Towards "Digital Sovereignty": Explaining Digital Repression in Russia

Aram TERZYAN*

Abstract

This paper explores the main features of digital repression in Russia, especially in the context of the Russian invasion of Ukraine. The repression of digital activism is not a new phenomenon in Russia; however, it gained fresh momentum during the Russian-Ukrainian war. Security has been used as a pretext to expand the state's authority at the cost of individuals' rights and freedoms. To control political narratives, suppress online dissent and surveil regime critics, the government has significantly tightened the national legislation through its media regulator, Roskomnadzor. The aftermath of the war, harsh sanctions and increased anti-regime movements have also deepened Russia's aspirations toward 'digital sovereignty'. Meanwhile, regardless of a number of important initiatives in this direction, domestic digital space still remains an ambitious goal to be fulfilled. This paper concludes that, along with other devastating consequences, the war in Ukraine will provoke further digital repression in Russia aimed at achieving the Kremlin's goal of "digital sovereignty".

Keywords: Russia, digital repression, human rights, online space, 'digital sovereignty'

Introduction

Digitalization has affected politics in manifold ways and brought new dimensions to political repression. On the one hand, digital technologies empower civil society and provide additional platforms for the fulfillment of fundamental human rights and freedoms. On the other hand, these same technologies are deployed by autocrats to persecute, silence and punish regime critics, activists and other civil society members. This affects not only freedom of expression online, but also the rights to assembly and association, privacy, participation in political and public life, etc.

The suppression of digital activism through network disruptions, internet shutdowns and bans on social networks are on the rise globally. This is particularly evident in autocratic environments where repression is used to raise the costs of disloyalty, promote the favored stories and suppress mass mobilization movements against the regime. The COVID-19 crisis has further enhanced governments' capacities for digital repression (Bleyer-Simon, 2021). The resulting proliferation of censorship and surveillance technologies introduced in a number of countries under the guise of anti-

* Aram Terzyan, PhD is Research Director of Center for East European and Russian Studies, Eurasia Institutes- California, USA, e-mail: a.terzyan@eurasiainstitutes.org.

pandemic measures provided an opportunity to further promote their model of digital governance (Feldstein, 2021).

Since the Kremlin launched its “special military operation” in Ukraine, the authorities have significantly narrowed the space for online activism. Media censorship has reached new extremes with almost all independent media being banned, blocked or declared as ‘foreign agents’ by the Russian authorities. To endorse state narratives about the war, suppress online dissent and surveil critics, the government has adopted a series of vague and ill-defined laws causing dramatic deterioration in the already restrictive online environment in Russia.

Against this backdrop, two questions lie at the heart of this research:

1) What are the basic features of digital repression in autocratic environments?
2) What is the state of digital repression in Russia during wartime?

The paper is structured as follows. Firstly, the study discusses the core features of digital repression through providing main theoretical perspectives. Subsequently, it focuses on the specific forms and shapes that digital repression has tended to take in Russia. The conclusion briefly discusses the main findings.

On the theory of digital repression

The sharp rise of digital technologies in the past two decades has substantially increased the capacity for repression of digital activism and tools used for that purpose. More and more governments are deploying new technologies to silence critical voices, suppress anti-regime protest movements, enhance political control, seeking to ensure regime survival (Głowacka *et al*., 2021).

Feldstein defines digital repression as “the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state” (Feldstein, 2021). Davenport refers to it as “an actual or threatened use of physical sanctions against an individual or organization … for the purpose of imposing a cost on the target” (Davenport, 2007). Regardless of numerous definitions, it is commonly held that the purpose of repressive actions is to raise the “cost” of political participation to such a degree that citizens would not consider or be aware enough to engage in political actions deemed undesirable by state authorities. This could be accomplished in many forms - from online harassment, to disinformation, to internet shutdowns, cyberattacks and targeted surveillance using social media, artificial intelligence (AI) and facial recognition software (Lamensch, 2021).

