The Battle for the Internet:

The Kremlin V. the People

Diana Hajali

INTRODUCTION

Russia emerged after the fall of the Soviet Union in 1991 as a presidential republic based on democracy, free elections, and the division of power. Yet Russia has exhibited authoritarian tendencies since President Vladimir Putin's rise to power, including a heightened security force, electoral fraud, political corruption, the suppression of political and civil dissent, and state control of information. The most recent Russian presidential election in 2018 publicly highlighted the Kremlin's practice of bending the law to maintain the current regime, as well as Russian citizens' awareness of and intolerance for further corruption. One of Putin's political opponents, anti-corruption activist Alexei Navalny, was barred from competing in the election due to a previous conviction altered by the Kremlin. Unhappy with Putin's easy reelection and the Kremlin's attitude toward any opposition to the regime, people took to the streets to protest. Although Putin's Russia has made it more difficult for democracy to flourish, the population has found ways to keep it alive through large protest movements and free speech aided by the internet and social media.

Control of information took place prior to the formation of the Soviet Union. However, stricter government efforts to control information began around the 1950s and have only increased and transformed with the introduction and expansion of the internet. Putin, who tends to have a KGB mindset, believes that the internet was created by the West as a method to sway other countries' populations, and that a severe level of control is necessary not only to protect Russia from any external cyberattacks, but to prevent U.S. influence from taking hold. Therefore, the Kremlin today, backed by the Federal Security Service (FSB), the successor to the KGB, controls the spread of information through surveillance, internet legislation, pressure on internet service providers (ISPs), propaganda, state-controlled media, and the use of the internet itself as a weapon. Defense against this control exists in the form of independent companies, non-compliant ISPs, international social media companies, and Russia's own youth. Other factors, including the Kremlin's inability to account for all internet and social media users' activity, and its struggle to keep up with new technologies, also pose a challenge. This paper begins by outlining the start of information control under the Soviet Union, then describes the development and control of the internet post-1991, and then discusses the new forms of internet control under Putin. This paper also identifies opposition forces and how they challenge Putin's efforts to

control the internet, as well as outlines the Kremlin's own shortcomings. Finally, the paper concludes by evaluating potential outcomes for Russia's future, specifically whether the regime or the internet will prevail.

THE HISTORY AND EVOLUTION OF INFORMATION CONTROL

In 1702, *Vedomosti*, Russia's first newspaper, was used as a tool of political propaganda to spread the czar's plans and to build his popular support.[1] During the Russian Empire, media in the form of books, newspapers, music, and art was censored by the emperor or his delegations. By the nineteenth century, censorship powers were handed to the Ministry of Internal Affairs. Once the Bolsheviks seized power in 1917, the Soviet government passed a law to limit free speech by prohibiting the publication of any critical articles. Censorship further increased under Joseph Stalin through intense control over which books could be read, but people opposed to censorship were able to circulate handmade copies of the books. Media control expanded under Leonid Brezhnev, briefly relaxed under Mikhail Gorbachev, and returned with a modern twist under Vladimir Putin.[2]

The Soviet Union's Tight Grasp

Information during the Soviet era was viewed as a danger rather than a freedom, and was subject to tight control.[3] In the Soviet Union, media censorship was primarily done by Glavlit, a government agency created in 1922. Glavlit had the authority to censor the performing arts and any publications in order to suppress political dissidence.[4] Over the years, Glavlit became more pervasive, controlling not only hostile newspapers, but what items the post office could deliver, which books the libraries could put on display, and how erotic literature could be.[5] By 1961, Glavlit had the authority to control the communications of foreign correspondents in Moscow.

