The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 29-50.

Russia's Digital Repression Landscape: Unraveling the Kremlin's Digital Repression Tactics

ANASTASSIYA MAHON AND SCOTT WALKER

Abstract

Building upon the existing scholarship on Russia's departure from liberalism, this paper analyzes the Kremlin's recent use of digital technologies to curb political dissent, constrain civil society, and control the media. Investigating both historical precedents and contemporary strategies, the study reveals two key trends. Firstly, it uncovers a convergence of traditional and digital repression, challenging simplistic views of the regime. Secondly, it highlights the remarkable effectiveness of covert physical coercion, deeply rooted in the collective memory of the Soviet era, as a means to deter anti-government sentiments. The paper also elucidates the prioritization of specific digital repression tools, drawing connections between efficacy, historical memory, and cost considerations.

Keywords: Russia, digital repression, illiberal regime, illiberal policymaking, invasion of Ukraine, information control

Anastassiya Mahon
Associate Lecturer in Security Studies, Aberystwyth University, UK
anm155@aber.ac.uk

Scott Walker
Independent Researcher
tabernash@hotmail.com

DOI: 10.53483/XCQU3579

For decades, the Kremlin has employed a variety of technologies to suppress dissent, conduct surveillance on the civilian population, and launch disinformation campaigns, among other tactics. This use of technology has gained more international and media attention since the start of the Russo-Ukrainian War in early 2022.[1] In this paper, "digital repression" refers to "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."[2] While these technologies are used for a number of illiberal purposes, including the manipulation of social media, cyberattacks, and disinformation campaigns, little attention has been paid to the continuity of repression in Russia. Meanwhile, Russia's illiberal use of technology has a historical and cultural context, which becomes more important to address as the state is building on the well-known traditional repression approaches to venture out in the online space.

Russia has a long history of information control that can be traced back to pre-revolutionary times. For example, Marxist thinkers such as Nikolai Bukharin, Karl Kautsky, and Rosa Luxemburg emphasized the importance of resource control and systemic oppression for the regime's ability to function.[3] Bukharin referred to the pre-revolutionary oppression in Russia as systemic: "a system of gagging and oppression such as Russia had not known since the failure of the first Revolution. The labor press was suspended, labor unions dissolved, striking workers were sent to the front, were thrown into prison or summarily shot."[4] In 1909, Kautsky and Algie Martin Simons denounced the media for its influence on the people: "the colourless unprincipled press, which demoralises and poisons large sections of the community,"[5] reflecting a focus on the importance of the control over information channels. The state's repressive tactics did not ease after the Bolshevik Revolution. On the contrary, the Soviet Union continued to invest in information control and shaping the political narrative.

Following the Revolution's ideological legacy, the Soviet regime tightly regulated information channels, forcing citizens to rely on underground methods of generating or receiving dissenting information. In the post-Soviet era, the media environment has not become as liberal as in the West. Despite the post-Soviet privatization of the media, the state continues to impose control and promote self-censorship. Following the dissolution of the Soviet Union in 1991, Russia underwent a turbulent transition to democracy. Under Vladimir Putin, the government implemented measures to restrict independent journalism and dissenting voices, leading the country further away from the democratic ideals that the country had made efforts to espouse during the early 1990s. The regime also applied restrictive measures to society, leading to a dramatic closing of the public space and a notable decrease in political activism.[6]

[1] Sophie Bushwick, "Russia Is Using 'Digital Repression' to Suppress Dissent: An Interview with Jennifer Earl," *Scientific American*, March 15, 2022, https://www.scientificamerican.com/article/russia-is-using-digital-repression-to-suppress-dissent/; Steven Feldstein, "Disentangling the Digital Battlefield: How the Internet Has Changed War," War on the Rocks (blog), December 7, 2022, https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/.

[2] Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Oxford: Oxford University Press, 2021), 25.

[3] Nikolai Bukharin, "The Russian Revolution and Its Significance," *The Class Struggle* 1, no. 1 (1917), https://www.marxists.org/archive/bukharin/works/1917/rev.htm; Karl Kautsky and Algie Martin Simons, *The Road to Power* (Germany: S. A. Bloch, 1909); Rosa Luxemburg, "The Russian Tragedy," *Spartacus* 11 (September 1918), https://www.marxists.org/archive/luxemburg/1918/09/11.htm.

[4] Bukharin, "The Russian Revolution and Its Significance."

[5] Kautsky and Simons, *The Road to Power*, 40.

[6] Maria Lipman, "At the Turning Point to Repression," *Russian Politics & Law* 54, no. 4 (July, 2016): 341–350, https://doi.org/10.1080/10611940.2016.1207468.

While the government's interference in the media environment has not achieved the totalitarian level of control as the Soviet Union saw, Moscow's increased control of media outlets has led to their alignment with state interests, with independent journalists facing threats, violence, and even assassination attempts, fostering an atmosphere of fear and self-censorship.[7] Additionally, laws were enacted regulating the internet, curbing online freedom of expression, and allowing the regime to circumvent traditional political decision-making channels.[8]

State-owned and state-influenced media became predominant, enabling pro-government narratives to dominate and marginalize opposition viewpoints. This media control played a crucial role in shaping public opinion, reinforcing the government's authority, and suppressing dissent.[9] Thus, when examining Russia's political history of repression, the continuity of historical approaches to information control becomes increasingly evident. Drawing from a legacy rooted in systemic oppression, the Kremlin's deployment of various technologies for illiberal purposes, as well as the use of illiberal technologies, represents a modern manifestation of a longstanding commitment to shaping political narratives and stifling dissent. In this paper, we recognize that there is a distinction between the usage of technologies for illiberal purposes, meaning that many technologies that we use for everyday life can be weaponized by illiberal actors for surveillance and repression purposes (for example, app tracking, mobile services, or online banking), and purposefully illiberal technologies (that is, technologies whose main purpose is to aid an illiberal actor with surveillance, repression, or a breach of social contract).[10]

However, while making a distinction between technologies that are not specifically intended to be used for repressive purposes and those technologies that are expressly designed for repressive purposes is important, the main focus of this paper is to document the ways Moscow uses digital technologies for achieving illiberal goals, thus expanding the context in which digital repression can be analyzed and providing analysis of the emerging pattens in the Kremlin's digital repression landscape. Previous studies have addressed topics such as digital authoritarianism[11] and

[7] Michael J. Bazyler and Eugene Sadovoy, "Government Regulation and Privatization of Electronic Mass Media in Russia and the Other Former Soviet Republics," *Whittier Law Review* 14 no. 2 (1993): 427, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/whitlr14&section=25; Brian McNair, "Power, Profit, Corruption, and Lies: The Russian Media in the 1990s," in *De-Westernizing Media Studies*, ed. James Curran and Myung-Jin Park (London: Routledge, 2005), 69–83, https://www.taylorfrancis.com/chapters/edit/10.4324/9780203981764-8/power-profit-corruption-lies-brian-mcnair.