Digital repression resembles traditional repression in many ways. Like traditional repression, digital repression allows identification of critical voices, and decreases the likelihood of mass mobilization against the regime. Nevertheless, despite considerable similarities, there is a number of dissimilarities between traditional and digital repression. Notably, digital repression considerably increases the effectiveness of longstanding repressive practices and tactics, while lowering the costs (Frantz *et al*., 2020, p. 2).

Feldstein (2021) identifies three important insights into the patterns of digital repression. Firstly, there is a strong statistical relationship between regime type and digital repression. Secondly, autocracies seek to enforce digital repression at a level greater than their capabilities, forcing them to make up the gap with external sources or reliance on less advanced digital tools. Conversely, digital repression capacity in democracies outstrips enactment, meaning that democracies choose to not to apply the excess capabilities they possess. Thirdly, not only do autocracies and democracies deploy contrasting digital strategies, but among autocracies there is significant variance regarding which digital methods these regimes choose to implement (Feldstein, 2021, pp. 62-63).

Though dictatorships vary in the extent to which they rely on repression, all regimes use it to some degree. Reliance on digital repression increases reliance on more "high intensity" forms of repression, such as the use of torture and imprisonment (Frantz *et al*., 2020, p. 1). Thus, it can be argued that autocratic governments are not totally substituting the new tools for their old ones, but they are merely using them to make the existing mechanisms more effective.

Digital repression has become the 'new frontier of the autocratic survival toolkit' (Frantz *et al*., 2020). Recent research has shown that where digital repression is highest, leaders survive in office longer than in places where it is less significant. The use of digital repression reduces the likelihood of authoritarian regimes facing internal protest or sustained mobilization efforts, which represents perhaps the most serious threat to dictatorships today (Kendall-Taylor *et al*., 2020, p. 103).

Autocratic governments mostly rely on such tools as online censorship, surveillance, and internet shutdowns to control online communications, selecting what they believe will be effective in the respective political situations on the ground (Weidmann and Dainotti, 2022, p. 60). Although these measures are generally applied under the name of defending national security, social morality, and public order, in a number of contexts they are being used for the personal advantages of those in power.

Online censorship involves government suppression of the free flow of information and ideas that threatens the *status quo*, and demarcation on what is acceptable and unacceptable communication in society (Liu and Wang, 2021). A recent study of cross-sectional time-series data of 153 countries

from 1995 to 2018 reveals that internet censorship is a reactive strategy used by autocracies to suppress civil society. It is argued that the use of censorship as a political reaction to technological diffusion and contentious politics worldwide has damaged the development of civil society (Chang and Lin, 2020).

Because of the nature of information, censorship can be disguised, making it difficult to notice that information is being manipulated. While fear-based censorship, aimed at intimidating and deterring, must be visible in order to be effective, more sophisticated forms of censorship that work through “friction and flooding”, such as blocking of websites, reordering of search results, and covert information campaigns, can exert effects without alerting users (Roberts, 2020, p. 406).

Like censorship, digital surveillance creates an information imbalance between the citizen and his or her government. It may lead to an increase in information on dissidents and regime critics, particularly on the opposition leaders most likely to mobilize against the regime (Frantz *et al*., 2020, p. 14). Internet monitoring helps rulers observe patterns of human behavior that are unknown to the ruled and permits top-down governance structures but is fundamentally incompatible with securing the consent of the populace (Robbins and Henschke, 2017).

Using country- and multi-level analysis, Stoycheff *et al*. (2018) reveals the negative effect of digital censorship and surveillance on democratization, providing the first cross-national tests of the effects of online surveillance. By investigating 63 countries, the study evidenced that online government monitoring is negatively associated with democratization (Stoycheff et. al., 2018, p. 1).