In 1947, a small village outside of Moscow, Marfino, was transformed into a secret research facility known as a *sharashka* – a camp in which scientist prisoners worked to develop technology for the state. In the 1950s, the Marfino project worked with the secret police to provide telephone technology for Stalin, and it succeeded at catching foreign spies through the interception of phone calls. Another compound, named Kuchino, opened in 1953 and became the

KGB's "main research center for surveillance technologies, including the all-pervasive system of phone tapping and communications interception."[6] The KGB played a large role in preventing the spread of information, and would often have its officers sit for hours listening to a multitude of phone recordings and transcribing the conversations. The KGB was especially quick to act when it found dissidents exchanging information over the phone. The secret research facilities thus served the KGB's purpose of controlling all information flow in the Soviet Union and suppressing any opposition, but other media developments in the 1950s presented both new challenges and new opportunities for control.

Vladimir Fridkin developed the Soviet Union's first photocopying machine in 1952 and soon after, the ministry ordered it into mass production. Five years later, a female KGB employee told Fridkin that the machine had to be destroyed due to its capability to copy prohibited materials. The copying machine was completely destructed, illuminating the Communist Party's paranoia and its power over the spread of information. Even later, when photocopying became a routine practice, the Soviet Union kept photocopiers locked in specific offices, staffed by a designated operator and placed under watchful KGB surveillance. After Stalin's death in 1953, the totalitarian system of repression began to loosen as leader Nikita Khrushchev implemented reforms intended to reverse Stalin's fearful regime. However, this brief period of optimism did not last long.

In 1964, Khrushchev was replaced by Leonid Brezhnev, who ended reforms and tightened censorship. Under Brezhnev, the KGB was able to pass a new law that prohibited the use of international phone lines "in a manner contrary to the public interest and public order of the USSR," and had the power to turn off peoples' phone lines in the middle of their conversations.[7] This regulation was only halted ahead of the 1980 Olympic Games in Moscow, when the Soviet Union decided to increase the number of international lines and open an international telephone exchange station. Unfortunately, this positive change was reversed after the Olympics.

Mikhail Gorbachev became General Secretary of the Communist Party in 1985, and "by 1986 the Soviet Union had thirteen powerful long-range [radio] jamming stations, and local city jamming stations were established in eighty-one cities."[8] Though Gorbachev's policies of *glasnost* (openness) and *perestroika* (restructuring) signaled a more open Soviet Union, these changes were desperately needed in order to save the country from economic collapse.

Gorbachev's plan was for glasnost was "to allow more freedom while trying to maintain party control over what could be made public and what would still be decreed secret."[9] Yet once censorship eased, journalists began to test *glasnost's* limits, publishing books and articles that covered once-forbidden topics and a wide range of social problems, such as homelessness and pollution.[10] By 1991, the fall of the Soviet Union was accompanied by an explosive revival of journalism, visual media, and literature – information had finally broken free from its prison.

In 1989, a programming team at the Kurchatov Institute in Moscow built a computer network called Demos, a mobile operating system. The team later separated into two groups, with one group forming Demos as a "cooperative," or a private business, and the second remaining to create the network Relcom. Relcom connected to other research centers in Russia through e-mail exchange, and in 1990, "the very first Soviet connection to the global Internet was made when the Kurchatov programmers exchanged e-mails with a university in Helsinki, Finland."[11] Soon, the connection extended far beyond the borders of the Soviet Union, allowing for the circulation of political information on Russia. The KGB surprisingly did not intervene when Russia made its first connection to the internet. Although it was wary of the spread of information through the internet, the organization hardly understood it.[12]

Post-1991 Developments

By 1995, the rate of information sharing had accelerated rapidly. Demos had transformed into an ISP, and was making large profits by selling personal computers to Russians. Relcom, Demos, and other networks all passed through station M9 in the MSK-IX internet exchange point in Moscow. The Ministry of Security, the successor to the KGB, had been put in charge of intercepting phone calls and mail in 1992, but it could not keep up with the introduction of new forms of information sharing. The Ministry was restructured in 1995 due to Yeltsin's desire to create an intelligence service that more closely resembled the West. Therefore, the KGB was renamed the FSB, and the department once responsible for eavesdropping and cryptography became the Federal Agency for Government Communications and Information (FAPSI). At Yeltsin's decree, the FSB was given broader surveillance and interception powers.[13]

By 1997, the Russian internet had undergone explosive growth. The first search engine, Rambler.ru appeared, as well as the first political party website. Interfax news agency also

launched its own website and internet advertising became a paying business. Many new ISPs formed and the first blog in Russia, the Evening Internet, allowed for a quicker delivery of traditional print media to internet users. However, with the expansion of the internet also came a fight for control, as "oligarchs used their news media outlets as weapons to fight for control of the nation's vast resources."[14] Now the security services began to pay more attention to online activity, and decided that there needed to be an update to their surveillance methods in order to sufficiently control the spread of information.