[8] Anastassiya Mahon and Scott Walker, "Counterterrorism Policy in the Russian Federation: Furthering the Needs of the Regime," *Studies of Transition States and Societies* 15, no. 1 (2023): 3–17, https://doi.org/10.58036/stss.v15i1.1097.

[9] Renira Rampazzo Gambarato and Sergei Andreevich Medvedev, "Grassroots Political Campaign in Russia: Alexey Navalny and Transmedia Strategies for Democratic Development," in *Promoting Social Change and Democracy through Information Technology* (Hershey, Penn.: IGI Global, 2015), 165–192, https://www.igi-global.com/chapter/grassroots-political-campaign-in-russia/134258; Sofya Glazunova, " 'Four Populisms' of Alexey Navalny: An Analysis of Russian Non-Systemic Opposition Discourse on YouTube," *Media and Communication* 8, no. 4 (October 2020): 121–132, https://eprints.qut.edu.au/203451; Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

[10] Scott J. Shackelford, Frédérick Douzet, and Christopher Ankersen, *Cyber Peace: Charting a Path toward a Sustainable, Stable, and Secure Cyberspace*, Social Sciences (Cambridge, UK: Cambridge University Press, 2022).

[11] Richard Fontaine and Kara Frederick, "The Autocrat's New Tool Kit," *Wall Street Journal*, March 15, 2019, https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637; Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," Brookings Institution *Policy Brief, Democracy and Disorder Series*, 2019, 1–22, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

artificial intelligence and its influence on repressive technologies,[12] paving the way to rethink the role of digital technologies in repression and illiberalism. This paper approaches the subject of digital repression from the position of expanding upon the traditional repression approaches employed by the Russian state to analyze how and why the regime ventures out into the online space.[13]

This paper's mapping[14] of Russia's digital repression landscape provides insights into government tactics: by contextualizing Russia's approach, it identifies broader authoritarian trends in the digital space, while also outlining how potential international efforts might promote an anti-regime agenda in Russia. It also contributes to the literature on autocratic resilience, particularly to analyzing the ways of deepening autocratization in already authoritarian countries.[15]

The paper is structured as follows: The first section provides a concise overview of the research methodology employed to analyze Russia's utilization of illiberal digital technology. Then, in the following section, we apply Earl et al.'s typology of digital repression to explore Russia's distinctive use of illiberal technologies, emphasizing their role in limiting opposition to the regime and suppressing dissent. This section also delves into the extent to which Russia's recent digital repression profile relies on both physical control and information control technologies. The "Discussion" section addresses the origins of Russia's current digital repression profile. We posit that a combination of historical developments, political realities, and economic constraints collectively elucidates the rationale behind Russia's choices in digital repression. Finally, in the conclusion, we summarize the main points presented throughout the paper, offering a cohesive conclusion to our analysis.

Methodology

Technologies are integral instruments the regime utilizes to manage dissent and political opposition. In our investigation, we adopt a typology of digital repression introduced by Earl et al. in "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review." This work provides a framework for analyzing and understanding the complexities of digital repression, considering various influencing factors, and linking it to the broader discussion on traditional oppression. The typology helps with recognizing relationships between different types of digital coercion and control, understanding the role of infrastructure, linking threat perception to digital repression, and integrating these with existing research on repression.

[12] Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," *Journal of Democracy* 30, no. 1 (2019): 40–52, https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-how-artificial-intelligence-is-reshaping-repression; Feldstein, *The Rise of Digital Repression*; Allie Funk, Adrian Shahbaz, and Kian Vesteinsson, "The Repressive Power of Artificial Intelligence" Washington, DC: Freedom House, 2023, https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence.

[13] Jennifer Earl, Thomas V. Maher, and Jennifer Pan, "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review," *Science Advances* 8, no. 10 (March 2022): 1–15, https://www.science.org/doi/epdf/10.1126/sciadv.abl8198.

[14] Fiona Campbell, Andrea C. Tricco, Zachary Munn, Danielle Pollock, Ashrita Saran, Anthea Sutton, Howard White, and Hanan Khalil, "Mapping Reviews, Scoping Reviews, and Evidence and Gap Maps (EGMs): The Same but Different— the 'Big Picture' Review Family," *Systematic Reviews* 12, no. 1 (March, 2023): 45, https://doi.org/10.1186/s13643-023-02178-5.

[15] Elina Sinkkonen, "Dynamic Dictators: Improving the Research Agenda on Autocratization and Authoritarian Resilience," *Democratization* 28, no. 6 (August 2021): 1172–1190, https://doi.org/10.1080/13510347.2021.1903881.

Our analysis concentrates exclusively on the first of the two levels of the Earl et al. typology, which focus on digital repression organized by the state or entities directly under state control, or what Earl et al. term "state agents tightly coupled with national political officials."[16] We exclude the actors in the second level of the Earl et al. typology, which encompasses those loosely affiliated with the state, as well as private actors. We do this because, in the Russian context, digital repression is usually utilized by the regime itself rather than by other actors. While local and regional governments may play a secondary role, the Kremlin remains the primary source of political changes shaping the present environment. Notably, the involvement of private actors in digital repression is limited, with relatively few entities (such a hackers) opting at times to cooperating with the government in such endeavors. Such a repressive environment has been characterized by Tatiana Stanovaya as "Russia's Digital Gulag."[17]

According to the Earl et al. typology, digital repression manifests itself in two principal forms: (1) physical control and (2) information control. Physical control encompasses government utilization of overt and covert means, including violence, arrests, and surveillance against digital activists, as well as channeling through digital technology to incentivize cooperation or enforce compliance. Information control involves overt and covert tactics such as restricting internet connectivity, content filtering, and the dissemination of distracting or misleading information.

In order to analyze the Kremlin's digital repression landscape, this paper accepts the theoretical distinction between overt and covert means of digital repression, as it aids our discussion in three major ways. First, it allows us to bring nuance to how we characterize the repression techniques and goals of Moscow's use of digital technologies. This is helpful in understanding the continuity of Russia's digital repression through the use of traditional forms of repression and the Kremlin's preferences for certain approaches. Second, differentiating between overt and covert repression technologies has significant implications for understanding the cost-benefit analysis of the repressor states, as we still know little about how repression in the digital space shifts and changes the cost-benefit analysis for an illiberal regime.[18] It is possible that illiberal regimes may choose to move towards those digital repression techniques that are more cost-beneficial, even if they do not present an opportunity to showcase the regime's approach (that is, the techniques that are used are covert). Third, a better understanding of the subtle (or covert) ways of using technology for illiberal purposes has the potential to improve the chances of political dissent resisting the digital repression landscape in Russia.