Government-led internet shutdowns are also one of the tactics of digital repression. Researchers have illustrated that shutdowns take a toll on local economies, and they have been shown to correlate with higher levels of violence, undermining the argument that they are necessary to maintain peace and security (Freedom House, 2022, p. 23). In autocracies, they are widely used to push back against mass demonstrations and entrench military coups (Feldstein, 2022, p. 6). They are also frequently reported during armed operations, severely restricting reporting and human rights monitoring. The inability to access tools to document and rapidly report abuses contributes to further violence and may lead to atrocities. Some shutdowns may even be used with the intention of covering up human rights violations (Human Rights Council, 2022, p. 7). In Myanmar, for instance, shutdowns have blocked the capacity to report air strikes on civilians, the burning of houses, and extrajudicial killings and arrests, including of children (Myanmar Now, 2022).

Markedly, the level of control and censorship increases during the wartime. Conflict situations become fertile ground for mass disinformation campaigns intended to undermine the proper understanding of developments, as well as more generally, of security, public order and peaceful democratic processes (Council of Europe, 2022).

The groups most targeted and subjected to repression are commonly journalists, human rights defenders, whistle-blowers, political opposition, and other civil society activists. At the same time, for instance, expanding AI-driven data collection systems increasingly affects the wider population, among whom the most severely affected are the poor and other most disadvantaged groups in society (Glowacka, 2021, p. 4). Interestingly, the majority of people do not immediately feel the effect of crackdowns. The prevailing sense of indifference in autocracies goes a long way toward redefining the state-citizen relationship in favor of the regime, which progressively but methodically uses its heavy-handed approach as a deterrent to dissent. In such environments, "repression becomes an instinct, security an obsession, and social control a policy" (Zayani, 2015, p. 48).

While digital repression mostly affects freedom of expression (just as in the case of widespread surveillance), it also interferes with multiple other rights, such as the right of association and peaceful assembly, participation in political and public life, privacy, etc. (Glowacka, 2021, p. 14). Meanwhile, it is recognized that the laws on human rights are applicable to the internet and other digital technologies. In 2012, the UN Human Rights Council (2012) adopted a 'Resolution on the promotion, protection and enjoyment of human rights on the Internet', for example, affirming that 'the same rights that people have offline must also be protected online - in particular, freedom of expression, which is applicable regardless of frontiers and through any media of one's choice' (Human Rights Council, 2012). Thus, international human rights instruments, such as such as the International Covenant on Civil and Political Rights ('ICCPR') or the European Convention of Human Rights ('ECHR'), though not specific to new and emerging technologies, may be invoked to address the current human rights challenges posed by them (Human Rights Council, 2012).

Digital repression has gone so far so as to give rise to the term "digital authoritarianism", which is defined as "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations" (Polyakova and Meserole, 2019). It is evident that there has been a rise in digital authoritarianism in the midst of the Covid-19 pandemic, which has significantly accelerated and expanded the implementation of advanced digital technologies that are aimed to tighten the authoritarian hold over society. In a number of countries, security has been used as a pretext to expand the state's authority at the cost of individuals' rights (Domańska, 2020, p. 21).

In recent years, more governments than ever have tightened control over what people can access and share online by blocking foreign websites, hoarding personal data, and centralizing their countries' technical infrastructure (Freedom House, 2022, p. 2). Fragmentation is also accelerating at a rapid pace and not only in authoritarian contexts. Some governments are cultivating domestic spaces in order to suppress critical information, promote disinformation, and access users' personal

information more easily. However, others contribute to fragmentation more carelessly in their efforts to tackle disinformation, protect user data, and deter genuine cybercrimes (Funk, 2022).

During 2022, online censorship reached an all-time high, with a record number of governments blocking political, social, or religious content, often targeting information sources based outside their own borders. The most severe manifestations of digital repression are currently traced in Russia, Myanmar, Libya, and Sudan, which have experienced the world’s steepest declines in internet freedom (Freedom House, 2022).

The state of digital repression in Russia

Despite its long history of censoring traditional media, under President Putin’s regime the Russian government for many years adopted a relatively liberal approach to online speech and the Russian Internet. That began to change in early 2012, after online news sources and social media played a central role in organizing protests following the parliamentary elections of December 2011 (Duffy, 2015). Russia started to expand its censorship capacities and has gradually updated its legal system to prevent dissent and to silence critical voices.

