The Unfreedom Monitor

The Unfreedom Monitor

A Methodology for Tracking Digital Authoritarianism Around the World

RUSSIA

COUNTRY REPORT

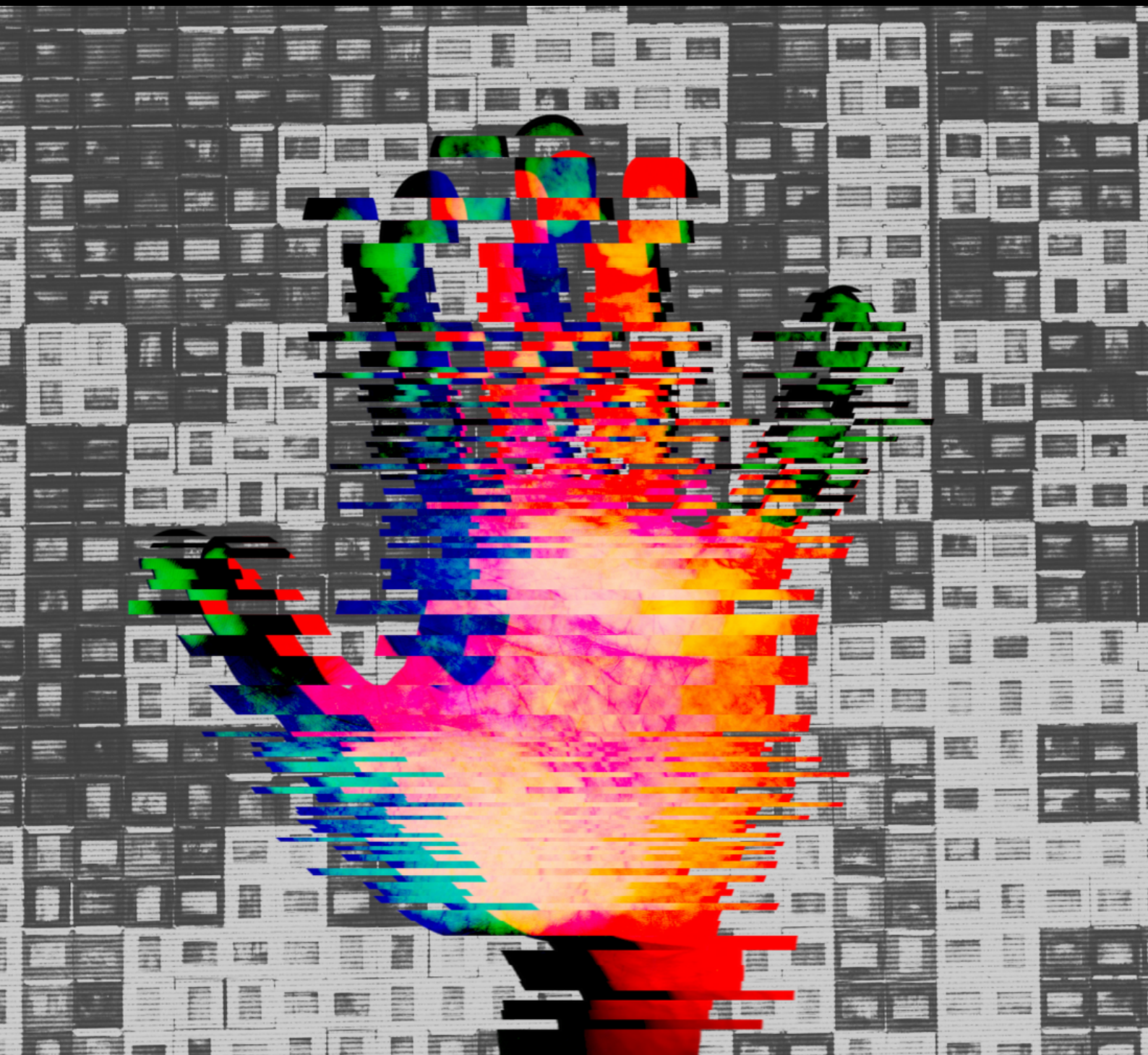


Table of Contents

Acknowledgements

The Unfreedom Monitor is the collective work of dozens of researchers and writers spread across multiple countries and working in time zones. Desk research was supported by colloquia and research assistance from the Global Voices community. In the interests of security, the names of all the team members have been withheld in this report. For citation purposes, the report can be attributed to "Global Voices Advox." Any errors or omissions should also be addressed to Advox at advox@globalvoices.org. Funding for this project was provided by the Deutsche Welle Academy (DW) which in turn received funding from the Federal Republic of Germany through the BMZ, as well as by other Global Voices supporters, a list of which can be found on our sponsors page.

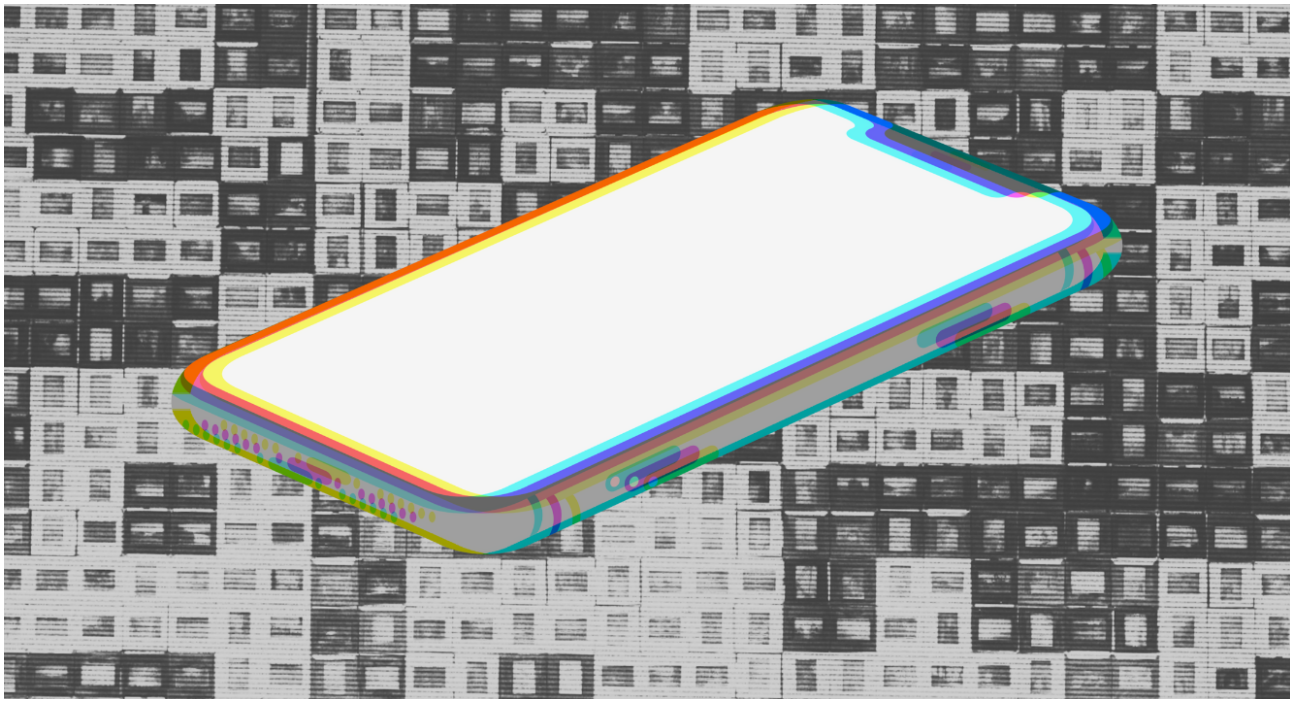
Stichting Global Voices
Kingsfordweg 151
1043GR Amsterdam
The Netherlands
https://globalvoices.org

EXECUTIVE SUMMARY

This report analyses the key motives for, methods of and responses to digital authoritarianism in Russia, relying on existing research and advocacy materials, as well as an in-depth examination of media coverage of key events relating to internet governance and regulation of the online sphere in the country, using a unique methodology pioneered by Global Voices' Civic Media Observatory and adapted by Advox's Unfreedom Monitor project.