As a measure to monitor the entire internet, the FSB introduced SORM (System of Operational-Investigatory Measures). While SORM had existed prior to 1995 in the form of phone call interception, the updated SORM (SORM2) required telecommunications operators to "install FSB-provided hardware allowing the agency to monitor users' communications metadata and content – including phone calls, email traffic, and web browsing activity."[15] The hardware, which resembled small electronic boxes, was located in phone station M9, where it gave FSB officers access to all of Russia's internet traffic. These "black boxes" were forced onto ISPs, which not only had to pay for SORM equipment and its installation, but had no access to any of its information.

SORM2 gave the FSB so much power that any internet provider that did not cooperate with its conditions was forced offline by the FSB, which also controlled ISP licensing procedures. In the late 1990s, many ISPs were shut down or had their finances frozen after refusing to provide client information to the FSB without a warrant. Also, as a result of the high cost of SORM equipment, small internet providers began going out of business, giving larger ISPs a greater market share. Though SORM was later revised so that the FSB would be required to obtain a warrant to access user's internet activity, the FSB did not always abide by the rule.[16]

In 1998, Anatoly Levenchuk, the founder of libertarian website, Libertarium.ru, posted a document online that revealed FAPSI's SORM plans. He then "launched a public campaign to call attention to the draft and, in a larger sense, to push back against SORM."[17] He met with news editors, telecom operators, and ISPs for interviews, and published articles online that revealed the black box's purpose to the rest of the world. Through his investigation, Levenchuk learned that the FSB's surveillance allowed it to interfere in politics by producing kompromat, or compromising material, that targeted "business rivals, prominent journalists, and politicians."[18]

Despite his efforts to bring SORM to public attention, Levunchuk could not get the large ISPs to support his cause, and he gave up fighting.

Putin, former director of the FSB, was appointed Yeltsin's prime minister in 1999, and was unaccustomed to the free exchange of information since he had been in Germany working for the KGB during the *glasnost* campaign. In 1999, the main Kremlin politicians saw all investigative and critical journalism as a threat and a conspiracy against them – especially NTV, a popular television channel that spotlighted Yeltsin's family corruption. While television dominated the media arena, a man named Gleb Pavlovsky used the internet to launch websites filled with kompromat aimed at anti-Kremlin businessmen and politicians. Pavlovsky also created a website, elections99.com, that "published real-time exit polls from the Russian regions" on Election Day.[19] The data provided on the website was disseminated by the media and may have swayed voters to support Putin's Unity Party. A few months later, Yeltsin announced Putin as his successor.

The Rise of Putin and the Internet

President Putin went to work on controlling television at once, sending in officers to raid media offices and detain their executives. Journalists and TV anchors were interrogated, NTV was closed down, and newspaper staffers were ejected from their offices. As television and the newspaper industry succumbed to government control, oligarchs turned to the internet and state-run media began to appear online. In the mid-2000s, media shifted from journalism to online blogging, where reports were "highly critical of Russian domestic policy."[20] LiveJournal emerged as one of the most popular blogging platforms during this time. The Kremlin, unhappy with the new form of media, had loyal oligarchs buy off or merge with blogging and news platforms.