In the past, instead of blocking or censoring an overwhelming amount of content, Russian government actors simply flooded the information market with news stories supporting government endorsed narratives (Morgus, 2019, p. 94). However, the adoption of new and harsh laws and the government’s endeavors to nationalize the Internet in Russia have significantly changed the Russian model of information control.

Since 2012, Russia has maintained a centralized Internet blacklist kept by the Federal Service for Supervision of Communications, Information Technology and Mass Media, commonly known as *Roskomnadzor*. Furthermore, the Duma granted the Prosecutor General the authority to block sites without a court order and expanded the blacklist to include sites publicizing unsanctioned mass events (Cebul and Pinckney, 2021, p. 12). Although Russian telecommunications surveillance (the SORM system) has been in operation since the 1990s, emerging technologies are enhancing these tools. The 2016 Yarovaya amendments require all “organizers of information dissemination” to archive user data for three years on Russian servers and to grant the Federal Security Service (FSB) access to these communications and to any encryption codes (Cebul and Pinckney, 2021, p. 14).

Overall, Roskomnadzor has played a significant role in slowly increasing the state’s control over digital space. The agency was established on December 3, 2008, following presidential decree no. 1715, which granted only censorship powers (Sherman, 2022). Nevertheless, reporting on

thousands of leaked Roskomnadzor documents shows that it acts as an element in a repressive apparatus. A New York Times' investigation (2022) reveals that Roskomnadzor has gone far beyond what was publicly known on managing website blocklists and filing censorship orders. For a couple of years now, the internet censor has compiled dossiers on individuals and organizations posting regime-critical content. According to the New York Times, Roskomnadzor has "worked to unmask and surveil people behind anti-government accounts and provided detailed information on critics' online activities to security agencies" (New York Times, 2022).

Since 2014, to evoke fear and justify greater digital control, Putin's regime has repeatedly presented a scenario in which Russia finds itself switched-off from the global internet and hit by technological sanctions from the United States (Epifanova and Dietrich, 2022, p. 5). Thus, the Kremlin justified initiating a series of legal and technical procedures aimed at 'sovereignization' of the Internet. In May 2019, Putin signed new legislation banning fake news and the showing of 'blatant disrespect' for the state online. The law defines the status of and requirements for the "critical infrastructure" of the Runet, with a specific focus on international communication lines and internet exchange points. Their owners and operators are supposed to ensure centralized traffic management amidst "external threats". The latter is a vague term that the authorities can easily manipulate to tighten their grip on the relevant infrastructure for any reason (Freedom House, 2022). Critics have been concerned that legislation could create a mechanism for state censorship, whereas lawmakers argued that the new measures would be used to combat false news reports and abusive comments (Reuters, 2019).

'Sovereignization' of the Internet can be seen to be a common pattern in authoritarian regimes, where the internet is viewed by the authorities both as a threat to regime survival and as a tool to be used against state enemies. Thus, in an attempt to control the political narrative and suppress all dissent, authoritarian rulers are severely tightening national legislation on the internet.

The Russian-Ukrainian war has brought further deterioration in the already restrictive online space in Russia and has hastened the Kremlin's path toward digital isolation. Within several weeks, Russian digital space has been put into an unprecedented situation. One the one hand, international sanctions cut off many services from abroad, on the other hand the Russian government has harshly restricted online speech and access inside its borders.

Concerns about Russia's fractured Internet ecosystem have only grown since the war. Through its media regulator Roskomnadzor, which is included on the international Reporters Without Borders (RSF) list of digital press freedom predators (RSF, 2020), the government has been controlling independent mass media outlets since the start of the war (Amnesty International, 2022).

Roskomnadzor launched an investigation against the Novaya Gazeta, Echo of Moscow, inoSMI, MediaZona, New Times, Dozhd (TV Rain), and other Russian media outlets for allegedly publishing false information about the Russian military actions in Ukraine (shelling of Ukrainian cities, casualties, etc.) within the Russian “special military operation” (Radio Free Europe, 2022).