While conducting an evidence-based systemic review proves difficult due to the nature of the research[19] and the discrepancy between published evidence in English and Russian, mapping offers an opportunity to provide a more comprehensive overview of the digital repression landscape in Russia. This approach to analyzing Russia's digital repression landscape helps to identify evidence and research gaps, which, in turn, should guide future research.[20]In order to contextualize Russia's

[16] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism," 2.

[17] Tatiana Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer," Carnegie Endowment for International Peace, April 17, 2023, https://carnegieendowment.org/politika/89553.

[18] Shackelford, Douzet, and Ankersen, *Cyber Peace*.

[19] Campbell et al., "Mapping Reviews, Scoping Reviews, and Evidence and Gap Maps (EGMs)."

[20] Ashrita Saran, Howard White, and Hannah Kuper, "Evidence and Gap Map of Studies Assessing the Effectiveness of Interventions for People with Disabilities in Low-and Middle-Income Countries," *Campbell Systematic Reviews* 16, no. 1 (March 2020): e1070, https://doi.org/10.1002/cl2.1070.

digital repression landscape and map Moscow's usage of digital technologies for illiberal purposes, we analyze Russia's use of digital repression over the last decade (2013–2023). Our analysis is restricted to this timeframe to focus on more recent technological developments rather than on ones that were used during earlier periods and may now be irrelevant or outdated.

Russia's Digital Repression Landscape: How Moscow Uses Digital Repression Tools

Physical Control

Earl et al. describe physical control as the exertion of influence or authority over digital activists and their activities through various tangible actions.[21] This control can manifest in both coercive and non-coercive forms. Coercive physical control involves overt actions, such as arrests, violence, or harassment, intended to raise the costs of engaging in digital social movement activities. On the other hand, non-coercive physical control, termed "channeling," seeks to guide activists through incentivizing preferred behaviors and expressions without direct physical force.[22] According to Earl et al., the concept of physical control builds on the traditional approaches to repression, both historical and contemporary, and encompasses a spectrum of strategies aimed at shaping the course of digital activism, emphasizing the tangible measures taken to influence activists and their activities.[23]

Physical Coercion

Physical coercion refers to a form of digital repression characterized by visible actions intended to raise the costs of engaging in digital social movement activities.[24] These actions can involve, but are not limited to, direct physical force, such as arrests, violence, or harassment, with the aim of deterring or suppressing digital activism. The term "coercion" emphasizes the use of forceful measures to influence the behavior of digital activists, and "physical" underscores the tangible and observable nature of these interventions. Physical coercion represents a clear and visible exertion of power to hinder or control digital social movements. This type of digital repression can be seen as one of the most observable, as cases of physical coercion are often documented by nongovernmental organizations, if not by the state itself.

Overt Physical Coercion

The concept of overt physical coercion refers to a form of coercion whereby explicit and visible physical force is wielded to exert control over digital activists and their endeavors.[25] This facet of repression involves direct actions by the Russian state with the explicit aim of escalating the costs associated with engaging in digital social movement activities. Examples of overt physical coercion can be arrests of political bloggers, instances of physical violence perpetrated by members of the military or national police against online activists, and the initiation of harassment through legal means.[26] The term "overt" underscores the transparent and observable nature

[21] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[22] Earl, Maher, and Pan.

[23] Earl, Maher, and Pan.

[24] Earl, Maher, and Pan.

[25] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[26] Shackelford, Douzet, and Ankersen, *Cyber Peace*.

of these coercive actions, emphasizing the intent to conspicuously influence and discourage digital activism.[27]

Since the annexation of Crimea in 2014, the Kremlin has been consistently introducing more overt physical coercion measures to restrict public expression of anti-expansionist and, later, anti-war sentiments, aiming to impose the state's narrative of Russia being under attack such that its survival might be endangered, as well as to dissuade the public from contradicting said narrative in the online space. The annexation of Crimea has resulted in a wave of various anti-government and anti-expansionist attitudes from the Russian public, so in order to be able to control the narrative, the Russian state has reacted by tightening its grip on protests and public displays of discontent with the government. Much of the government's suppression of anti-war protests in the online space has been carried out through prosecuting individual protesters, such as when an individual posts or reshares anti-regime or anti-war content online. However, according to the 2020 Blackscreen Report, in 2015–2019, the number of prosecutions for online activity had not significantly increased.[28] Instead, the sentences that these cases received have become more severe over the years, with non-custodial sentences decreasing and more people being incarcerated: from 18 prison sentences in 2015 to 38 in 2019.[29] This movement towards heavier sentences (prison time as opposed to non-custodial sentences) frames the state's understanding of the cost-benefit balance of digital repression, which suggests that that this policy is intended to raise the cost of online activism.

Over half of the cases brought to trial have been regarding publications on the Russian online platform VKontakte (which means "InContact"), a platform similar to Facebook that was created in Russia and is popular there.[30] After banning the Meta corporation, including Facebook and Instagram,[31] Moscow is paying close attention to local social networks, such as VKontakte, which shows the regime's extensive capabilities for monitoring activity on them as much as the intent to do so. Following the full-scale Russian invasion of Ukraine in February 2022, the Russian state has accelerated its prosecution of online displays of dissent and political discontent with the government and Vladimir Putin on the grounds of "disrespect of [*sic*] authority."[32] This overt representation of the consequences that even public figures can face for their opinions voiced online works towards raising the cost of expressing any anti-war sentiments significantly. In these conditions, few would risk their freedom and future prospects to engage in online activism—thus the state is achieving its goal of imposing the desired high cost for political activism.[33]

The government's approach of intimidation and telegraphing a message of control has successfully deterred Russian citizens from expressing their grievances with

[27] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[28] Sarkis Darbinyan, Ekaterina Abashina, and Artem Kozlyuk, "Blacksreen Report" RosKomSvoboda website (a public organisation that monitors digital rights protection in Russia), 2020, https://docs.google.com/document/d/17-2Z3_51FF1nmKMrH3cBPXCuPSHC05Lk/edit?pli=1.

[29] Darbinyan, Abashina, and Kozlyuk, "Blackscreen Report," 5.

[30] Darbinyan, Abashina, and Kozlyuk, "Blacksreen Report"; Perrine Poupin, "Social Media and State Repression: The Case of *VKontakte* and the Anti-Garbage Protest in Shies, in Far Northern Russia," *First Monday* vol. 26, no. 5 (May 2021), https://firstmonday.org/ojs/index.php/fm/article/view/11711.

[31] "Telegram Channel of Roskomnadzor," March 4, 2022, https://t.me/rkn_tg/206.