The report provides a brief overview of Russia's political system and regime, as well as its international standing and key political and social transformations. Reviewing Russia's media system and the state of media freedom, the report then relays comprehensive background information on the development of the internet and its use in Russia and the evolution of the state's approach to governing content, information and activity in the online space.

Building on this foundation, the report uses the Unfreedom Monitor approach to analyse recent state-owned and independent media coverage with a view to uncovering the key tenets of digital authoritarianism in Russia. The analysis is performed through the prism of several key events or incidents, such as recent parliamentary elections, the passing of significant relevant legislation or implementation of state governance strategies, and Russia's more recent full-scale invasion of Ukraine. The aim of the analysis is to determine the key narrative frames offered by the state and its discontents to explain, defend or critique the key motives, methods and responses to digital authoritarian practices. Tracing these frames and studying the practices and strategies of state internet governance, censorship and control allows to present a more coherent picture of how digital authoritarianism operates in Russia today and to understand the centrality of the internet in Russia's political and social life, and thus, the state's urgency in cementing control over the networked information space, data flows, and telecommunications and internet infrastructure.



BACKGROUND

Technology and digital media have become increasingly central to social and political life in Russia as internet penetration grew and the Russian state realized the potential of e-governance and digitization. Internet penetration saw dramatic growth in the last decade: from 43 percent in 2010 to 85 percent in 2020 (International Telecommunications Union). The Russian digital business industry is home to a number of local internet companies, such as search engine leader and digital service provider Yandex and VK (formerly Mail.Ru Group), which leads the local social media platform market. There is also a broad range of companies (both national and regional) providing internet access services, including broadband and mobile connectivity. A number of international tech companies have also been operating in Russia, with Google commanding a share of the search and advertising market, and Meta (Facebook, Instagram and WhatsApp) enjoying a limited but stable share of the social media market. Alongside this sizeable commercial digital industry, the Russian state has also prioritised the digitisation of state governance and public services, as part of its "Electronic Russia" programme. Under its auspices, in 2009 state operator Roskomnadzor developed and launched GosUslugi, a state portal for public service and municipal service provision for citizens. It has since grown to encompass everything from passport renewals and tax records to paying traffic fines, and currently accumulates probably the largest volume of data on Russian citizens, including personal, financial and biometric data.

The internet in Russia has been pivotal in the democratic transformations of the last decade. It aided mobilization in mass protests — against election falsifications in 2011–12 (known as Bolotnaya Square protests), against pervasive state corruption in 2017–2019, and against crackdowns on opposition activists and candidates around the elections in 2021 — allowing for spaces to organize, share information and recruit protest participants. It also enabled a flourishing independent media scene of online news outlets, investigative media, and Telegram news channels in an otherwise state co-opted media sphere. In 2021, some 42 and 39 percent of Russians received their news from social media and internet news sites respectively (Levada Center). Today, many of these media are operating in exile or have shut down due to growing state pressure.

> *"Russia has a unique networked authoritarian environment where the state is both highly supportive of technological innovation and digital development and increasingly restrictive and controlling towards digital spaces and online expression."*

At the same time, the Russian state has also taken advantage of technology to boost its control over citizens and their data, investing in digital development and e-governance alongside extensive surveillance networks. It has done so by expanding online censorship infrastructure, passing a host of new restrictive data and internet governance laws, and enabling more sophisticated surveillance tools based on citizen data gathering and facial recognition technology. This has created a unique networked authoritarian environment in Russia where the state is both highly supportive of technological innovation and digital development and increasingly restrictive and controlling towards digital spaces and online expression. Russia's networked authoritarians are relying on the very same technologies used by activists to carve out space for free expression to usurp power over digital spaces,

data flows and citizens' online agency. It is therefore important to trace state-crafted and alternative narrative frames used to explain the role of the digital media and platforms in the country's social and political life, to understand how these frames are activated during specific incidents and circulated in the media system, and how they are used by both state actors and state-controlled media to justify greater control and state repressions, and on the other hand, by independent media and digital rights activists to argue for a more independent and free Russian internet where citizens' rights and freedoms take precedence over state interests.

RUSSIA: A BRIEF POLITICAL HISTORY

GOVERNMENT, REGIME TYPE AND INTERNATIONAL STANDING

Since the fall of the Soviet Union in 1991, the Russian Federation adopted a new constitution in 1993 and is governed as a federal semi-presidential republic, with regular presidential and parliamentary elections. Despite the appearance of democratic institutions, President Vladimir Putin and the ruling United Russia party monopolise Russia's politics. Since his election in 2000, Putin has dominated the political system, remaining president until this day save for a single term (from 2008 to 2012,when he became prime minister while Dmitry Medvedev served as President). In 2020, new constitutional amendments were signed into law, limiting the president to two terms overall rather than two consecutive terms, with this limit reset for current and previous presidents, thus allowing Putin to remain in power further.

By the end of 2021, Russia's political order was firmly led by President Putin and his loyalists both within formal institutions and informal networks of power led by political and economic elites. The Russian political system concentrates power in the executive, with the judiciary and the legislative branches either corrupt or subservient, and mechanisms of popular accountability severely weakened. All major channels of communication, including national media channels, are currently firmly controlled by actors committed to disseminating the values and ideology of the current state order.

During Putin's rule, Russia has experienced democratic backsliding, shifting into an authoritarian state (Zimmerman 291), with widely reported election falsifications, and opposition parties and forces largely excluded from mainstream politics. The most recent Freedom House Freedom in the World report ranks Russia as "not free" (Freedom House) in terms of both political rights and civil liberties. Freedom House's Nations in Transit report for 2021 defines Russia as a "consolidated authoritarian regime" (Freedom House), ruling through a combination of executive power, rule by law, and managed democratic institutions. Yet, despite its virtual monopoly over the levers of power, the Putin government has been fearful of popular dissent and has gone to great lengths to silence a small but vocal opposition, led by Alexei Navalny, and to crack down on mass protests and alternative opinions online.

Russia is a member of the United Nations and is one of the five current permanent members of the United Nations Security Council, though the UNGA recently voted to remove Russia from the UN Human Rights Council due to its unprovoked war of aggression against Ukraine. Russia is also a long-standing member of the G20, the Council of Europe, the Organization for Security and Cooperation in Europe (OSCE), and the Asia-Pacific Economic Cooperation (APEC). Russia also plays a leading role in organizations such as the Commonwealth of Independent States (CIS), the Eurasian Economic Union (EAEU), the Collective Security Treaty Organisation (CSTO), the Shanghai Cooperation Organisation (SCO), and BRICS, the economic union between the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China, and the Republic of South Africa.

A key player in the global energy and trade market, Russia maintains strong economic and political ties with neighbouring Belarus, Serbia and China, and a working mutual-interest based relationship with Iran, Turkey and Israel. Its relations with the Western world — especially the United States of America, the European Union states, and NATO countries — have worsened over the past decade, most recently over its invasion of Ukraine. Despite its economic might, Russia has also been described as a kleptocracy due to high levels of corruption, and was the lowest rated European country in Transparency International's 2021 Corruption Perceptions Index, coming in at 136th place out of a total of 180 countries (Transparency International).

"Despite its economic might, Russia has also been described as a kleptocracy due to high levels of corruption, and was the lowest rated European country in Transparency International's 2021 Corruption Perceptions Index, coming in at 136th place out of a total of 180 countries"

In May 1998, Russia ratified the European Convention on Human Rights; however, its relationship with the European Court of Human Rights remains fraught, and Russia remains the country against which the largest number of ECHR applications is lodged (Stichting Justice Initiative). Despite a 2011 local bill granting the Russian Constitutional Court powers to retain any law the application of which was found by the ECHR to violate the convention in a case against Russia, as compliant with the Russian Constitution, Russia as a member of the Council of Europe has been duty-bound to abide by ECHR rulings where it is a party (Issaeva, Sergeeva and Suchkova). In March 2022, following the start of Russia's illegal war of aggression in Ukraine, Russia was expelled from the Council of Europe, which means the country will cease to be a High Contracting Party to the European Convention on Human Rights on 16 September 2022 (Council of Europe). This is bound to have a detrimental impact on the human rights environment in Russia, which has already been deteriorating.