When Dmitry Medvedev became president in 2008, the Russian search engine, Yandex, was the "ninth-largest search engine in the world."[21] Fear of a popular uprising was high so the FSB launched a program to monitor civil activity and to invest findings in a database on "would-be troublemakers."[22] The FSB then purchased surveillance technologies, such as drones, and placed them on modes of public transportation, using their database to target activists and prevent them from participating in demonstrations. This activity starkly contrasted Medvedev's

personal actions, such as his appearance in a television interview with TV Dozhd in 2011. That same year, Medvedev endorsed Putin for a return to the presidency, sparking anger and public protests during the 2012 election period.[23]

With Putin's return to the presidency in 2012, distributed denial of service (DDOS) attacks, advanced electronic surveillance, computer malware, and deep packet inspection (DPI) emerged as information controls used by the state to censor media and limit user's online rights. The 2011-2012 Arab Spring movement, which heavily utilized social media and the internet to garner support and organize demonstrations, increasingly made Putin see the internet as a threat to Russia's security. As a result, SORM was updated to include social networking sites.[24] Social media, which moves horizontally rather than vertically, does not have a hierarchical structure of leadership and thus challenges the regime.[25] The Arab Spring and the expansion of social media only served to further the Kremlin's paranoia.

In 2014, Putin stated that the internet was "a special project of the U.S. Central Intelligence Agency" and Russian "officials became increasingly outspoken about the need to protect the 'RuNet,' which refers to […] the segment of the internet where the Russian language and Cyrillic letters are used."[26] Therefore, measures were put in place to further control content for the protection of the state. Media content could be blocked by Roskomnadzor – the Federal Service for Supervision of Communications, Information Technology, and Mass Media – without a warrant. In 2014, Roskomnadzor created a list of blocked, or "blacklisted," websites featuring any banned or "extremist" content.[27] Though this fell under state control, ISPs were held legally responsible to prevent their users from accessing forbidden content by acquiring DPI technology, which filters data "sent from one computer to another over a network, and thus enables its users to track down, identify, categorize, reroute or stop internet traffic."[28] Another 2014 law required users to provide their personal information when signing on to public Wi-Fi or acquiring a SIM card so that the state could link their online activity to their identity.[29]

Recently, Russia has been attempting to control its own social media platforms, as well as global platforms, such as Google and Facebook. In 2018, Russia moved to ban the messaging app, Telegram, over 'terrorism' concerns. As a result, Roskomnadzor banned millions of IP addresses hosted by Telegram, but the move ended in failure because users were still able to use the app despite the ban.[30] On the international stage, the Kremlin has tried to pass an international law regulating the global internet, has interfered in post-Soviet states' internet, and

has pushed "for global companies to register in Russia and thereby become subject to Russian federal and regional legislation."[31] Many international companies have also been the target of Russian legislation requiring them to store user data in Russia.[32] For example, Roskomnadzor has pressured Facebook, Twitter, and Apple to locally store data, as this would give the government "access to encrypted communications."[33]

In November, 2019, the Russian government adopted a sovereign internet law aiming to disconnect the Russian internet from the global internet, furthering the Kremlin's control over the spread of information. The law not only expands on previous requirements for ISPs to buy and implement surveillance and filtering equipment, but it also gives Roskomnadzor the right to censor any information deemed a threat, without letting anyone know. It also goes beyond earlier methods of censorship by proposing a filter on Virtual Private Networks (VPNs), which are often used to bypass website blocking. In addition, it requires that all ISPs use a national domain name system (DNS), thereby creating an "address book of the internet" to connect users to their websites.[34] This allows for government manipulation of search results and other information. Finally, the sovereign internet law is riddled with vague terms lacking specific definitions in order to reduce transparency and avoid any legal opposition.[35] However, opposition to Russia's increased censorship of information exists in the form of its youth, independent media companies, and the challenges of controlling the internet.