Repression of the independent media has been exercised primarily through tightened censorship legislation. On March 4, 2022 Russia enacted two laws criminalizing independent war reporting, with penalties of up to 15 years in prison. The laws make it illegal to spread “fake news” about the Russian armed forces, to call for an end to their deployment and to support sanctions against Russian targets (HRW, 2022). Commenting on this legislation, Kremlin spokesperson Dmitry Peskov told reporters that “unprecedented conditions require unprecedented solutions.” He explained that the current situation can be described as unprecedented “in terms of imposing absolute hatred on everything Russian, whether it is Russian missions, Russian citizens, or foreign citizens who are of Russian origin” (Russia Today, 2022). Nevertheless, the laws are not limited to the war in Ukraine but apply to any deployment involving Russian armed forces, such as those under the regional military alliance, the Collective Security Treaty Organization. These new laws have been regarded internationally as “part of Russia’s ruthless effort to suppress all dissent and make sure the population does not have access to any information that contradicts the Kremlin’s narrative about the invasion of Ukraine” (HRW, 2022).

Since the adoption of the March censorship legislation, the authorities have blocked access to a number of independent media outlets and opened criminal cases against those speaking out against the war. Kremlin blocked Facebook, Instagram, and Twitter, depriving Russians of access to reliable information about the war and limiting their ability to connect with users in other countries (Freedom House, 2022). Russian media regulator Roskomnadzor based its decision on claims that these popular platforms were discriminating against the Russian media and information resources, such as RT, RIA Novosti, and Sputnik (RFE/RL, 2022).

Furthermore, the government expanded its foreign agent law and mandated that media outlets refer to the war as a “special military operation” (Freedom House, 2022). Some human rights NGOs, such as Memorial and Civil Assistance Committee, “Pskovskaya Gubernia” newspaper and a number of human rights defenders have been subjected to persecution and punishment for their opposing views. This has had a disastrous effect on the human rights situation in the country, prompting hundreds of journalists, human rights defenders and civil society activists to seek refuge abroad (Council of Europe comments, 2022). It is estimated that at least 150 journalists, including both foreign and Russian reporters, fled Russia within two weeks of the start of the war (Amnesty International, 2022). As Morgus (2019) aptly argues, Russian censorship and surveillance technology

relies less on filtering information before it reaches citizens (as is the case in China) and more on a repressive legal regime coupled with tightening information control and intimidation of internet service providers (ISPs), telecom providers, private companies, and civil society groups (Morgus 2019, p. 91).

Despite the harsh March laws, which strictly limit the freedom of assembly, anti-war demonstrations began to appear across the country. Nearly 1,200 Russians were arrested in cities including Moscow and St. Petersburg, according to the independent Russian human rights group OVD-Info (Euronews, 2022). Particularly in the Russian region of Dagestan, protests continued for several days with hundreds of people taking to the streets of the capital, Makhachkala, where clashes erupted between demonstrators and the police. Dozens of people were reported to have been arrested (UN Office of the High Commissioner for Human Rights, 2022). The federal agencies significantly contribute to spying on protesters and anti-war activists. In the spring and summer of 2022, when the Russian government had not yet launched a massive crackdown on anti-war protests, activists in Moscow and St. Petersburg were identified by the city CCTV systems through facial recognition (Soldatov and Borogan, 2022). These systems (four of which are based in Moscow) are run by Moscow's Department of Information Technology (DIT) and aim at introducing and running new technologies in the Moscow administration. Thus, the DIT serves as a repressive tool in the hands of the Russian authorities (Soldatov and Borogan, 2022).

Notably, cyberattacks against state and state-affiliated websites increased significantly throughout the war. According to a Freedom House report (2022), at the end of February 2022, the hacking group Anonymous claimed responsibility for cyber-attacks that conveyed anti-war messages on the Russian government websites, Roskomadzor, and other state entities, along with other state-affiliated media outlets, such as RT, TASS, and Kommersant. Over 2,500 Russian- and Belarusian-linked websites have been targeted throughout the campaign, while experiencing the repercussions of cyberattacks (Freedom House, 2022).