MAJOR POLITICAL EVENTS AND TRANSFORMATIONS

After the 2014 Revolution of Dignity in Ukraine, a mass protest that ousted a pro-Russian president (Lokot 13), Russia occupied Ukraine's southern Crimea peninsula and militarily supported the separatist uprising and occupation of parts of Donetsk and Luhansk regions in eastern Ukraine (known as Donbas). After an unrecognised referendum, Crimea was annexed by Russia as "historically Russian", and Russia continued to support armed rebel forces in occupied Donbas engaging in a protracted war with Ukrainian military, which, after a hot period in 2014–2015, became a simmering conflict. On 24 February 2022, after months of massing Russian troops near Ukraine's border, Russia began a full-scale invasion into Ukraine and has been engaged in an illegal war of aggression on Ukrainian territory ever since (as of 29 June 2022), facing a raft of economic sanctions from the global community. Following the Russian invasion of Ukraine in 2022, anti-war protests broke out across Russia. The protests have been met with widespread repression, leading to over 16,000 citizens being arrested. In response to Russia's aggression and a swell of state propaganda, many social media platforms blocked the accounts of Russian state media, while, inside Russia, the censorship of online spaces and independent media escalated sharply.

The state crackdown on political opposition forces in Russia, which previously manifested in physical attacks and legal persecution, as well as attempts to prevent opposition activists from running in elections, came to a head in 2020. In August of that year, Alexei Navalny, Russia's most prominent anti-corruption activist and political opposition leader, was poisoned in Omsk on August 20 while being tailed by the Federal Security Service (FSB), and later fell into a coma for weeks before waking to a slow recovery after treatment in Germany (Seddon). Navalny accused Putin of being behind the poisoning attempt. In January 2021, Navalny returned to Russia and was detained on accusations of violating parole conditions while he was in Germany, originally imposed as a result of a prior 2014 conviction.

Following Navalny's arrest and subsequent jailing, his team released "Putin's Palace", a documentary that accused President Putin of corruption. The revelations in the documentary alongside Navalny's jailing led to mass protests across Russia in the winter and spring of 2021. The state responded with a crackdown on street rallies and hundreds of protesters were detained, fined or jailed. State censors also cracked down on dissent, requiring platforms to delete calls to protest and information about the rallies. The state pressure extended into the September 2021 parliamentary election, where opposition candidates were excluded or pushed out, and the Navalny team's online voter information tool Smart Voting faced blocks and deletions at the behest of the Russian authorities.

MEDIA FREEDOM AND THE STATE OF THE MEDIA IN RUSSIA

Mainstream media in Russia is largely run or co-opted by the state, including several national television channels (such as Pervyy Kanal and Rossiya 24), a number of national newspapers (such as Vedomosti), and a host of news websites, including state news agencies TASS and RIA Novosti. Independent media, both print and online, have been gradually squeezed out of the media marketplace, and currently exist in limbo, with a number of them, such as Latvia-based Meduza, working from exile. While the regional media are diverse and relatively free, they face lack of funding and strong competition from national (federal) state channels. Many independent outlets, including investigative media outlets The Insider, iStories and Proekt Media as well as online TV channel Dozhd, were recently labelled by the state as foreign agents for receiving alleged foreign funding, and now operate on a much reduced scale or have paused operations.

Until recently, the internet remained a relatively free though contested space for alternative opinions and dissent (Oates). Technically, the Russian constitution guarantees freedom of speech and press freedom, but the politicised judicial system is routinely used to harass independent journalists and civil society activists. In 2021, Russia was ranked 150th out of 180 countries in Reporters Without Borders' Press Freedom Index (Reporters Without Borders). Its low ranking is attributed to expansive media censorship, economic and administrative pressure on independent journalists, and large investments into state-owned media that serve as the state's propaganda arm, both inside Russia and beyond its borders. The proliferation of state efforts to usurp media audiences in both traditional and online media spaces is evidence of the Kremlin's growing realisation that it is no longer enough to retain control only of national broadcast media. Dissenting internet users, including popular bloggers, have to contend with an increasingly sophisticated state surveillance apparatus (Gunitsky). Russian law also contains a broad definition of extremism that officials use to

silence critics of the government, including journalists and protesters. Enforcing this and other restrictive legal measures encourages self-censorship among media professionals and ordinary internet users. While blogging has seen a drop in popularity since the heydays of LiveJournal in early 2000s, there are a number of influential vloggers on YouTube, including Yuri Dud, known for his in-depth interviews and documentaries, and opposition Alexei Navalny who works with his team to release well-produced video investigations documenting the illicit wealth of Russian officials and oligarchs.

THE RUSSIAN INTERNET: PATTERNS AND PENETRATION

KEY FACTS AND STATISTICS

The internet in Russia has been shaped by the state's Soviet legacy as well as its aspirations to remain a global superpower. Some of the first networks and connections were introduced in then-Soviet Russia in the 1980s, when the All Union Scientific Research Institute for Applied Automated Systems (VNIIPAS) was working to implement data connections over the X.25 telephone protocol to form the USSR-wide Academset (Academic Network). However, mass internet adoption didn't begin until the fall of the USSR in 1991, when Russia and other Eastern Bloc countries were allowed to join the global TCP/IP network.

In 2000, when Putin became president only two percent of the Russian population had internet access. By 2010, this had increased to 43 percent. By 2020, Russia had one of the highest internet penetration rates in the developed world – 85 percent, as well as high mobile broadband penetration rates of up to 60 percent (International Telecommunications Union). The average internet connection speed of 7.4 Mbit/s is almost twice the global average of 3.8 Mbit/s (Gelvanovska, Rossotto, and Gunzburger). Despite this, there is an ongoing urban/rural divide in access, with Moscow's penetration rate far higher than those in remote regions of Russia. There is also a generational divide, with younger users far outpacing those over 60.

Much of the content on the Russian internet is produced in Russian or English, while the over 100 indigenous minority languages of the Russian Federation are vastly underrepresented online (Nikitina, Antonova and Evgrafova).

State-owned internet service provider Rostelecom holds the largest share of the broadband market (over 35 percent), competing with several other commercial ISPs, the majority of which are under Russian-based ownership. Despite a competitive ISP market in large cities, most of the existing country-wide cable lines are held by a small number of large operators such as the state-controlled Rostelecom and the Russian railways-affiliated Transtelecom, which operates the country's biggest fibre backbone. The state has invested consistently in improving and expanding Russia's internet backbone network and high-speed transit. In the years since 2015, the Russian state has made an effort to nationalise the country's traffic exchange points and take control over major internet infrastructure.

THE ROLE OF THE INTERNET IN THE MEDIA SYSTEM

By the start of the 2010s, some information networks in Russia retained their freedom, yet key political structures such as the ruling party were focused on self-enrichment and retaining long-term control, while social movements and civic activity were thin on the ground. Though there was comparative media diversity, the media system overall was not free, with a large proportion of national mainstream media channels owned or co-opted by the state. New independent media were aided by the proliferation of the internet (known colloquially in Russia as the RuNet).

Russian authorities have employed an evolving system of what experts refer to as "information controls": techniques, practices and regulations that circumscribe the kinds of information technology, media channels and electronic communications available to citizens (Deibert et al.). This ecosystem works at many levels and may include technical means such as "filtering, distributed denial of service attacks, electronic surveillance, malware, or other computer-based means of denying, shaping, and monitoring information," as well as more opaque measures such as "laws, social understandings of 'inappropriate' content, media licensing, content removal, defamation policies, slander laws, secretive sharing of data between public and private bodies, or strategic lawsuit actions" (Citizen Lab). Meanwhile, independent media and opposition actors rely on websites, digital platforms and networked media channels such as YouTube and Telegram to spread alternative narratives about infighting, corruption, and human rights violations among Russian officials.