DIGITAL REVOLUTIONARIES AND THE BARRIERS TO CONTROL

Russian Youth

While information in Russia has been tightly censored and manipulated for hundreds of years, the Kremlin now faces an unexpected opponent: Russian youth. In the past decade, young Russians have been incredibly active in protesting the government's policies and demanding that their voices be heard. In the 2019 summer protests in Moscow, "59 percent of protestors were thirty-five years old or younger, and 23 percent were twenty-five or younger."[36] Also, younger rally participants "were much more likely to use social media to gather information about the street actions."[37] Younger Russians simply consume information differently than older generations. Most Russian youth have an online presence through the internet or social media

and are "largely immune to the Kremlin's propaganda that flows from national TV networks."[38] This is because the digital sphere allows for information that fills the gap found between state-run information and information from a friend or an anti-regime website.[39]

A 2018 Levada Centre poll shows "that 90 percent of Russians aged 18-24 are daily internet users."[40] A 2017 study by Valeria Kasamara indicates that Russian college students' main news sources are social networks, such as VKontakte, Instagram, Facebook, and Google. While young Russians' news sources cater more to culture, entertainment, and music, rather than politics, their attachment to the internet and their tech-savviness serve as a direct counterweight to state efforts to censor information.[41] Yegor Zhukov is an example of Russia's youth turning to the digital arena to protest Kremlin policies. A university student, Zhukov had a YouTube channel with more than "100,000 subscribers on which he discussed the strategy of non-violent protests."[42] In the summer of 2019, Zhukov's doorbell rang and he was arrested by Russian police on charges of mass unrest for taking a part in protests to demand free and fair elections, a violation which carried a maximum sentence of eight years in prison.

Immediately following Zhukov's arrest, students and professors protested for his release, newspaper editors vouched for him, and famous rappers offered to post his bail. Zhukov's friends also turned to the internet to organize assistance for Zhukov, and they "set up a chat platform with tips for the parents of those who find themselves in pre-trial detention."[43] Neither Zhukov nor his friends were afraid of the government, representing what some call "youthful fearlessness" of the "Putin Generation."[44] Zhukov's arrest also sent a statement that Russia's youth is resistant to the Kremlin's intimidation tactics and that the internet is their domain. While Putin continues to try and connect with Russia's youth, the Kremlin's policies on internet censorship only serve to distance the youth further from the state.

Independent Media

Aside from Russia's youth, Russian independent media companies and ISPs also form a strong defense to the Kremlin's censorship controls. For instance, many urban-class Russians responded to the government's use of SORM by developing homegrown social media platforms.[45] The head of Golos, Russia's "only independent election watchdog organization," Grigory Melkonyants, began to gather information about election fraud from polling stations in

Russia in 2004.[46] Suddenly, in 2011, Golos came out with an updated system in which an "interactive digital map [marked] all questionable activity and violations in campaigns and during elections."[47] Melkonyants also wanted to publish fraud data and the interactive map online and, after partnering with Gazeta.ru, the map was available for online viewing by millions of people. Authorities were threatened by the map and made their own version, but no one trusted it. Pro-Kremlin "hacktivists also tried to compromise the Golos map by feeding it false information," but Melkonyants caught them in the act.[48] Finally, the authorities took down the map's banner, but other news organizations kept it visible online.

When citizens learned of the election fraud through Golos and through an undercover story published online by Ilya Azar, they took to the streets to protest. Police responded violently, arresting more than three hundred people, mostly activists, including Alexei Navalny. In response to the arrests, Grigory Okhotin and his brother began posting information on Facebook about "whom was arrested and where they were being held, […] using the hashtag OVD, meaning in Russian, the police station."[49] Before long, the Okhotin brothers launched a website, OVD-info, which "became a public forum for sharing information about Russian citizens detained during protests."[50] Facebook also became a popular spot for journalists and activists to plan protest movements. Even efforts by the Kremlin to prove that few people went to protests backfired when aerial drone shots taken of the demonstrations were published online, showing enormous crowds.[51] Clearly, independent journalists and activists were able to bypass government shutdowns of anti-government websites or blogs by creating their own independent sites and using social media to raise awareness and gather critical information.