Overall, internet freedom in Russia has declined by seven points, reaching an all-time low and representing the year's largest national decline in Freedom on the Net. "With loyalist security forces, a subservient judiciary, a controlled media environment, and a legislature consisting of a ruling party and pliable opposition factions, the Kremlin is able to suppress genuine dissent" (Freedom House, 2022).

Apparently, Russia is today seeking to export its state-controlled version of the internet on the global stage, promoting its own candidate to lead the United Nations International Telecommunications Union (ITU), the agency responsible for information and communication technology (Committee to Protect Journalists, 2022). Meanwhile, Russia's path to 'digital

sovereignty’ has a long way to go. Currently, it is heavily dependent on external actors, especially the information and communications technology (ICT) of the United States and Europe. A number of externally owned hardware, software, and social media networks are widely used in Russia both the public and private sectors (Epifanova and Dietrich, 2022, p. 5). The dependence on foreign technologies challenges Russian both externally (the weaponization of digital technologies against Russia from abroad) and internally (the problem of controlling all levels of Russian political life to ensure regime survival).

Conclusion

The repression of digital activism is on the rise globally and significantly undermines international efforts toward democratization. In autocratic environments, digital technologies are increasingly used to reduce the likelihood of internal protests or sustained mobilization efforts, which represent the most serious threat to dictatorships today. While digital repression restricts mostly freedom of expression, it also interferes with multiple other rights, such as the right of association and peaceful assembly, participation in political and public life, privacy, etc.

The Russian-Ukrainian war has brought further deterioration in the already restrictive online space in Russia. Within several weeks, Russian digital space was in an unprecedented situation. One the one hand, international sanctions cut off many services from abroad, on the other hand the Russian government harshly restricted online speech inside its borders. Security has been used as a pretext to expand the state’s authority at the cost of individuals’ rights and freedoms.

In an attempt to control state-endorsed narratives and suppress dissent across the country, the Russian authorities have severely tightened national legislation on the network. A series of vague and ill-defined laws introduced in Russia severely narrowed the digital space and subjected the critics of the government to unjustified raids. This has mostly affected journalists, human rights defenders and civil society activists, prompting many of them to seek refugee abroad. Through its media regulator Roskomnadzor, which is a central element of the Russian repressive apparatus, the government surveilled people behind anti-government movements and obtained information on critics’ online activities.

The war has also hastened Russia’s path to ‘digital sovereignty’. The aftermath of the war, tough international sanctions and increasing domestic unrest have made the ‘sovereignization’ of the Internet a priority for Kremlin. Although several important initiatives have been made in this regard, the cultivation of a sovereign digital space has still a long way to go in Russia. Clearly, Russian citizens are facing formidable challenges. While they have every right to express their dissenting

views, the Kremlin's massive crackdown on anti-regime activists is bound to further restrict the freedom of expression across the country. A question remains as to whether the Kremlin's repressive tools will suffice to silence dissent, amid mounting international sanctions on Russia, coupled with the Russian citizen's growing resentment towards the government's repressive practices. Further research is essential for exploring what other forms and shapes the Kremlin's digital repression will take amid the escalating war in Ukraine.

References

Amnesty International (2022), *Russia: Kremlin's Ruthless Crackdown Stifles Independent Journalism and Anti-War Movement* (retrieved December 27, 2022 from https://www.amnesty.org/en/latest/news/2022/03/russia-kremlins-ruthless-crackdown-stifles-independent-journalism-and-anti-war-movement/).

Bleyer-Simon, K. (2021), Government repression disguised as anti-disinformation action: Digital journalists' perception of covid-19 policies in Hungary, *Journal of Digital Media & Policy*, 12(1), pp. 159-176.