Social media platforms are popular in Russia and enjoy mass use, with 99 million social media users in January 2021 (Datareportal). YouTube is the top social media website in the country, with a monthly audience of over 85 percent of internet users between 16 and 64 years old. Russian-made VK (formerly Vkontakte) is the second most popular social media website and the top conventional social network platform in Russia with a monthly audience of 78 percent of internet users between 16 and 64 years old or 74 million users (Datareportal). While YouTube is popular as a content consumption platform, VK is the top website used for communication and information sharing. These are followed in popularity by WhatsApp, Instagram, Odnoklassniki (another local social network), Viber, Facebook, Tiktok and Telegram.

VK is the most popular social network as it was created with the Russian-speaking audience in mind and connects users in Russia and in many other post-Soviet countries where Russian speakers reside. VK is also well integrated into the Russian media and consumer markets. Despite its popularity, VK has faced accusations of cooperating with Russian law enforcement and state censors (Lokot). The messaging platform Telegram, founded by VK creator Pavel Durov after his exit from Russia, has fewer users, yet remains a key channel for uncensored access to news and opinions due to its skillful circumvention of state blocking attempts and lax moderation policies (Lokot).

Since the massive protests against electoral fraud in 2011–2012, to which the internet and social media were crucial, the Kremlin has gone to considerable lengths to control the digital space and centralise internet governance, media censorship, and content regulation. Roskomnadzor, the regulatory body overseeing the internet, media, and telecommunications, is now enforcing more rules and restrictions. There are a host of new laws limiting foreign ownership of media and policing online speech, as well as recent legislation to secure greater control over national internet infrastructure. Criminal defamation was reintroduced in a law adopted in 2012, providing for large fines or weeks of forced labour as punishment. Another restrictive law that came into force in 2012 granted unprecedented blocking powers to Russian telecommunications regulator Roskomnadzor and other state bodies (Rothrock). Still another 2012 federal law mandated the creation of a "blacklist" registry of websites that disseminated allegedly illegal or otherwise harmful material.

Kremlin control over the media expanded still further in the late 2010s and early 2020s, as control over digital media and communications became part of a national governance and security agenda. Key legislative changes have contributed to the further normalisation of state censorship in digital spaces, targeting media outlets, NGOs, and private citizens. These include an infamous "bloggers' law" that required popular bloggers with over 3,000 daily views to register with the state and disclose their personal information; a law creating a state-run list of "organisers of information distribution" and requiring social networks, portals, and similar sites to register and share certain data with the state; and measures limiting the anonymous use of public Wi-Fi networks and banning sales of prepaid SIM-cards to customers without state IDs.

> *"Social media content is regularly deleted or blocked on grounds of intolerance or disrespect toward government officials, and users have been fined and even jailed for posting, sharing, or liking content deemed to contain extremist language, calls to mass disorder, or unverified information about public figures"*

Some of the most far-reaching censorship- and surveillance-oriented measures have been adopted in the past several years. These include a data localisation law that came into force in 2016 that requires internet companies to store Russian users' data on servers located within Russia. Although some companies (e.g., eBay, Booking.com and Samsung) have complied with the demands, others (such as Facebook and Twitter) have yet to do so and have been fined or threatened with blocking. The professional social network LinkedIn has been blocked in Russia since 2016 for failing to comply with the legal requirements.

Another comprehensive legal tool is an "anti-extremism" package of amendments, which was adopted in the summer of 2016 and took effect in 2018. This includes measures such as increased sentences for the use online of "extremist" language (a designation that state authorities can apply with great discretion), a push for internet companies to share encryption keys with the state and to decrypt user communications, and requirements to store user communications for six months and metadata for up to three years. In 2018, Russian censors used these legal grounds to block the Telegram messenger after it refused to share encryption keys with law enforcement. The attempt proved mostly unsuccessful due to Telegram's sophisticated circumvention efforts and the state's clumsy blocking approach; the ban was ultimately lifted in 2020.

Social media content is regularly deleted or blocked on grounds of intolerance or disrespect toward government officials, and users have been fined and even jailed for posting, sharing, or liking content deemed to contain extremist language, calls to mass disorder, or unverified information about public figures. Data from Russia's Supreme Court shows that convictions under the extremism charge more than tripled between 2012 and 2017; a large number of these have involved online activity (Gainutdinov and Chikov).

METHODOLOGY

The Unfreedom Monitor analysis for Russia combines the methodology used in Global Voices' previous work on media observatories with an in-depth analysis of the contextual issues around digital authoritarianism. This approach is primarily qualitative and looks beyond socio-technical causes to consider power analysis, offer a way to discuss effects, and to emphasise what works as well as what's negative. It is a framework that can be consistently applied across a range of contexts, in order to identify and contextualise both positive and disruptive developments, to explain the forces and motives underlying them, as well as the narrative framing devices that often require local knowledge to interpret and weigh. This research method allows us to compare, draw lessons, and consolidate learning about the trends, systems and rules that influence what we know, and how we know it.

The Russia observatory dataset includes 39 media items published in state-owned or state-run and independent Russian media between March 2020 and March 2022, as well as key incidents and narrative frames observed in this media coverage. These are combined with structured analysis of context and subtext, and a civic impact score that rates media items for positive or negative impact on civic discourse. We use Airtable, a relational database, for documentation and collaborative work. The country analysis focuses on identifying and giving context to instances of digital authoritarianism in the Russian context.

As for other countries, the key research question is: "what are the key motives for, methods of, and responses to, digital authoritarianism in selected national contexts?" The country report builds on the initial Airtable Russia dataset to address this larger question, also considering dominant and influential narratives, how they are promoted and by which actors, evidence that supports or negates them, the impact and harm that come from the use of technology that augments repression, and potential solutions for technology interventions and policy advocacy.

The findings of the observatory research on Russia are presented separately as part of a larger cross-country dataset on the Advox website, and form a foundational part of the analysis presented in the individual country report for Russia below.

MAPPING THE COUNTRY CHALLENGE WITH DIGITAL AUTHORITARIANISM

KEY INDICATORS OF DIGITAL AUTHORITARIANISM

Main events of note and key authoritarian practices

The Russian state's authoritarian approach to governing information and communication spaces has a long history: from the normalised surveillance and wiretapping of dissidents in Soviet times to usurping control over the national media channels in the post-USSR era. With the development of digital communications and the internet in the country, Russian authorities have exhibited a growing recognition of their importance — and a growing desire for greater control over expression, content and infrastructure.

Between March 2020 and March 2022, a number of notable events demonstrated how Russia is extending its networked authoritarian approach to governing media and information spaces, political expression, digital platforms and internet users. Many of these incidents stem from and are supported by targeted legislative activity and government regulatory measures, as well as judicial prosecution and administrative and criminal sanctions.

In the period chosen for the analysis of media coverage, we saw state-owned media promoting narratives around several key incidents that predominantly focussed on governance and policing speech and media work (including freedom of expression, freedom of information and freedom of opinion), data governance (including privacy, data protection and surveillance) and issues of access (including targeted service interruptions, blocking of platforms and punitive legislation).

The most notable events during the period include country-wide parliamentary elections in September 2021 and the accompanying wave of government repressions and censorship aimed at restricting Russian liberal opposition candidates from participating in the electoral process. The desire by the ruling authorities to discredit opposition politicians and delegitimise their participation in the elections to ensure a clearly rigged yet decisive victory for the ruling United Russia party saw the government resort to a number of digital authoritarian measures. These included finding pretexts to remove opposition candidates from regional electoral rosters and accusing them of all sorts of violations to undermine their reputation. Crucially, it also saw the authorities block important voter information resources and tools, including Smart Voting, a tool designed by opposition leader Alexey Navalny's team to provide information on which candidates not from the ruling party were more likely to win in various districts. The Kremlin's campaign to block Smart Voting targeted the initiative's website, social media pages and mobile apps and put pressure on digital platforms such as Google, Apple and Telegram to force takedowns of opposition content and independent voter information.