Challenges to Information Control

The power of its citizens set aside, the Kremlin also faces challenges in its efforts to control information in the form of costs, limited reach, and the nature of the internet itself. Even in the early days of government surveillance, the security services struggled to use SORM to its full effectiveness. The Twelfth Department of the KGB, in charge phone call interception using SORM at the time, "could simultaneously wiretap no more than three hundred people. Twenty-four hours of eavesdropping produced between eight and eleven hours of recordings, but one hour of recording required seven hours of transcribing by controllers."[52] It was not until the

developments of new technologies that the Kremlin could more efficiently monitor its citizens' activity, but even then, the internet itself posed many challenges. First, the very nature of the internet makes it almost impossible to control. In 2016, 87.55 million Russians had access to the internet.[53] While the Kremlin has arrested influential anti-government bloggers or activists, such as Alexei Navalny, or carried DDOS attacks on popular sites, such as LiveJournal, the government does not have the capability to stop the entire population from discovering, creating, or sharing information.

The internet itself "enables users to create networks outside state control" and has an extremely low cost of production.[54] This makes it easy for users to cheaply upload YouTube videos, memes, and blogs that ridicule or criticize the government, with little consequence. Further, the internet transcends national borders, making information control near impossible. Though Russia has its own search engines and social media platforms, international companies such as Facebook and Google have an even stronger presence among internet users in the country. The Kremlin's attempts to control foreign-owned social media platforms and ISPs have mostly been unsuccessful.[55] Additionally, "96 percent of state institutions still use unapproved foreign software despite an attempt to move them on to domestically produced alternatives," further illustrating the Kremlin's inability to force compliance, even on their own institutions.[56]

While media and internet access come at a low cost to users, the information control systems the Kremlin has in place are expensive and resource-heavy. Not only do they require advanced technologies, but their intent is to monitor millions of users' activity, ensure ISP compliance with Russian legislation, and prevent dissidence, which incurs high costs. For instance, the cost of the project to disconnect the Russian internet from the global internet was initially set at $38 million, but estimates of the actual cost reach up to $304 million. Experts say that even a figure that large "won't be enough to get the system up and running, let alone maintain it."[57] When Russia's sovereign internet law was passed in November, it required ISPs to only use Russian exchange points and to submit to a global domain name system (DNS). While the details of the law's outcomes are unknown, the reconfiguration of "tens of thousands of systems necessitates the identification of "all the different access points citizens use to get online," some of which are abroad.[58] This is nearly impossible to accomplish, signifying again the costly struggle the Kremlin faces in attempting to control all information in Russia.

OUTLASTING CONTROL: THE FUTURE OF INFORMATION

Though Russia claims that its censorship controls and its desire to disconnect from the global internet are meant to protect the state from outside threats, such as cyberattacks, the Kremlin's underlying motive is self-preservation. Ever since the first newspaper in 1702, Russian leaders have, in one way or another, attempted to control the spread of information to maintain popular support and suppress dissidence. In the modern era, Putin has made significant strides in censoring information by jailing journalists, shutting down news agencies, and using advanced technologies to monitor Russian citizens. The passage of the sovereign internet law in November further serves Putin's purpose of maintaining control and preserving his regime, and signals a shift towards authoritarianism. Through the use of technology and the loyalty of various actors in the Kremlin, Putin has effectively created a system of control: the Russian parliament produces repressive legislation, pro-Kremlin hacktivists and trolls are hired to attack liberals online, security services spy on the opposition, Roskomnadzor has the power to censor and filter the internet, friendly oligarchs bankroll and take over media companies, and manufacturers provide surveillance equipment.[59]

Yet Putin's tactics, brutal as they may appear on the surface, are not fully effective. Internet filtering is easily bypassed by tech-savvy citizens, very few people are jailed for criticizing the government online, and media organizations are rarely shut down. Rather, the Kremlin relies on threats and intimidation to get ISPs and media companies to obey, but this does not always work. Rather, independent media companies often choose not to comply with the Kremlin's regulations, international companies refuse to heel to Russia, and citizens, especially the youth, find ways to access blocked information. This is because networks are horizontal, not vertical, and the internet is a powerful and uncontrollable force – facts which Putin and his close circle have never fully grasped.[60]

When evaluating potential outcomes of information control in the future, it is unlikely that the Kremlin will ever be able to fully prevent the spread of information in Russia. Due to the cost of ensuring compliance with internet regulations, the independence of international companies from Russian legislation, the resilience and knowledge of Russian youth, and the nature of the internet itself, it is more likely that information will run free. This presents a potential future complication for Putin, who may or may not seek to continue his rule in 2024.