Cebul, M. and Pinckney, J. (2021), *Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution*, United States Institute of Peace, Special Report (retrieved December 27, 2022 from https://www.usip.org/sites/default/files/2021-07/sr_499-digital_authoritarianism_and_nonviolent_action_challenging_the_digital_counterrevolution.pdf).

Chang, Ch., and Lin, Th. (2020), Autocracy Login: Internet Censorship and Civil Society in the Digital Age, *Democratization*, 27(5), pp. 874-895.

Committee to Protect Journalists (2022), *'Disastrous for Press Freedom': What Russia's Goal of an Isolated Internet Means for Journalists* (retrieved December 27, 2022 from https://cpj.org/2022/05/disastrous-for-press-freedom-what-russias-goal-of-an-isolated-internet-means-for-journalists/).

Council of Europe (2022), *Freedom of Expression in Times of Conflict* (retrieved December 27, 2022 from https://www.coe.int/en/web/freedom-expression/freedom-of-expression-in-times-of-conflict#).

Council of Europe comments (2022), *Support Russian and Belarusian Civil Societies and Human Rights Defenders* (retrieved December 27, 2022 from https://www.coe.int/en/web/commissioner/-/support-russian-and-belarusian-civil-societies-and-human-rights-defenders).

Davenport, Ch. (2007), State Repression and Political Order, *Annual Review of Political Science*, 10 (1), pp. 1-23.

Domańska, M. (2020), Russian Digital Authoritarianism at the Time of COVID-19. *New Eastern Europe*, 5 (43), pp. 21-27.

Duffy, N. (2015), Internet Freedom in Vladimir's Putin Russia: The Noose Tightens, *AEI Papers* (retrieved December 27, 2022 from https://www.aei.org/wp-content/uploads/2015/01/Internet-freedom-in-Putins-Russia.pdf).

Epifanova, A. and Dietrich, Ph. (2022), Russia's Quest for Digital Sovereignty: Ambitious, Realities, and Its Place in the World, *DGAP Analysis*, 1 (retrieved December 27, 2022 from https://dgap.org/sites/default/files/article_pdfs/DGAP-Analyse-2022-01-EN_0.pdf).

Euronews (2022), *Ukraine War: Hundreds Arrested in Russia After Putin's Troops Call-Up Order Sparks Protests* (retrieved December 27, 2022 from https://www.euronews.com/2022/09/21/russian-protesters-take-to-the-streets-over-putins-mobilisation-order).

Feldstein, S. (2021), *Digital Technology's Evolving Role in politics, protest and Repression*, United States Institute of Peace (retrieved December 27, 2022 from https://www.usip.org/publications/2021/07/digital-technologys-evolving-role-politics-protest-and-repression).

Feldstein, S. (2021), The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance, US: Oxford University Press.

Feldstein, S. (2022), Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond. *Carnegie Papers* (retrieved December 27, 2022 from https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687).

Frantz E., Kendall-Taylor, A., and Wright, J. (2020), *Digital Repression in Autocracies*, V-Dem Institute, Working Papers 27 (retrieved December 27, 2022 from https://www.v-dem.net/media/publications/digital-repression17mar.pdf).

Freedom House (2022), *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet* (retrieved December 27, 2022 from https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet).

Funk, A. (2022), *Digital Repression is Deepening, But Civil Society Wins Give Reason for Optimism*, Freedom House articles (retrieved December 27, 2022 from https://freedomhouse.org/article/digital-repression-deepening-civil-society-wins-give-reason-optimism).

Glowacka, D., Youngs, R., Pintea, A., Wołosik, E. (2021), Digital Technologies as a Means of Repression and Social Control, *EU Papers* (retrieved December 27, 2022 from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf)

HRW (2022), *Russia Criminalizes Independent War Reporting, Anti-War Protests* (retrieved December 27, 2022 from https://www.hrw.org/news/2022/03/07/russia-criminalizes-independent-war-reporting-anti-war-protests).

Human Rights Council (2012), *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development* (retrieved December 27, 2022 from https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf).

Human Rights Council (2022), *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights* (retrieved December 27, 2022 from https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human).

