–41. https://doi.org/DOI: 10.17645/mac.v5i1.808

Medvedev poruchil sokratit' stoimost' podkl͡iuchenia͡ k internetu v Rossii. (2013, January 21). RIA Novosti. https://ria.ru/20130121/918943794.html

Meet the 25 Most Influential People on the Internet. (2017, June 26). Time. https://time.com/4815217/most-influential-people-internet/

Meichtry, S., & Schechner, S. (2021, April 28). France's Macron Eyes Artificial Intelligence to Monitor Terrorism. Wall Street Journal. https://www.wsj.com/articles/frances-macron-seeks-broader-counterterror-surveillance-11619629713

Morgus, R. (2018). The Spread of Russia's Digital Authoritarianism. In N. D. Wright (Ed.), Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives (pp. 89–97). Air University Press. https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0161_WRIGHT_ARTIFICIAL_INTELLIGENCE_CHINA_RUSSIA_AND_THE_GLOBAL_ORDER.PDF

Mueller, M. (2017). Will the Internet Fragment? Polity Press.

Navaln'nomu dali 20 sutok aresta. Ego obrashchenie v sude. (2017, October 2). Naval'nyĭ. https://navalny.com/p/5575/

Navalny's Campaign 2018. How it was. (n.d.). Naval'nyĭ20!8. Retrieved February 22, 2021, from https://2018.navalny.com

Nocetti, J. (2015a). Contest and conquest: Russia and global internet governance. International Affairs, 91(1), 111–130. https://doi.org/10.1111/1468-2346.12189

Nocetti, J. (2015b). Russia's "dictatorship-of-the-law" approach to internet policy. Internet Policy Review, 4(4). https://doi.org/10.14763/2015.4.380

Nocetti, J. (2018). Cyber Power. In A. P. Tsygankov (Ed.), Routledge Handbook of Russian Foreign Policy (pp. 182–198). Taylor & Francis Group.

Ognyanova, K. (2010). Careful What You Say: Media Control in Putin's Russia – Implications for Online Content. International Journal of E-Politics, 1(2), 1–15. https://doi.org/10.4018/jep.2010040101

Pavel Chikov. (n.d.). Wilson Center. Retrieved June 3, 2021, from https://www.wilsoncenter.org/person/pavel-chikov

Perechen’ organizat͡siĭ i fizicheskikh lit͡s, v otnoshenii kotorykh ime͡iut͡sia svedeni͡ia ob ikh prichastnosti k ekstremictckoĭ de͡iatel’nosti ili terrorizmu. (n.d.). Rosfinmonitoring. Retrieved May 6, 2021, from https://www.fedsfm.ru/documents/terr-list

Placek, M. (2019). Social media and regime support in Russia: Does it matter which website is used? East European Politics, 35(4), 496–516. https://doi.org/10.1080/21599165.2019.1658078

Political trust. (2019, November 11). [Polling Results]. Levada Center. https://www.levada.ru/en/2019/11/11/political-trust/

Pomerantsev, P. (2015). Authoritarianism Goes Global (II): The Kremlin’s Information War. Journal of Democracy, 26(4), 40–50. https://doi.org/10.1353/jod.2015.0074

Pomeranz, W. E., & Smith, K. E. (2018). A Traditional State and a Modern Problem: Russia Rewrites its Internet Extremism Laws. Kennan Cable, 39, 10.

Pristavy oshtrafovali Naval’nogo eshchë na 5 tys rub iz-za rolika pro Usmanova. (2018, February 16). RAPSI. http://rapsinews.ru/moscourts_news/20180216/281968446.html

Protesty i Naval’nyĭ. (2017, July 17). [Polling Results]. Levada Center. https://www.levada.ru/2017/07/17/protesty-i-navalnyj/

Putin signs law partially decriminalizing Article 282 of Russian Criminal Code on extremism. (2018, December 28). Interfaks. https://interfax.com/newsroom/top-stories/21714/

Ri͡abova, I. (2017, October 11). Servis 2GIS udalil s kart adresa predvybornykh shtaba Naval’nogo. https://republic.ru/posts/86949

Robertson, G., & Greene, S. (2017). How Putin Wins Support. Journal of Democracy, 28(4), 86–100. https://doi.org/10.1353/jod.2017.0069

Roudik, P. (2020). Legal Provisions on Fighting Extremism: Russia [Web page]. Law Library of Congress. https://www.loc.gov/law/help/fighting-extremism/russia.php#_ftn28

Russia: Freedom on the Net 2020 Country Report. (2020). Freedom House. https://freedomhouse.org/country/russia/freedom-net/2020

Russia: Halt Orders to Block Online Media. (2014, March 23). Human Rights Watch. https://www.hrw.org/news/2014/03/23/russia-halt-orders-block-online-media

Russia internet blacklist law takes effect. (2012, November 1). BBC News. https://www.bbc.com/news/technology-20096274

Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election, Senate, 116th Congress 1st Session (2019). https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