The critical events observed during the research period also include the introduction of a number of key legislative measures specifically aimed at cementing state control over digital spaces, the media system, internet users and online communities,and communications infrastructure. These include the development and implementation of Russia's sovereign

internet strategy and accompanying legislation. The Kremlin's persistent efforts to gain greater control over online communications and critical expression on the Russian internet came to a head in late 2019 with the implementation of a comprehensive "sovereign internet" strategy. A set of new regulations and technical upgrades aimed at more autonomy and state control over internet infrastructure, the "sovereign internet" was presented by the authorities and state media as a means of protecting Russian cyberspace from external threats (Epifanova) posed by foreign governments and hostile platforms. So far, however, it has mostly been used to consolidate control over information flows and internet infrastructure within Russia's borders and to stifle dissent, imposing new centrally controlled and less transparent website blocking and traffic filtering mechanisms and targeting opposition websites and social media platforms (Lipman and Lokot).

> *"The coupling of internet and media censorship and misinformation further narrowed the space for independent media and voices in Russia, pushing the remaining journalists to leave the country and threatening anyone who intended to dispel state disinformation about the war online"*

Alongside restrictions aimed at impeding the role of the internet as an alternative source of news and a space for debate, the Kremlin further expanded its efforts to control independent media outlets through a mix of coercion, ownership change and new regulations, such as the recent "foreign agent" laws. These laws target journalists, media outlets, NGOs and civil society activists and impose high penalties on newsrooms and journalists for violating "anti-extremist" regulations and set limits on the share of foreign ownership in media companies (Wijermars and Lehtisaari 3). Our analysis of media coverage from the period indicates that the state campaign to ostracise key media and civil society actors by labelling them "foreign agents" and placing upon them a burden of compliance with a host of petty rules (e.g., regular reporting to the state on their funding and activities or placing long-winded labels indicating their status on every social media post) has been largely successful. Because of the reputational damage, loss of advertising revenues and potential sanctions making their work difficult, a number of Russian independent media outlets have exited Russia and are now working from exile, while others have shut down.

The final example of regulatory action targeting the internet and social media platforms specifically are Russia's most recent "hostage-taking" laws adopted in June 2021. These measures are aimed at upping the pressure on foreign social media platforms with over 500,000 daily views operating in Russia, by obliging them to register a legal entity and open a local office in Russia, thus making themselves vulnerable to judicial pressure and administrative or criminal prosecution. These regulations are presented by state officials and state-owned media as necessary to combat "hostile" external actors (and the Western influence behind them) operating in the Russian digital environment. While independent media framed these laws as a dangerous precedent that could inspire foreign platforms to exit Russia, the Russian authorities argued that the laws were necessary to ensure that influential foreign social media companies were truly "grounded" in the country, operated within Russian regulatory rules and complied swiftly and efficiently with requests to take down illegal content or share account information with law enforcement.

Another key event was the more recent (and ongoing) Russian full-scale invasion of Ukraine in February 2022, characterised by a sharp expansion of media censorship and repression of free speech in order to present a carefully sanitised and legitimised version of Russia's military incursion into the neighbouring state. Here, the authorities used state media strategically to justify attacking Ukraine and frame their incursion as a limited "special operation" in order to conceal the scale, the losses and details of manoeuvres. This was combined with legislatively prohibiting independent media and internet users from referring to Russia's actions in Ukraine as a "war" or divulging any information about the nature of Russia's actions in the country under threat of hefty fines and even prison time. For instance, the authorities swiftly adopted a new "fake news" law that allowed them to sanction any coverage of Russia's invasion of Ukraine not in line with state narratives as "disinformation," essentially blocking Russian internet and media audiences' access to any independent reporting on the war or casualties. The coupling of internet and media censorship and misinformation further narrowed the space for independent media and voices in Russia, pushing the remaining journalists to leave the country and threatening anyone who intended to dispel state disinformation about the war online.

Of note across all these incidents is the central role of legislation and policies produced by the Russian state in buttressing digital authoritarianism through either targeted legislation or overbroad implementation of existing legal acts. Another key factor that emerges from the media analysis is the frequent designation of external actors (be they governments, platforms or individuals) as hostile agents interfering in Russia's internal affairs and the use of this narrative as a rationale for greater state control over the digital environment. These external "threats" are often used as a pretext for instituting even more censorship of key voices (journalists, activists) and of digital and media platforms (both domestic and foreign). This is done using both administrative instruments such as legislative amendments and fines and technical means such as equipment for DPI (deep-packet inspection) used to filter, throttle and block certain kinds of traffic.

Together, these events and trends reveal a clear slide towards a more hardline networked authoritarian approach that Russian authorities have increasingly adopted with regard to governing the internet, digital media and citizen activity online. The state's aim here is to argue for and achieve greater control of the digital information and media space, as well as internet infrastructure, as evident from the narratives promoted in state-owned media outlets. The digital rights groups, political activists and other proponents of internet freedom have been resisting these moves and have argued that the Russian internet would benefit from remaining open, giving platforms and media outlets space to operate freely and ensuring its users are able to protect their privacy, retain access to a variety of information sources and enjoy freedom of expression online, as evident from the alternative narratives observed in independent Russian media coverage.

Main contours of digital authoritarianism in Russia

Motives

Across the main events outlined in the preceding section, it is clear that the key threat perceived by Russian authorities is the threat of losing political control both internally and externally and the danger of waning narrative dominance over the country's media space, information flows, and the hearts and minds of citizens.

In the case of the September 2021 elections, the ruling United Russia party, closely aligned with President Vladimir Putin, used digital repression as an additional tool to allow it to influence election results and to remain in power through pushing out the opposition, restricting independent election monitoring, and silencing dissenting voices on the streets and online. In doing this, it blamed liberal opposition candidates for undermining the integrity of the electoral process and using digital platforms and voter information tools (such as Smart Voting) to allegedly engage in "extremist" activity.

In the case of legislative activities, there is a pervasive focus on seizing more control over the information, communication and media space. This motivation is underpinned by the state narrative of beefing up national security in the face of global (i.e., Western) threats. With internet sovereignty laws affecting ISPs, traffic exchanges and ordinary users, Russia aims to gain more power over internet content, traffic and infrastructure, as well as reduce its dependency on global tech markets as part of its strategy of "import substitution."

At the same time, the growing host of foreign agent laws are motivated by the need to control information and speech generated by media companies, non-profits and individuals, especially when it relates to political, geopolitical or rights-related matters. By placing excessive bureaucratic requirements on those deemed to be "agents of foreign influence," the authorities aim to crack down on independent thought and activity in Russia and to discredit independent voices, including online.

The "hostage-taking" laws complement these efforts and target large digital platforms as the state seeks to delegate online censorship to social media companies to put the onus of policing online spaces on them and to further restrict opportunities for dissent or alternative expression online for activists, opposition leaders and ordinary citizens, by delegitimising them as "illegal speech." The state's narrative in this case is that large platforms should cooperate with the state's efforts to police online space but that they largely remain uncooperative as is typical for "Western" companies and therefore hostile to Russia's interests.

As the case of Russia's ongoing invasion of Ukraine demonstrates, moments of crisis present additional opportunities for promoting such state narratives of "external threats" and "national security" and using them to justify greater censorship and persecution of alternative opinions in the media and online. In this situation, the authoritarian state uses the familiar language of "fake news" to couch the real motivation for censoring war-related content and media coverage in the country: that is, the need to conceal the real motives, actions and, certainly, war crimes and war casualties occurring as a result of its attack on Ukraine.