[32] "Submission to the United Nations Human Rights Council on the Universal Periodic Review 44th Session Fourth Cycle for the Russian Federation," Article 19, Access Now, Justice for Journalists: Foundation for International Investigations of Crime against Media, and OVD-Info, April 4, 2023, https://www.article19.org/wp-content/uploads/2023/04/Russia_Joint-UPR-Submission_JFJ_OVD_A19_Access_Final-.pdf.

[33] Feldstein, *The Rise of Digital Repression*.

the regime, especially regarding Russia's actions in Ukraine. Following Earl et al.'s theorizing of overt physical coercion as tangible tactics to increase the people's fears of prosecution, the Kremlin has successfully used this approach to deter political activism.[34]

Covert Physical Coercion

In the landscape of digital repression, the notion of "covert physical coercion signifies a form of coercion where physical force is surreptitiously employed to shape and control the activities of digital activists."[35] Unlike overt methods, covert physical coercion involves actions taken by the Russian state with the aim of heightening the costs associated with participating in digital social movement activities, all while strategically maintaining an elusive and less visible presence. Examples encompass discreet surveillance, subtle legal maneuvers such as collecting *kompromat* (a term from Russia's Stalinist times meaning "compromising material") on those who are targeted, or subjecting individuals to unattributed physical harassment.[36] The term "covert" underscores the discreet nature of these coercive tactics, highlighting the intentional effort to exert influence while concealing the mechanisms employed.

The Russian government habitually uses covert physical control methods to identify, discourage, and eventually raise the cost of activism for dissenting voices. Surveillance techniques are used to track dissidents and gather information, which can be used against people to restrict their freedom of movement and speech.[37] Some of this surveillance can be done to build cases, or to collect *kompromat* that can be used against activists to build criminal cases later on. For example, the Russian state has used its counterterrorism policy, which grants counterterrorism actors a wide mandate with little scrutiny, to prosecute what it perceives as a threat to the state while setting a deterrence example for potential anti-government sentiment.[38] In the case of *Set'* (The Network), the prosecution's arguments were based on evidence collected via online surveillance by undercover agents.[39] The case resulted in the members of the group receiving from 6 to 18 years in prison on terrorism charges.[40] The case has been widely criticized as unjust and unfair,[41] but it has not dissuaded the state from using covert physical coercion tactics to raise the cost of expressing any anti-government political views.

Moscow has increased online surveillance following the invasion of Ukraine, especially after its mobilization efforts of September 2022, when men of military recruitment age tried to leave Russia to avoid being drafted. The state used various online tracking tools to prevent them from leaving, thereby revealing its covert digital coercion capabilities. The state employed tracking of social media accounts, monitored banking activities, and used facial recognition software, to name a few

[34] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[35] Earl, Maher, and Pan.

[36] Earl, Maher, and Pan.

[37] Feldstein, *The Rise of Digital Repression*.

[38] Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

[39] Oksana Chizh, " 'Kem ja dolzhen stat' - fashistom?' Delo 'Seti' doshlo do prigovora," BBC News Russia, February 4, 2020, https://www.bbc.com/russian/features-51362582; Andrey Kaganskikh, " 'The Network': How Russian Security Services Are Targeting Russian Anarchists and Anti-Fascists," Open Democracy, April 27, 2018, https://www.opendemocracy.net/en/odr/the-network/.

[40] Kaganskikh, " 'The Network.' "

[41] Change.org, " 'Trebuem Prekratit' Sudy Po Delu 'Seti' i Rassledovat' Fakty Pytok!" Change.org, April 19, 2019, https://www.change.org/p/delo-seti-stopfsb.

such methods—an unprecedent level of surveillance in post-Soviet Russia.[42] Non-governmental organizations promoting anti-war sentiment have issued handbooks and guides on how to avoid being tracked by the government, mentioning the use of geolocation, bank cards, and various governmental services,[43] in line with Earl et al.'s theorizing on the government's covert physical control tactics leading to increasing tension between activists and authoritarian regimes.[44]

Physical Channeling

Physical channeling refers to a form of digital repression characterized by attempts to influence or control digital activists and their activities through non-coercive means.[45] Unlike physical coercion, channeling involves incentivizing preferred forms of expression and behavior, steering digital activists toward conforming actions without resorting to overt force.[46] This form of repression aims to shape the trajectory of digital social movement activities through indirect, nonviolent means. The term "channeling" underscores the intention to guide and direct actions, providing insight into how regulatory frameworks and incentives can be strategically employed to control the course of digital activism.

Overt physical channeling is an explicit strategy aimed at influencing the conduct of digital activists through non-coercive means. This method involves the implementation of clear-cut laws, policies, or online platforms explicitly crafted to overtly promote desired behaviors while discouraging others.[47] An example of such a strategy can be an online platform that allows citizens to lodge their grievances with all branches of the government, and is run by the Prosecutor General's Office of the Russian Federation.[48] This service can be used to report any inappropriate material found online, but it is prone to abuse by someone who might want to degrade or vilify another person for their anti-government and anti-war political views. While there is an option to lodge a complaint anonymously, using the unified portal as a registered user would immediately disclose the complaining individual's personal information, making it easier for the regime to monitor them to collect information on both complainers and those they complain against. Unsurprisingly, the government encourages the usage of online tools for lodging grievances; however, at the same time the setup of this online tool leaves a loophole for increased surveilling and tracking. Thus, the state promotes desired behaviors (participation in the nation's life) while leaving itself with multiple options for abusing the information that is shared through these channels.

While overt physical channeling clearly addresses the state's desire to encourage certain types of behavior, covert physical channeling refers to a form of digital repression characterized by discreet and concealed efforts to guide or control

[42] Farah Qasem Mohammed and Basim Muftin Badr, "A Critical Discourse Analysis of Russian-Ukrainian Crisis in Selected English News Channels," *Nasaq* 37, no. 7 (March 2023), https://www.iasj.net/iasj/download/f5d66f6a36c5a801; Pavel K. Baev, "The Russian War Machine Fails the Tests of War," *Current History* 122, no. 846 (March 2023): 243–248, https://online.ucpress.edu/currenthistory/article-abstract/122/846/243/197313.

[43] Iditelesom.org, "Help Iditelesom," May 17, 2023, https://iditelesom.org/en/; Julia Selikhova, "How Not to Fall under the Law on Electronic Conscription," Holod.ru, April 17, 2023, https://holod.media/2023/04/17/zakon-ob-elektronnykh-povestkakh/.

[44] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[45] Earl, Maher, and Pan.

[46] Earl, Maher, and Pan.

[47] Earl, Maher, and Pan.