Kendall-Taylor, A. Frantz, E., and Wright, J. (2020), The Digital Dictators: How Technology Strengthens Autocracy, *Foreign Affairs*, 99 (2), pp. 103-115.

Lamensch, M. (2021), *Authoritarianism Has Been Reinvented for the Digital Age*, Centre for International Governance Innovation (retrieved December 27, 2022 from https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/).

Liu, S., and Wang, D. (2021), Censorship: State Control of Expression, in: Valverde M., Clarke K., Darian-Smith E., Kotiswaran P. (eds.), *Routledge Handbook of Law and Society*, New York, NY: Routledge.

Morgus, R. (2019), The Spread of Russia's Digital Authoritarianism, in: Wright, N. D. (ed.), *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, Washington, DC: United States Department of Defense.

Myanmar Now (2022), *Myanmar junta cuts off internet access 'indefinitely' to resistance stronghold of Sagaing* (retrieved December 27, 2022 from https://www.myanmar-now.org/en/news/myanmar-junta-cuts-off-internet-access-indefinitelyto-resistance-stronghold-of-sagaing).

New York Times (2022), *'They are Watching': Inside Russia's Vast Surveillance State* (retrieved December 27, 2022 from https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html).

Polyakova, A. and Meserole Ch. (2019), Exporting digital authoritarianism: The Russian and Chinese models, *Brookings*, August 2019 (retrieved December 27, 2022 from https://www.brookings.edu/research/exporting-digital-authoritarianism/).

Radio Free Europe (2022), *Russian Government Orders Media Outlets to Delete Stories Referring to 'Invasion' Or 'Assault' On Ukraine* (retrieved December 27, 2022 from https://www.rferl.org/a/roskomnadzor-russia-delete-stories-invasion/31724838.html).

RFE/RL (2022), *Russian Media Watchdog Blocks Facebook after Limiting Access to Multiple Other Sites* (retrieved December 27, 2022 from https://www.rferl.org/a/russia-rferl-bbc-facebook-google-twitter-blocked/31735597.html).

Robbins, S., and Henschke, A. (2017), The Value of Transparency: Bulk Data and Authoritarianism. *Surveillance & Society*, 15(3–4), pp. 582–589.

Roberts, M. (2020), Resilience to Online Censorship, *Annual Review of Political Science*, 23, pp. 401-421.

RSF (2020), *RSF Unveils 20/2020 List of Press Freedom’s Digital Predators* (retrieved December 27, 2022 from https://rsf.org/en/rsf-unveils-202020-list-press-freedom-s-digital-predators).

Russia Today (2022), ‘Fake News’ about Russian State Bodies Abroad Criminalized, *Russia Today* (retrieved December 27, 2022 from https://www.rt.com/russia/552481-lawmakers-criminalize-fake-news/).

Sherman, J. (2022), Russia’s Internet Censor is Also a Surveillance Machine, *CFR Papers* (retrieved December 27, 2022 from https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine).

Soldatov, A. and Borogan, I. (2022), Russia’s Surveillance State, *CEPA papers* (retrieved December 27, 2022 from https://cepa.org/article/russias-surveillance-state/).

Stoycheff, E., Burgess, S., and Martucci, M. C. (2018), Online Censorship and Digital Surveillance: The Relationship between Suppression Technologies and Democratization across Countries, *Information, Communication & Society*, 23 (4), pp. 1-17.

UN Office of the High Commissioner for Human Rights (2022), *Arrests in Russia at Protests Over Troop Mobilization* (retrieved December 27, 2022 from https://reliefweb.int/report/russian-federation/arrests-russia-protests-over-troop-mobilization).

Weidmann, N. and Dainotti, A. (2022), Attack or Block: Repertoires of Digital Censorship in Autocracies, *Journal of Information Technology & Politics*, 20(1), pp. 60-73.

Zayani, M. (2015), *Networked Publics and Digital Contention: The Politics of Everyday Life in Tunisia*, US: Oxford University Press.