Justification and involvement of various branches of government

In general, digital authoritarian measures are justified by the Russian authorities using concerns about national security, as the digital networked sphere has come to be seen as an important part of the national security apparatus. In the case of Russia's internet sovereignty doctrine and other laws policing online spaces and data localisation, the state also justifies repressive measures against platforms and ISPs by the need to protect Russians' data and information from varied external threats.

> *"Close cooperation between branches of power results in a well-oiled repressive machine churning out court sentences in quick succession, making control over the digital information sphere more straightforward than in functioning democracies with separation of power and independent courts"*

Whether these measures are aimed against specific forms of expression, such as calls for protest and political satire, or against certain types of individuals such as independent journalists and human rights activists, they are almost always underpinned by the accusation that those repressed have violated one of more laws or engaged in activity that the state deems extremist, terrorist or otherwise illegal. The labels are assigned based on murky court decrees and expert opinions, meaning that anyone can be designated an "extremist" for any number of activities online. For instance, opposition politician Alexey Navalny's political and activist networks were labelled as extremist in June 2021 with criminal prosecutions opened against many employees and Navalny himself for their organising and online campaigning (The Moscow Times). As digital authoritarian practices become more mainstream, Russian authorities have been targeting large-scale actors as well: in April 2022, Meta's Facebook and Instagram were labelled 'extremist' in order to justify complete blocking of the platforms for enabling users to freely share information about Russia's invasion of Ukraine (The Moscow Times).

The pervasive digital authoritarian measures result from close cooperation between branches of power, with the legislative branch (largely devoid of real opposition lawmakers) passing a plethora of restrictive laws to police online activities, which are then enforced by the executive branch, including key ministries and agencies such as Roskomnadzor, and interpreted by the judiciary which has close ties to the other branches and is known to be co-opted and closely controlled by the executive powers. Many law enforcement agencies also exercise extra-judicial power to gain access to user data and shut down websites or block content deemed illegal. This arrangement results in a well-oiled repressive machine churning out court sentences in quick succession, making control over the digital information sphere more straightforward than in functioning democracies with separation of power and independent courts.

The role of foreign governments and foreign corporations

As can be observed in the key narrative frames emerging out of the media monitoring, the state seeks to present Western governments and digital platforms as overwhelmingly hostile to Russia and Russian internet users. Many of the digital authoritarian activities are meant to thwart foreign government meddling in Russian affairs: internet sovereignty measures seek to give Russia autonomous control over its online space and infrastructure, while "foreign agent" legislation seeks to target and tarnish independent media and NGOs by accusing them of being agents of foreign governments and receiving Western funding. This rhetoric allows Russian authorities to place these measures in the context of Russia's geopolitical interests and to justify repressive regulations and actions by claiming they are in the name of national security and protecting ordinary citizens from harmful external influence.

At the same time, the state is co-opting the language of foreign internet and media policies and regulations to be used for their own digital authoritarian ends: for instance, Russian legislation on "data localisation" harkens back to EU regulations about data protection, while in reality it provides easier access to data for Russian law enforcement. The "foreign agents" legislation is modelled on the US FARA laws, though resembles them in name only and is used to repress opposition activists and independent media. In the latest example, after the invasion of Ukraine was launched, Russian lawmakers adopted a law criminalising "fake news" about Russia's "special operation" in Ukraine (TASS). The law draws on the mainstream language and concerns of Western officials about disinformation, but is actually aimed at preventing the circulation of any independent coverage or credible information about the actions of the Russian military in Ukraine.

Digital corporations such as Meta (Facebook/Instagram), Apple and Google have also been caught up in Russia's efforts to squeeze out opposition politicians and alternative views from mainstream political and social life. Threatened with massive fines, Google and Apple in September 2021 removed Alexey Navalny's Smart Voting app from their app stores in Russia (Roskomsvoboda). Those companies that have staff in Russia, like Google, have been threatened with staff arrests and detentions, or turnover fines (for Google and Facebook), while Twitter has been throttled, as Russian censors pressed them to remove protest-related posts or other content deemed illegal. More recently, Russia has placed the burden of monitoring and removing "'illegal" content on the platforms themselves (instead of responding to state requests), promising fines and other sanctions for non-compliance.

Methods

Among the key technologies used to advance digital authoritarianism in Russia are those that allow for the filtering and blocking of content, accounts and websites. This was first done through crude IP-based blocks which lacked precision, and later using sophisticated deep-packet inspection tools to make specific pages or posts unavailable in the country. Until the introduction of the internet sovereignty legislation, authorities relied on ISPs to use their own equipment to block pages and websites added to the official state blacklist. However, this censorship recently became more centralised: the sovereignty legislation mandates the installation of new DPI equipment in ISP premises that is centrally controlled by the Russian state and Roskomnadzor. This equipment, referred to as "technical means of countering threats" uses more sophisticated deep-packet inspection technology to allow for large-scale filtering and blocking of specific resources without relying on ISPs.

Lately, Russia has also resorted to blocking specific social media platforms: LinkedIn was blocked in 2016, and in 2022 Facebook, Instagram and Twitter were also blocked following Russia's invasion of Ukraine. In 2018, Russian censors unsuccessfully attempted to block Telegram messenger, but failed to achieve complete blocking due to Telegram's circumvention prowess; they reversed the decision in 2020.

Another approach is the throttling of bandwidth and loading speeds for specific platforms (e.g., Twitter after it failed to remove a substantial proportion of protest-related content in 2021). Internet shutdowns have been rare in Russia, and have only been used on a local or regional scale during local protest events or elections.

In addition to censorship-enabling technology, Russian authorities also embrace surveillance technologies such as SORM and other tech used for wiretapping of communications and facial recognition to police behaviour online and offline. Additionally, the personal inboxes, accounts and devices of activists and opposition figures are widely hacked to steal information and leak personal data to discredit these individuals.

Key mechanisms to acquire and deploy technology

In terms of technology for filtering, blocking and shutdowns, Russian authorities rely on a combination of locally made technological solutions and imported foreign ones. For instance, the bulk of the new "technical means of countering threats" DPI tools, including software and hardware, was reportedly created by a Russian company, RDP.ru, owned by state-run telecommunications giant Rostelekom (Roskomsvoboda). However, there have also been reports of Russia using equipment from US-headquartered Lenovo and Super Micro Computer for its new "sovereign internet" control centre, and relying on digital surveillance technology from Israeli company Silicom and internet traffic analysis solutions developed by IXIA, which is part of Keysight Technologies, a US-based company (Soldatov and Borogan).

Legislation is central to Russia's approach to expanding their authoritarian capacity, as evident from the multiple legal acts adopted by lawmakers in the past decade alone that regulate online speech, expression, banned content, platform responsibilities and many other aspects. However, despite the proliferation of these laws, many of them contain norms that are deliberately vague and leave room for abuse, allowing the state to interpret violations and attribute blame where they see fit. For instance, deciding whether an individual or organisation is considered extremist often hinges on witness testimony, and determining whether a satirical image or retweet contains "speech offensive to state officials or incitement to hate" is decided by linguistics experts with dubious credentials. Courts (which are rarely independent as part of a highly corrupt justice system) also play a role in the arbitrary application and implementation of laws that police digital speech and activity, targeting those the state deems undesirable.

"There have been reports of Russia using equipment from US-headquartered Lenovo and Super Micro Computer for its new "sovereign internet" control centre, and relying on digital surveillance technology from Israeli company Silicom"

The role of money

As part of its digital authoritarian turn, Russia has been investing funding from the state budget heavily into technologies and solutions that underpin its "sovereign internet doctrine" as part of the national security agenda.

Such technologies are purchased as predominantly civilian investments, despite being implicated in ensuring national security. Some public procurement information is available, including on state procurement website zakupki.gov.ru, but remains limited as those records contain little information about the purpose or implementation for these technologies, and most of what is known about the details is based on follow-up investigative reporting by independent media tracking Russian procurement expenditure in this area.