[48] The portal for the Prosecutor General's Office of the Russian Federation can be found here: https://epp.genproc.gov.ru/web/gprf/internet-reception/personal-receptionrequest.

the behavior of activists through non-coercive means.[49] Unlike overt methods, covert physical channeling involves strategies that are not overtly visible or easily discernible. This could include the implementation of laws and policies that subtly incentivize certain behaviors while discouraging others, all while maintaining a degree of secrecy. The term "covert" underscores the clandestine nature of these efforts, emphasizing the intention to subtly influence potential dissent without overtly signaling these interventions.

An example of covert physical channeling can be seen in the decriminalizing of the offenses outlined in Article 282 of the Criminal Code of the Russian Federation, an instrument that has been widely used to persecute people for online activity. Instead, a potential offender now faces an initial warning as opposed to a criminal case. The decriminalization of these Article 282 offenses led to an almost tenfold decrease in the number of prosecutions, allowing the regime to continue to use the article to covertly surveil and threaten citizens thus deterring them from protesting online or voicing anti-government opinions.[50] Thus, while the decriminalization of the offenses listed in Article 282 might at first glance be seen as a positive step toward a reduction in digital repression, it is still being used for limiting online dissent. However, following the decriminalization of Article 282 offenses, the overall number of incarcerations for online activity did not actually go down. Instead, the government has begun to prosecute online activity using other articles of the Criminal Code more frequently.[51] For instance, Article 20.1 of the Administrative Code was amended to add "disrespect for power" to the list of offenses for which people criticizing Putin could be prosecuted. In 2019, 44 out of 78 cases brought to court on charges of breaching Article 20.1 cited "disrespect for power" as the reason for prosecution.[52]

This development reveals two things: first, following the annexation of Crimea, people were taking their grievances online and voicing their opinions; and second, the regime was prepared for such a turn of events and chose to deal with this through covert physical and digital repression tools, as opposed to overt physical coercion in the form of arrests or probation. It is clear that the regime updates the punitive system of persecuting dissent in the online space, which is indicative of the regime's motivation to keep digital repression at least at the same level (or potentially higher) as with the case of traditional repression. This suggests that the regime is responsive to the challenges that the existing system of repression is experiencing.

Another example of covert physical channeling is the 2023 change towards more centralized digital control over conscription. The conscription-eligible population may now face restrictions on movement and their other rights (such as driving, buying and selling property, and conducting banking and business activities) if they do not properly respond to the draft papers. There is no leniency in the government's attitude despite the draft notices being served electronically, which means that people might be unaware that the notices were served because they might have no access to online government services.[53] Since November 1, 2024 draft notices will be served electronically via the public service portal Gosuslugi, and the notice would

[49] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[50] Darbinyan, Abashina, and Kozlyuk, "Blacksreen Report," 12.

[51] Darbinyan, Abashina, and Kozlyuk.

[52] Darbinyan, Abashina, and Kozlyuk, 8.

[53] Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer."

be considered as having been delivered seven days after it has been placed on the register even if the recipient does not have a Gosuslugi account.[54]

The government has thus created a system that promotes a specific pro-regime behavior (joining the army) and increases the costs of going against the regime (avoiding military service). Stanovaya terms this refusal to comply with the new system a "social death,"[55] when such refusal leads to engaging in actions like registering for a government identification, pension, or social services becoming a significant obstacle to people's ability to conduct their everyday activities. This government technique can be seen as a part of the digital gulag that Russia has been creating, akin to China's surveillance and monitoring system.[56] Therefore, Russian citizens find themselves in a difficult situation: they must use digital services in order to have a legal and documented life in Russia, but the digital footprint of the information that they share with digital government services can easily be used against them.

Information Control

The control of information both in the media and online space has become an inalienable and paramount part of political processes. Greg McLaughlin aptly summarizes these changes: "Whereas military power and global reach were key points of confrontation during the old Cold War, now these are information and geo-economics with the West way out in the lead."[57] This section looks at information control, in both its coercive and non-coercive (channeling) forms, in relation to the political and societal changes that have followed.

According to Earl et al., "information control" refers to the manipulation, regulation, or restriction of information flows to shape narratives, control public discourse, and suppress dissent.[58] This concept encompasses various tactics that are employed by entities like the Kremlin to influence public opinion and maintain political control. Information control involves not only such traditional methods as censorship and propaganda, but also modern strategies, including the use of technology and online platforms to manage and manipulate information dissemination to change people's behavior.[59] The historical roots of information control in Russia can be traced back to pre-revolutionary, tsarist times, reflecting a consistent effort by the Kremlin to manage and shape the information landscape for political purposes.[60]

Information Coercion

Information coercion refers to the use of various tactics and strategies to manipulate, control, or influence the flow of information with the aim of achieving specific objectives. It involves the intentional exertion of pressure or force on individuals, groups, or the general public through the manipulation of information channels. Information coercion can take different forms, including propaganda, censorship,

[54] "Briefing: Russia Setting Up Electronic 'Single Register' of Men Subject to Draft—BBC Monitoring," accessed June 5, 2024, https://monitoring.bbc.co.uk/product/b0001j3c.

[55] Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer."

[56] Polyakova and Meserole, "Exporting Digital Authoritarianism;" Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer."

[57] Greg McLaughlin, *Russia and the Media: The Makings of a New Cold War* (London: Pluto Press, 2020).

[58] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[59] Earl, Maher, and Pan, 6.

[60] Bukharin, "The Russian Revolution and Its Significance."

disinformation, and other methods designed to shape perceptions, control narratives, or achieve particular outcomes.[61] The coercive aspect implies that there is an intentional effort to compel or influence behavior, beliefs, or opinions by leveraging the power of information.

Information coercion can occur in various contexts, such as political campaigns, military operations, social movements, or even in commercial and corporate settings. It is essential to recognize that information coercion can be either overt, conducted openly and acknowledged; or covert, where the manipulative efforts are concealed or not readily apparent. The effectiveness of information coercion often depends on the degree of control or influence wielded over communication channels and the target audience.

Overt Information Coercion

Examples of overt information coercion include the government restricting access to certain information via limiting or slowing internet connectivity, state-controlled media pushing a particular political agenda, or the spreading of misinformation to influence public opinion via state-based content filtering.[62] The control of access to the internet and news is paramount for successful information control: internet shutdowns can be used as a brute force technique to suppress dissent.[63] In response to perceived discriminatory actions against Russian media by Facebook, the Russian state implemented restrictions on access to both Facebook and Instagram shortly after Russia's full-scale invasion of Ukraine. The rationale behind this action is ostensibly grounded in the principle of safeguarding freedom of speech and the need to maintain influence over the flow of information.[64]

Control over the media and the internet, as discussed by Daniëlle Flonk, plays a pivotal role in the Kremlin's control of the political narrative in Russia.[65] The regime exercises dominance over a significant portion of the media landscape, including television channels, newspapers, and online news platforms. This authoritative control allows the regime to have a significant impact on the levels of opposition expression[66] and to mold public opinion by steering the narratives disseminated to the populace and preventing Russian citizens from accessing alternative news sources.[67] Any remaining media outlets striving for independence face silencing and eventual expulsion, particularly in the aftermath of the Ukraine invasion.[68]

Simultaneously, the Russian government employs measures to limit access to foreign media within the country. The Law on Foreign Agents, enacted to label

[61] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

[62] Earl, Maher, and Pan.