However, this paper finds that opposition forces, and the internet itself, are too strong to fall prey to any plans that Putin or the Kremlin have for an authoritarian future. The regime may develop new methods of control, but they will never be effective enough to censor or monitor the activity of millions of users, or halt the spread of information.

[1] Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication, Vol. 5, Issue 1*, 2017. https://www.cogitatiopress.com/mediaandcommunication/article/view/808
[2] Yegorov, Oleg. "Soviet censorship: How did the USSR control the public?" *Russia Beyond*, 2017. https://www.rbth.com/arts/history/2017/06/27/soviet-censorship-how-did-the-ussr-control-the-public_790892
[3] Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication, Vol. 5, Issue 1*, 2017. https://www.cogitatiopress.com/mediaandcommunication/article/view/808
[4] Newth, Mette. "Forbidden Books and Newspapers." *Russia Beacon for Freedom*, 2002. http://www.beaconforfreedom.org/liste.html?tid=415&art_id=555
[5] Keller, Bill. "The Life of a Soviet Censor: Anything Goes? Not Just Yet." *The New York Times*, 1989. https://www.nytimes.com/1989/07/18/world/the-life-of-a-soviet-censor-anything-goes-not-just-yet.html
[6] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[7] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[8] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[9] Cooper, Ann. "The death of glasnost: How Russia's attempt at openness failed." *Committee to Protect Journalists*, 2015. https://cpj.org/2015/04/attacks-on-the-press-death-of-glasnost-russia-attempt-at-openness-failed.php
[10] Cooper, Ann. "The death of glasnost: How Russia's attempt at openness failed." *Committee to Protect Journalists*, 2015. https://cpj.org/2015/04/attacks-on-the-press-death-of-glasnost-russia-attempt-at-openness-failed.php
[11] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[12] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[13] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[14] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[15] Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication, Vol. 5, Issue 1*, 2017. https://www.cogitatiopress.com/mediaandcommunication/article/view/808
[16] Alexander, Marcus. "The Internet and Democratization: The Development of Russian Internet Policy." *The Journal of Post-Soviet Democratization*, 2004. https://www.researchgate.net/publication/250209496_The_Internet_and_Democratization_The_Development_of_Russian_Internet_Policy
[17] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[18] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[19] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[20] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[21] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[22] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[23] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[24] Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication, Vol. 5, Issue 1*, 2017. https://www.cogitatiopress.com/mediaandcommunication/article/view/808
[25] Gainous, Jason, Kevin M. Wagner and Charles E. Ziegler. "Digital media and political opposition in authoritarian systems: Russia's 2011 and 2016 Duma elections." *Democratization*, 2018. https://www.tandfonline.com/doi/abs/10.1080/13510347.2017.1315566
[26] Pallin, Carolina Vendil. "Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 2017. https://www.tandfonline.com/doi/abs/10.1080/1060586X.2015.1121712
[27] Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication, Vol. 5, Issue 1*, 2017. https://www.cogitatiopress.com/mediaandcommunication/article/view/808
[28] Nocetti, Julien. "Contest and conquest: Russia and global internet governance." *International Affairs*, 2015. https://www.chathamhouse.org/sites/default/files/field/field_publication_docs/INTA91_1_07_Nocetti.pdf