Up to 2021, state funding for the sovereign internet and related technologies was allocated as part of the "Digital economy" national programme. Over 2019–2021, the federal subproject of this programme titled "Information security" was allocated over RUB 30 billion (USD 564 million) for these needs, with over RUB 20.8 billion (USD 391 million) meant to fund the DPI-based "technical means of countering threats" (RBC). However, how much the state actually spent on these technologies was never publicly announced.

In 2021, data from the projected state budget suggested that Russia could invest over RUB 31 billion (about USD 582 million) over three years (2022-2024) to support hardware and software solutions enabling filtering, blocking, surveillance and other measures "protecting against external threats."

Russia's total 2021 state budget expenditure amounted to RUB 24.8 trillion (USD 455 billion). According to reporting by RBC, in 2021 national expenditure in the area of internet sovereignty and ensuring the stability of the national internet segment amounted to RUB 9.97 billion (USD 187 million), but in the coming years the need to provide for RuNet's stability would cost the budget significantly more — up to RUB 19.9 billion (USD 374 million) in 2022, RUB 19 billion (USD 357 million) in 2023 and RUB 18.4 billion (USD 346 million) in 2024 (RBC).

Responses

Citizen and journalist responses and their freedom of expression

Russian citizens demonstrate a variety of responses to the expansion of the state's digital authoritarianism depending on their age and internet use intensity; however, the majority remain indifferent or supportive of internet censorship. Though internet penetration in the country is high, it is concentrated in urban agglomerations, and awareness of networked authoritarian practices aligns closely with digital literacy levels and social media use patterns.

In 2016, an independent Levada-Centre poll found that 60 percent of Russians were in favour of internet censorship, while only 25 percent were against it, and 32 percent said banning websites could infringe on citizens' rights and freedoms (Moskva24). In a more recent Levada-Centre poll conducted in May 2022, after Russia's invasion of Ukraine began, 57 percent of respondents in Russia said censorship online was necessary, while a third of the respondents said censorship was not acceptable (RTVI). At the same time, 46 percent were against the recent blocking of Facebook and Instagram related to sharing war news, while only 32 percent indicated support for the ban.

Protests for digital rights or against state censorship online are rare, compared to discontent on political grounds. One of the biggest street protests took place after the state attempted to ban the Telegram messaging app which is extremely popular in Russia. On April 18, 2018 over 12,000 people attended a protest in Moscow against state censor Roskomnadzor's banning of Telegram and in support of digital freedoms (Novaya Gazeta).

> *"Other neighbouring states and countries in Russia's orbit have long been cooperating and learning from its digital authoritarian strategies, with many Central Asian countries purchasing Russia's SORM telecommunications surveillance tech"*

Those most aware of the dangers of digital authoritarian actions of the state are also those who are most at risk: political and civic activists, opposition politicians, digital rights groups, and independent journalists. These groups are among the most prolific users of privacy-protecting technologies such as encryption and two-factor authentication, as well as circumvention tools. Independent media outlets and digital rights groups are also key providers of information about state censorship, surveillance and privacy or circumvention tools to the public. Organisations such as Roskomsvoboda and Internet Protection Society publish guides on how to use Tor and recommendations on VPN services, while rights groups such as Agora and Network Freedoms document civil and criminal prosecutions against internet users, while also offering legal advice. There are also a number of popular Telegram channels such as Za Telecom devoted to internet freedom, digital rights and censorship, run by tech and IT experts, though their following remains niche.

However, with the growth of the state crackdown on free speech online and especially after the unsuccessful Telegram ban, more ordinary users have become aware of VPNs (virtual private networks) and proxy servers as they sought to retain access to their favourite app, connections and channels. This share of internet users was still modest: this is evident from the explosive growth in VPN use after more popular social media platforms (Facebook, Instagram and Twitter) as well as most remaining independent media websites (e.g., Meduza, Dozhd or The Insider) were blocked following the start of Russia's full-scale war in Ukraine in February 2022.

Since February 2022, VPN apps have consistently featured in top-ten downloaded lists from most mobile app stores. According to data from ISPs, some of them (e.g., Yota) saw a 53-fold increase in the number of VPN users between January and April 2022, while some VPN providers, such as Surfshark VPN reported a sharp rise in VPN traffic from Russia over the same period — 75-fold, while the number of VPN users grew 172-fold from January to April (IXBT).

Response of neighbours and international community

Russia's escalating crackdown on digital rights and freedoms has been roundly condemned by most Western governments and rights groups such as Freedom House, EFF or Access Now. US and EU states have placed Russia's digital authoritarian practices in the context

of broader geopolitical struggles, focusing on cybercrime and disinformation as the major threats, while digital rights groups have also pointed to gross violations of user rights and privacy. However, other neighbouring states and countries in Russia's orbit have long been cooperating and learning from its digital authoritarian strategies, with many Central Asian countries purchasing Russia's SORM telecommunications surveillance tech. Turkey and China, where digital authoritarianism has become mainstream, have also been cooperating with Russia on cybersecurity, and there is clear evidence of authoritarian learning between these states and Russia, evident in similar legislative activity and the focus on quashing independent online voices, restricting the activity of foreign social media companies, and striving towards digital sovereignty.

ANALYSIS AND CONCLUSION

THE IMPACT OF DIGITAL AUTHORITARIANISM ON GOVERNANCE AND PUBLIC LIFE

Russia's digital authoritarian practices have become increasingly central to the country's approach to governing political and social life, as the state has recognised the importance of the networked sphere for regulating how information and power flow within its boundaries and outside of them.

The internet — both as a public space and as technical infrastructure — is finally seen by the Russian state as a sphere of strategic priority and it has therefore become imperative for the authorities to control all its aspects as part of a unique networked authoritarian governance framework. As a networked authoritarian state, Russia is overall highly supportive of technological innovation and readily invests into national digital infrastructure and IT development. At the same time, Russian laws and policies governing the internet have become increasingly restrictive and controlling, relying on the very same technologies to usurp the power over digital spaces, data flows and citizens' online agency.

The internet first emerged as an object of strategic state interest in the media and information space as the state was seeking to co-opt control over news and information flows during key political events such as elections. It then became an object of economic and financial interest as well as digital innovation, with the state seeing promise in being seen as technologically progressive and investing in internet infrastructure and digital development, while retaining authoritarian control in key areas.

The internet then gained centrality as a space of public opinion and political activity that became important for the Russian state to co-opt and control as part of the broader push for control of political elites and public perceptions as Putin and his ruling party pushed to eliminate any functioning opposition and cement their power. Finally, the internet gained importance as a geopolitical strategic object, given its centrality to conflicts, cyberwarfare and foreign policy operations. In the current and ongoing stage, the internet is now also an important object of critical technological infrastructure that is now also being co-opted into full state control as part of the national security and sovereignty agenda.

The past decade since 2012 has seen a gradual takeover by the state of key industry players such as VK and Yandex, a crackdown on political and media elites and ordinary users, and the introduction of a swathe of new regulations, all aimed at consolidating state control over an area of importance for the national security and sovereignty agenda. Today, digital authoritarianism is an integral part of Russia's state survival strategy and is likely to remain as such for the foreseeable future, given Russia's current international isolation and its fraught and increasingly hostile standoff with the democratic global community.

References

"Citizen Lab Summer Institute on Monitoring Internet Openness and Rights." *Citizen Lab*, 19 June 2015, https://citizenlab.ca/summerinstitute/2015.html.

Council of Europe. "Russia ceases to be a Party to the European Convention on Human Rights on 16 September 2022". *Council of Europe*, 2022. https://www.coe.int/en/web/portal/-/russia-ceases-to-be-a-party-to-the-european-convention-of-human-rights-on-16-september-2022.

Datareportal. "Digital 2021: Russian Federation." *Datareportal*, 11 Feb. 2021, https://datareportal.com/reports/digital-2021-russian-federation.

Deibert, Ronald, et al. *Access controlled: The shaping of power, rights, and rule in cyberspace*. the MIT Press, 2010.