[63] Earl, Maher, and Pan.

[64] Telegram Channel of Roskomnadzor.

[65] Daniëlle Flonk, Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control," *International Affairs* 97, no. 6 (November 2021): 1925–1944, https://doi.org/10.1093/ia/iiab146.

[66] Grigore Pop-Eleches and Lucan A. Way, "Censorship and the Impact of Repression on Dissent," *American Journal of Political Science* 67, no. 2 (April 2023): 456–471, https://doi.org/10.1111/ajps.12633; Sergei Guriev and Daniel Treisman, "The Popularity of Authoritarian Leaders: A Cross-National Investigation," *World Politics* 72, no. 4 (2020): 601–638, https://www.cambridge.org/core/journals/world-politics/article/popularity-of-authoritarian-leaders/3EB2352F226F8904DBB0293A83F10622.

[67] Freedom House, "Russia: Freedom on the Net 2022 Country Report," Washington, DC: Freedom House (think tank), 2022, https://freedomhouse.org/country/russia/freedom-net/2022.

[68] Reporters Without Borders, "Russia: Stifling Atmosphere for Independent Journalists," RSF website (international nonprofit organization), 2022, https://rsf.org/en/russia.

individuals receiving any form of foreign support as agents of foreign governments, has been instrumental in this strategy.[69] In the wake of the 2022 invasion, this law has been wielded to designate even regime critics as foreign agents, severely curbing their operational capabilities within Russia. Notably, this legislation is not confined to political adversaries alone: it has been applied to diverse individuals, including artists, bloggers, and even those uninvolved in politics. The consequences extend beyond mere labeling, compelling those affected to either curtail their activities within Russia or seek relocation.

Covert Information Coercion

Covert state control of information is evident through various covert measures aimed at shaping the narrative and controlling access to online content. An illiberal regime is expected to employ internet filtering and content-blocking mechanisms, and compelling internet service providers to restrict access to websites critical of the authorities, or to those associated with political dissent.[70] This extends to the maintenance of a registry of banned websites by the Federal Service for the Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), contributing to a controlled online environment. However, Moscow went further than just banning an occasional website for political purposes, as it decided to block popular Western social media platforms such as Facebook and Instagram.[71] Thus, by denying access to Western media, Moscow seeks to reduce the Russian population's exposure to Western values and critical takes on the Kremlin's policies.

There is also evidence of the Russian government engaging in social media manipulation through the use of bots and trolls.[72] These covert influence campaigns seek to disseminate disinformation, shape public opinion, and stifle dissenting voices on social media platforms. The manipulation of online discussions and the dissemination of state-approved narratives underscore the efforts to control the flow of information and maintain a certain discourse within the digital realm. Collectively, these tactics highlight the government's covert strategies to influence public perception and limit access to information deemed undesirable or threatening to its interests.[73] However, due to the nature of covert state information control, it is challenging to measure the full extent of this tool's usage by Moscow.

Information Channeling

Information channeling refers to the deliberate and strategic direction or control of information flows through specific communication channels, influencing the production and consumption of information.[74] This digital repression technique involves directing information along predetermined pathways or platforms to influence, shape, or control the dissemination and reception of messages. Information channeling can be employed for various purposes, including shaping public opinion, promoting a particular narrative, or advancing specific agendas.

[69] Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

[70] Shackelford, Douzet, and Ankersen, *Cyber Peace*.

[71] Mike Isaac and Adam Satariano, "Russia Blocks Facebook inside the Country, as the Kremlin Moves to Stifle Dissent," *New York Times*, March 4, 2022, https://www.nytimes.com/2022/03/04/world/europe/russia-facebook-ukraine.html.

[72] Andrew Roth, "Pro-Putin Bots Are Dominating Russian Political Talk on Twitter," *Washington Post*, June 20, 2017, https://www.washingtonpost.com/world/europe/pro-putin-politics-bots-are-flooding-russian-twitter-oxford-based-studysays/2017/06/20/19c35d6e-5474-11e7-840b-512026319da7_story.html.

[73] Shackelford, Douzet, and Ankersen, *Cyber Peace*.

[74] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

In practice, information channeling may involve utilizing media outlets, social media platforms, or other communication channels to convey messages in a targeted manner. This strategic approach is used by the government to manage the narrative, control the framing of issues, and influence the perception of information consumers. The concept of information channeling underscores the importance of understanding how information is guided through various channels and the impact this has on the shaping of public discourse and opinion. It can be observed in legitimate communication strategies, in manipulative tactics aimed at steering perceptions in a particular direction, and in both overt and covert ways.

Several examples of overt information channeling can be seen in Vladimir Putin's justification for Russia's invasion of Ukraine. Putin's article, "On the Historical Unity of Russians and Ukrainians,"[75] was published in July 2021. Pre-dating his well-known address[76] right before Russia invaded Ukraine in February 2022, it claims to be a frank and open explanation in which Putin lays out the reasons why the conflict in Ukraine is "the result of deliberate efforts by those forces that have always sought to undermine our unity."[77] Putin continues to put the blame on external forces that are coming for Russia, painting a dark and uncertain future for his country if no measures are taken to counter those evil forces. This illustrates a high level of overt information channeling, as evident by the head of state being complicit in spreading propaganda.

The state engaging in overt information channeling means that it deliberately chooses certain channels to convey messages, to influence public opinion, or to shape the narrative surrounding particular issues. Illiberal regimes often tend to opt for more control over information flows. In this case, the Kremlin's desire to keep a tight grip on the flow of information regarding the invasion of Ukraine can be seen in the introduction of various censorship laws that severely punish the sharing of anything but the government's official stance on the issue.[78] Overt information channeling can take various forms, including official statements, press releases, public speeches, or the promotion of specific content through openly acknowledged media channels. The goal is to guide the dissemination of information openly and intentionally in a manner that aligns with the objectives or perspectives of the government.

On the other hand, covert information channeling refers to the discreet and concealed management or manipulation of the flow of information through specific communication channels. In this context, "covert" signifies that the actions taken to direct or influence information are intentionally hidden, or at least not openly acknowledged.[79] Covert information channeling can manifest itself through tactics such as the surreptitious dissemination of information, manipulation of online platforms, or undisclosed sponsorship of content. The goal of this activity is to exert influence over the information landscape without making it apparent that specific entities are orchestrating or guiding the messaging.