[29] Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication, Vol. 5, Issue 1*, 2017. https://www.cogitatiopress.com/mediaandcommunication/article/view/808
[30] Roth, Andrew. "Russia blocks millions of IP addresses in battle against Telegram app." *The Guardian*, 2018. https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app
[31] Pallin, Carolina Vendil. "Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 2017. https://www.tandfonline.com/doi/abs/10.1080/1060586X.2015.1121712
[32] Pallin, Carolina Vendil. "Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 2017. https://www.tandfonline.com/doi/abs/10.1080/1060586X.2015.1121712
[33] Sherman, Justin. "Russia's Domestic Internet is a Threat to the Global Internet." *Slate Technology*, 2019. https://slate.com/technology/2019/10/russia-runet-disconnection-domestic-internet.html
[34] "Russia: New Law Expands Government Control Online." *Human Rights Watch*, 2019. https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online
[35] "Russia: New Law Expands Government Control Online." *Human Rights Watch*, 2019. https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online
[36] Smyth, Regina and Sarah Oates. "Mind the Gaps: Media Use and Mass Action in Russia." *Europe-Asia Studies*, 2015. https://www.tandfonline.com/doi/abs/10.1080/09668136.2014.1002682
[37] Smyth, Regina and Sarah Oates. "Mind the Gaps: Media Use and Mass Action in Russia." *Europe-Asia Studies*, 2015. https://www.tandfonline.com/doi/abs/10.1080/09668136.2014.1002682
[38] Khvostunova, Olga. "Russian youth in the Moscow protests." *Atlantic Council*, 2019. https://atlanticcouncil.org/commentary/long-take/russian-youth-in-the-moscow-protests/
[39] Smyth, Regina and Sarah Oates. "Mind the Gaps: Media Use and Mass Action in Russia." *Europe-Asia Studies*, 2015. https://www.tandfonline.com/doi/abs/10.1080/09668136.2014.1002682
[40] Milov, Vladimir and Olga Khvostunova. "Russian Youth: A Look Inside the 'Black Box.'" *Free Russia Foundation*, 2019. https://www.4freerussia.org/russian-youth-a-look-inside-the-black-box/
[41] Milov, Vladimir and Olga Khvostunova. "Russian Youth: A Look Inside the 'Black Box.'" *Free Russia Foundation*, 2019. https://www.4freerussia.org/russian-youth-a-look-inside-the-black-box/
[42] Esch, Christian. "Russian Youth Stand Up to the State." *Spiegel Online*, 2019. https://www.spiegel.de/international/world/fearless-generation-in-russia-stands-up-to-the-kremlin-a-1285954.html
[43] Esch, Christian. "Russian Youth Stand Up to the State." *Spiegel Online*, 2019. https://www.spiegel.de/international/world/fearless-generation-in-russia-stands-up-to-the-kremlin-a-1285954.html
[44] Esch, Christian. "Russian Youth Stand Up to the State." *Spiegel Online*, 2019. https://www.spiegel.de/international/world/fearless-generation-in-russia-stands-up-to-the-kremlin-a-1285954.html
[45] Gainous, Jason, Kevin M. Wagner and Charles E. Ziegler. "Digital media and political opposition in authoritarian systems: Russia's 2011 and 2016 Duma elections." *Democratization*, 2018. https://www.tandfonline.com/doi/abs/10.1080/13510347.2017.1315566
[46] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[47] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[48] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[49] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[50] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[51] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[52] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.
[53] "Forecast of internet user numbers in Russia from 2015 to 2022." *Statista*, 2017. https://www.statista.com/statistics/567007/predicted-number-of-internet-users-in-russia/
[54] Pallin, Carolina Vendil. "Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 2017. https://www.tandfonline.com/doi/abs/10.1080/1060586X.2015.1121712
[55] Pallin, Carolina Vendil. "Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 2017. https://www.tandfonline.com/doi/abs/10.1080/1060586X.2015.1121712

[56] Seddon, Max and Henry Foy. "Russian technology: can the Kremlin control the internet?" *Financial Times*, 2019. https://www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2

[57] Jee, Charlotte. "Russia wants to cut itself off from the global internet. Here's what that really means." *MIT Technology Review*, 2019. https://www.technologyreview.com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/

[58] Jee, Charlotte. "Russia wants to cut itself off from the global internet. Here's what that really means." *MIT Technology Review*, 2019. https://www.technologyreview.com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/

[59] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.

[60] Soldatov, Andrei and Irina Borogan. *The Red Web*. PublicAffairs, 2015.