Russian presidential elections. (2019, August 19). [Polling Results]. Levada Center. https://www.levada.ru/en/2019/08/19/russian-presidential-elections/

Russia's social networks users under martial law. (2017, February 7). Meduza. https://meduza.io/en/feature/2017/02/07/russia-s-social-networks-users-under-martial-law

Sauer, P. (2021, April 30). "End of an Era": Russia Adds Navalny Political Network to 'Terrorist and Extremist' List. The Moscow Times. https://www.themoscowtimes.com/2021/04/30/end-of-an-era-russia-adds-navalny-political-network-to-terrorist-and-extremist-list-a73796

Sivetc, L. (2019). State regulation of online speech in Russia: The role of internet infrastructure owners. International Journal of Law and Information Technology, 27(1), 28–49. https://doi.org/10.1093/ijlit/eay016

Smirnov, S. (2015, November 26). «Osoznannoe dopushchenie ugolovnogo dela I t͡iur'my». Mediazona. https://zona.media/article/2015/26/11/agora-international

Soshnikov, A., Napalkova, A., & Rustamova, F. (2019, February 5). Novyĭ khudshiĭ god. Glavnoe iz doklada o svobode interneta v Rossii. BBC News Russkai͡a sluzhba. https://www.bbc.com/russian/features-47123831

Stone, P. (2019, January 29). Is Oleg Deripaska the missing link in the Trump-Russia investigation? The Guardian. http://www.theguardian.com/world/2019/jan/29/oleg-deripaska-paul-manafort-trump-russia-investigation

Struktura FSB predupredila ob ugroze v svete zai͡avleniĭ CSHA. (2021, January 22). Interfaks. https://www.interfax.ru/russia/746316

Suleĭmanov, S. (2018, February 4). Osnovnaya mishen' – pol'zobateli Glavnoe iz doklada "Agori" o svobode interneta v Rossii. Meduza. https://meduza.io/feature/2018/02/05/osnovnaya-mishen-polzovateli

Sulim, S. (2017, April 12). Studentam prodolzhai͡ut ugrozhat' otchisleniem za uchastie v akt͡sii͡a 26 marta. Eshchë tri istorii. Meduza. https://meduza.io/feature/2017/04/13/studentam-prodolzhayut-ugrozhat-otchisleniem-za-uchastie-v-aktsiyah-26-marta-esche-tri-istorii

The Anti-Corruption Foundation. (n.d.). Retrieved February 22, 2021, from https://fbk.info/?lang=en

The number of Internet users. (2018, November 14). [Polling Results]. Levada Center. https://www.levada.ru/en/2018/11/14/the-number-of-internet-users/

The Yarovaya Law: One Year After (Information Security Series). (2017). Digital Report Analytica. https://analytica.digital.report/wp-content/uploads/2017/07/The-Yarovaya-Law.pdf

Tkacheva, O., Schwartz, L. H., Libicki, M. C., Taylor, J. E., Martini, J., & Baxter, C. (2013). Internet Freedom & Political Space. RAND Corporation.

Treisman, D. (2018). The New Autocracy: Information, Politics, and Policy in Putin's Russia. Brookings Institution Press. http://muse.jhu.edu/book/57413

T͡soĭ, I. (2017a, July 8). V Ti͡umeni zaderzhali prokhozhego, kotoryĭ snimal razgovor poliT͡seĭskikh s aktivistom, razdai͡ushchim listovki za Naval'nogo. The Insider. https://theins.ru/news/63350

T͡soĭ, I. (2017b, September 23). Glavnyĭ redaktor "Sib.fm" uvolilsi͡a iz izdanii͡a. Emu zapretili picat' o mitinge Navalnogo. The Insider. https://theins.ru/news/72144

UK RF Stat'i͡a 354.1 Reabilitat͡siia nat͡sizma. (2014, May 5). Konsul'tantPli͡us. https://www.consultant.ru/document/cons_doc_LAW_10699/be763c1b6a1402144cabfe17a0e2d602d4bb7598/

Upadhyay, A. (2018). Decoding Russia's 2018 Presidential Elections. International Studies, 55(3), 271–277. https://doi.org/10.1177/0020881718796986

Volkov, D., & Goncharov, S. (2014). Rossiĭskiĭ Media-Landshaft: Televidenie, Pressa, Internet (p. 15). The Levada Center. https://www.levada.ru/sites/default/files/levadareportmedia.pdf

What is Cybersecurity? (2019, November 14). Cybersecurity & Infrastructure Security Agency. https://us-cert.cisa.gov/ncas/tips/ST04-001

White, S., & McAllister, I. (2014). Did Russia (Nearly) have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism. Politics, 34(1), 72–84. https://doi.org/doi:10.1111/1467-9256.12037

Zamdirektora shkoly vo Vladimire prigrozila uchenikam iz"i͡atiem iz sem'I posle foto v shtabe Naval'nogo. (2017, May 2). Mediazona. https://zona.media/news/2017/02/05/family