[75] Vladimir Putin, "Article by Vladimir Putin 'On the Historical Unity of Russians and Ukrainians,' " President of Russia, July 12, 2021, http://en.kremlin.ru/events/president/news/66181.

[76] "Transcript: Vladimir Putin's Televised Address on Ukraine," *Bloomberg*, February 24, 2022, https://www.bloomberg.com/news/articles/2022-02-24/full-transcript-vladimir-putin-s-televised-address-to-russia-on-ukraine-feb-24.

[77] Putin, "On the Historical Unity of Russians and Ukrainians."

[78] Will Oremus, "In Putin's Russia, 'Fake News' Now Means Real News," *Washington Post*, March 11, 2022, https://www.washingtonpost.com/technology/2022/03/11/russia-fake-news-law-misinformation/; Shackelford, Douzet, and Ankersen, *Cyber Peace*.

[79] Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

Such covert approaches are closely associated with practices such as the dissemination of propaganda, disinformation campaigns, and other repressive tactics that seek to control narratives without openly acknowledging involvement in them.[80] Within the realm of covert information channeling, the term *dezinformatsiya* (disinformation) encompasses a spectrum of activities, including the use of bots, trolls, fake news, and more.[81] This multifaceted approach is exemplified by instances such as the sprawling and sophisticated Doppelgänger operation. Operating from within the Russian private sector, Doppelgänger mimicked various international media outlets to disseminate false narratives, particularly regarding European sanctions and Ukrainian refugees.[82] Another notable example is Cyber Front Z, a Russian network employing Telegram to task commentators with spreading anti-criticism posts and promoting anti-Ukraine propaganda. However, despite the Russian state's significant investment in covert information channeling, research shows that platforms with less moderation, such as Telegram, do not necessarily encourage users to share more fake news.[83]

Disinformation campaigns orchestrated by the Kremlin have become a prominent tool for swaying public opinion, both within Russia and on the international stage. Utilizing bots and trolls to disseminate propaganda through social media platforms is a prevalent practice. The case of Russia's interference in the 2016 US elections serves as a stark example of the strategic use of disinformation campaigns to influence political outcomes and sow discord.[84] These orchestrated efforts reveal the intricate and evolving landscape of Moscow's covert information channeling, which not only serves Moscow's various political goals but is exported abroad. Russia exports digital repression technologies to other countries by providing sophisticated tools and expertise that enable governments to monitor and control digital communication within their borders.[85] This includes the sale of surveillance software, censorship mechanisms, and expertise in online content control. The export of covert information channeling technologies can contribute to the establishment of authoritarian digital regimes, allowing recipient countries to exert control over internet activities, stifle dissent, and suppress freedom of expression. Russia's role in exporting these technologies reflects a broader trend, in which illiberal governments

[80] Earl, Maher, and Pan; Shackelford, Douzet, and Ankersen, *Cyber Peace*.

[81] Max Holland, "The Propagation and Power of Communist Security Services *Dezinformatsiya*," *International Journal of Intelligence and CounterIntelligence* 19, no. 1 (January 2006): 1–31, https://doi.org/10.1080/08850600500332342; John Curry and Lewis Blanks, "Dezinformatsiya and the Art of Information Warfare," *ITNOW* 60, no. 3 (2018): 34–35, https://academic.oup.com/itnow/article-abstract/60/3/34/5088160; Christopher Dornan, "*Dezinformatsiya*: The Past, Present and Future of Fake News," Series of Reflection Papers, Canadian Commission for UNESCO, 2017, https://www.researchgate.net/profile/Christopher-Dornan/publication/335881115_Dezinformatsiya_The_past_present_and_future_of_'fake_news'_A_Reflection_Paper_for_the_Canadian_Commission_for_UNESCO/links/5d81a738a6fdcc12cb989feb/Dezinformatsiya-The-past-present-and-future-of-fake-news-A-Reflection-Paper-for-the-Canadian-Commission-for-UNESCO.pdf.

[82] Funk, Shahbaz, and Vesteinsson, "The Repressive Power of Artificial Intelligence."

[83] Aliaksandr Herasimenka et al., "Misinformation and Professional News on Largely Unmoderated Platforms: The Case of Telegram," *Journal of Information Technology & Politics* 20, no. 2 (April 2023): 198–212, https://doi.org/10.1080/19331681.2022.2076272.

[84] Jean-Baptiste Jeangène Vilmer and Heather A. Conley, "Successfully Countering Russian Electoral Interference," Washington, DC: Center for Strategic & International Studies, 2018, https://www.jstor.org/stable/pdf/resrep22297.pdf; Marek Posard, Hilary Reininger, and Todd C. Helmus, "Countering Foreign Interference in US Elections" (Santa Monica, Calif.: RAND Corporation, 2021), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA700/RRA704-4/RAND_RRA704-4.pdf; Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95, no. 7 (June 2017), 1579-1598, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr95&section=58&casa_token=EoTNNLwAUTsAAAAA:IV9xuUfUb6sMCOWjsOPu0WDt6jTiG5NbByHHi67juZxyC3grZVYUgDiC-X2ZN5D3MCw24TWldg.

[85] Polyakova and Meserole, "Exporting Digital Authoritarianism."

seek to enhance their capabilities in digital repression through international partnerships and transfers of technological know-how.

Discussion

The previous section has examined the landscape of Russia's digital repression, outlining how the regime uses traditional repression while scaling up with digital technologies to limit opposition and anti-government sentiment and restrict dissent. In this section, we identify patterns, trends, and directions of illiberal digital strategies' development, enabling a deeper understanding of political phenomena. We argue that the country's history, political realities, and the regime's economic constraints all offer key reasons for Russia's current digital repression choices.

Through mapping out Moscow's uses of digital repression for illiberal purposes, our research identifies two primary directions in the Kremlin's approach: first, Moscow's increased usage of physical coercion and information channeling; and second, Moscow's weaponization of history and collective memory. As discussed in the previous section, the evidence indicates that Moscow has been scaling up its pre-existing traditional repression of political activists and opposition figures to create a more extensive system of digital repression. Such an approach incorporates the traditional repressive methods while employing technologies to deeply embed illiberal tactics into the fabric of society. This integration signifies a convergence between traditional forms of repression and the challenges presented by the digital landscape. While the prevailing Western commentary characterizes Putin's regime as fixated either on past Soviet achievements and global dominance aspirations, or on furthering personalistic aims,[86] our analysis indicates that the regime is actively addressing contemporary political challenges arising from dissent in the online space while simultaneously perpetuating the historical system of oppression. Moscow's approach suggests that Russia's digital repression landscape is multifaceted and nuanced.