Epifanova, Alena. "Digital Sovereignty on Paper: Russia's Ambitious Laws Conflict with Its Tech Dependence." *The Russia File, Kenna Institute, Wilson Center*, 23 Oct. 2020. https://www.wilsoncenter.org/blog-post/digital-sovereignty-paper-russias-ambitious-laws-conflict-its-tech-dependence.

Freedom House. "Freedom in the World 2022". *Freedom House*, 2022. https://freedomhouse.org/country/russia/freedom-world/2022.

Freedom House. "Nations in Transit 2021". *Freedom House*, 2021. https://freedomhouse.org/country/russia/nations-transit/2021.

Gainutdinov, Damir, and Pavel Chikov. "Internet Freedom 2017: Creeping Criminalisation." *Agora International*, 2018. http://en.agora.legal/articles/Report-of-Agora-International-"Internet-Freedom-2017-Creeping-Criminalisation"/8.

Gelvanovska, Natalija, Rossotto, Carlo Maria and Michael Lee Gunzburger. "Russia's Ambitious Broadband Goal: Is the Progress Sustainable?". *Connections*, 2016 (4). World Bank, 2016. https://openknowledge.worldbank.org/handle/10986/25012.

Gunitsky, Seva. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics*, vol. 13, no. 1, 2015, pp. 42–54., doi:10.1017/S1537592714003120.

International Telecommunications Union. "Percentage of Individuals Using the Internet. Russia Country ICT Data 2021." *ITU*, 2021. https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2021/PercentIndividualsUsingInternet_Nov2021.xlsx.

Issaeva, Maria, Sergeeva, Irina and Maria Suchkova. "Enforcement of the Judgments of the European Court of Human Rights in Russia". *SUR* 15, 2011. https://sur.conectas.org/en/enforcement-judgments-european-court-human-rights-russia/.

IXBT. "В России стало в 50 раз больше пользователей VPN-сервисов" (Number of VPN service users in Russia grows 50 times"). *IXBT*, 11 Apr. 2022. https://www.ixbt.com/news/2022/04/11/v-rossii-stalo-v-50-raz-bolshe-polzovatelej-vpnservisov-nazvany-samye-populjarnye-prilozhenija.html.

Levada Center. "Sotsialnye seti v Rossii" (in Russian). *Levada Center*, 23 Feb. 2021, https://www.levada.ru/2021/02/23/sotsialnye-seti-v-rossii/.

Lipman, Maria and Lokot, Tetyana. "Disconnecting the Russian internet: Implications of the new 'digital sovereignty' bill". *PONARS Eurasia*, 2019. https://www.ponarseurasia.org/disconnecting-the-russian-internet-implications-of-the-new-digital-sovereignty-bill/.

Lokot, Tanya. "Russian Social Network VK Claims to Protect Users From Warrantless Surveillance." *Advox*, 11 Feb. 2016, https://advox.globalvoices.org/2016/02/01/russian-social-network-vk-claims-to-protect-users-from-warrantless-surveillance/.

Lokot, Tetyana. "Telegram: What's In an App?". *Point & Counterpoint, PONARS Eurasia*, 26 Nov. 2018, https://www.ponarseurasia.org/telegram-what-s-in-an-app/.

Lokot, Tetyana. *Beyond the Protest Square: Digital Media and Augmented Dissent*. Rowman and Littlefield, 2021.

Moskva24. "Почти две трети россиян высказались за ввод цензуры в интернете" ("Almost two thirds of Russians support introducing internet censorship. *Moskva24*, 18 Nov. 2016. https://www.m24.ru/articles/internet/18112016/122481.

Nikitina, E. V., E. I. Antonova, and T. N. Evgrafova. " Russian Minority Languages Representation On The Internet As Their Social Status Reflection." 11th International Scientific and Theoretical Conference "Communicative Strategies of Information Society," 2019.

Novaya Gazeta. "«Настолько плохо, что даже интроверты здесь»" ("'It's so bad that even the introverts are here'". *Novaya Gazeta*, 30 Apr. 2018. https://novayagazeta.ru/articles/2018/04/30/76340-svoboda-internet.

Oates, Sarah. *Revolution stalled: The political limits of the Internet in the post-Soviet sphere*. Oxford University Press, 2013.

RBC. "Власти оценили обеспечение работы «суверенного Рунета» в ₽31 млрд" ("Authorities estimate provision of 'sovereign internet' to cost 31 billion rubles"). *RBC.ru*, 23 Sep. 2021. https://www.rbc.ru/technology_and_media/23/09/2021/614a2bb79a79471f3c2c269f.

Reporters Without Borders. "Russia: 2021 Press Freedom Index." *Reporters Without Borders*, 11 Mar. 2022. https://rsf.org/en/russia.

Roskomsvoboda. "«Тревожный прецедент» — Сеть про ограничение доступа к приложению «Навальный» в App Store и Google Play" (""A worrying precedent": the net about limiting access to Navalny's app in App Store and Google Play"). *Roskomsvoboda*, 17 Sep. 2021. https://roskomsvoboda.org/post/progib-apple-and-google/.

Rothrock, Kevin. "Russia: A Great Firewall to Censor the RuNet?" *Global Voices*, 10 Jul. 2012. https://globalvoices.org/2012/07/10/russia-a-great-firewall-to-censor-the-runet/.

RTVI. "Опрос: около трети россиян поддерживают блокировку Facebook** и Instagram**" ("Poll: about a third of Russians support blocking of Facebook and Instagram"). *RTVI*, 20 May 2022. https://rtvi.com/news/levada-tsentr-46-rossiyan-ne-podderzhivayut-blokirovku-facebook-i-instagram/

Seddon, Max. "How the Kremlin Kept Watch on Alexei Navalny," *Financial Times*, 25 Aug. 2020, https://www.ft.com/content/d6937ef3-15e1-4326-a41a-1828761a84d5.

Soldatov, Andrei and Irina Borogan. "How Western tech companies are helping Russia censor the Internet". *The Washington Post*, 21 Dec. 2021. https://www.washingtonpost.com/opinions/2021/12/21/how-western-tech-companies-are-helping-russia-censor-internet/.

Stichting Justice Initiative. "Russia and the European Court of Human Rights". *Stichting Justice Initiative*, 2011. https://www.srji.org/en/echr/russia/.

TASS. "Путин утвердил уголовную ответственность за фейки о действиях ВС России" ("Putin signs off on criminal responsibility for fakes about Russian army's activities"). *TASS*, 4 Mar. 2022. https://tass.ru/politika/13969809.

The Moscow Times. "Ex-Navalny Coordinators Detained for 'Extremism'". *The Moscow Times*, 29 Dec. 2021. https://www.themoscowtimes.com/2021/12/28/us-russia-to-hold-security-ukraine-talks-early-january-in-geneva-a75941.

The Moscow Times. "Russia Bans Instagram and Facebook as 'Extremist'". *The Moscow Times*, 22 Mar. 2022. https://www.themoscowtimes.com/2022/03/21/russian-court-bans-instagram-facebook-as-extremist-a77017.

Transparency International. "Corruptions Perception Index 2021: Russia". *Transparency International*, 2021. https://www.transparency.org/en/cpi/2021/index/rus.

Wijermars, Mariëlle, and Katja Lehtisaari. "Introduction: Freedom of expression in Russia's new mediasphere". *Freedom of Expression in Russia's New Mediasphere*. London: Routledge, 2020. 1-14.

World Bank. "Russia's Ambitious Broadband Goal: Is the Progress Sustainable?". *World Bank*, 11 Mar. 2022. http://www.worldbank.org/en/topic/ict/brief/russias-ambitious-broadband-goal-is-the-progress-sustainable.

Zimmerman, William. "The Past and Future of Russian Authoritarianism." *Ruling Russia*. Princeton University Press, 2016. 291-310.


GlobalVoices
advox


The
Unfreedom
Monitor