While the lack of the international recognition that Russia desires from the West continues to influence Russian politics, the invasion of Ukraine has compelled the Russian state to tighten its regional focus, as Moscow struggles to uphold the same level of security engagement with its near abroad or Russia's expansion in other regions, such as Africa and Latin America. Consequently, there is an increased emphasis on addressing domestic dissent and developing strategies to mitigate its impact, especially as the war in Ukraine continues to drain Russia's resources and war weariness sets in.[87] These findings contribute to a nuanced understanding of the complex interplay between geopolitical considerations and domestic political dynamics within the context of Russia's contemporary political landscape. Russia's invasion of Ukraine has changed Moscow's domestic and foreign policy priorities, thereby escalating the development of Russia's digital repression system. This can be seen as part of Moscow's attempts to exert tighter control over the public square, so that the Kremlin will not be challenged on its justifications for the invasion of Ukraine.

[86] Timothy Frye, *Weak Strongman: The Limits of Power in Putin's Russia* (Princeton, NJ: Princeton University Press, 2022); Kathryn E. Stoner, *Russia Resurrected: Its Power and Purpose in a New Global Order* (Oxford: Oxford University Press, 2020).

[87] Daniel Treisman, "Putin Unbound: How Repression at Home Presaged Belligerence abroad," *Foreign Affairs* 101, no. 3 (May/June 2022): 40, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/fora101&section=66; Ivan Gomza, "The War in Ukraine: Putin's Inevitable Invasion," *Journal of Democracy* 33, no. 3 (2022): 23–30, https://doi.org/10.1353/jod.2022.0036; Rajan Menon, "Ending the War in Ukraine: Three Possible Futures," CounterPunch (online magazine), 2022, https://www.counterpunch.org/2022/06/28/247611/.

The increased use of physical coercion methods can be attributed to two interconnected factors. Firstly, the regime has established a highly efficient apparatus of traditional repression that has been rigorously tested and utilized for various political objectives, notably in the context of managing dissent within the framework of counterterrorism measures.[88] The enduring efficacy of these established mechanisms renders them indispensable, as they have demonstrated consistent success over the years. Rather than discarding these proven methods, it appears rational for the regime to incorporate such repression mechanisms, in part, as a strategic response to the challenges posed by online activism.[89] This emphasizes the state's resilience and adaptive capacity to navigate a shifting sociopolitical landscape.

Key works in the academic literature on authoritarian resilience suggest that autocratization is a process that requires strategic hedging analysis to understand why some authoritarian regimes endure and some are short-lived.[90] The questions of the regime's adaptability and potential avenue of such adaptability's disruption become more than just theoretical as authoritarian Russia has risen to invade a neighboring country, thus changing the security landscape of Europe. Whether the objective is the democratization of Russia or the regulation of technology exports, recognizing the state's demonstrated ability to adapt to emerging realities is imperative. Anna Lührmann argues that one of the approaches to the democratization of autocratic regimes can be the disengagement of the regime's semi-loyal groups which are still possible to persuade towards democratic reforms—unlike the regime's hardline supporters, whose livelihoods depend on the regime's survival.[91] A better understanding of Russia's digital repression landscape, as well as Moscow's post-invasion approach to the expansion of digital repression, is paramount for locating possible semi-loyal political groups and gauging the possibility of support for anti-Putin initiatives. Acknowledging this resilience is integral to the development of nuanced and effective strategies that account for the multifaceted dynamics of state repression in the digital age.

Another piece of the puzzle of Russia's digital repression landscape is the close connection between the current level of repression and the collective memory of physical coercion by the Soviet Union. This connection is a useful tool for explaining the success of the regime in deterring Russian citizens from expressing more anti-government and anti-war sentiments through the covert physical coercion approach. Emerging collective-memory research emphasizes that shared intergenerational trauma can become a building block of a repressive system, since illiberal regimes frequently circle back to the memory of the traumatic event and manipulate the public's perception with the threat of reliving said experience.[92] Illiberal states may utilize propaganda campaigns to disseminate false or exaggerated information about

[88] Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

[89] Pop-Eleches and Way, "Censorship and the Impact of Repression on Dissent"; Sinkkonen, "Dynamic Dictators"; Anna Lührmann, "Disrupting the Autocratization Sequence: Towards Democratic Resilience," *Democratization* 28, no. 5 (July 2021): 1017–1039, https://doi.org/10.1080/13510347.2021.1928080.

[90] Sinkkonen, "Dynamic Dictators"; Milan W. Svolik, *The Politics of Authoritarian Rule* (Cambridge, UK: Cambridge University Press, 2012); Lührmann, Disrupting the Autocratization Sequence."

[91] Lührmann.

[92] Daria Khlevnyuk, "Narrowcasting Collective Memory Online: 'Liking' Stalin in Russian Social Media," *Media, Culture & Society* 41, no. 3 (April 2019): 317–331, https://doi.org/10.1177/0163443718799401; Noa Gedi and Yigal Elam, "Collective Memory—What Is It?" *History and Memory* 8, no. 1 (Spring/Summer 1996): 30–50, https://www.jstor.org/stable/25618696; Jan Assmann and John Czaplicka, "Collective Memory and Cultural Identity," *New German Critique*, no. 65 (Spring/Summer 1995): 125–133, https://www.jstor.org/stable/488538; Maurice Halbwachs, *On Collective Memory* (Chicago: University of Chicago Press, 2020), https://books.google.ca/books?id=ejfnDwAAQBAJ.

their digital repression efforts, as well as attempt to shield the general public from unwanted media influences through various digital manipulation techniques.[93]

A key aspect of using collective memory justification for digital repression purposes is the negative implication of manipulating collective memory to serve illiberal purposes, thus distorting history and making it a statecraft tool.[94] Moscow's digital repression system has been building on the collective memory of the 1937 repressions, evoking the fear of speaking up and uncertainty about the future. The events of 1937, often associated with Stalin's Great Purge, were a period of intense political repression marked by mass arrests, show trials, and widespread executions. This period caused the shared trauma inflicted on Soviet society, withy7 millions of individuals, including intellectuals, Communist Party officials, and ordinary citizens being accused of political crimes and subsequently purged.[95] The collective memory of the 1937 repressions in the Soviet Union is characterized by a complex interplay of historical interpretation, official narratives, and the impact on societal consciousness.

The uneasy relationship between digital repression in the last decade and the collective memory of the events of 1937 can partially explain the initial surprise expressed by Western journalists and politicians in what they perceived as the lack of public protests in Russia against the invasion of Ukraine in 2022. While the West was shocked and outraged by Putin's decision to invade a neighboring country, Russian citizens had to learn to live in the new reality of a physical coercion and repression environment. This oppressive environment has not only deterred them from wider public protests, but also triggered their collective memory trauma. This complex interplay between the current digital repressions and the collective memory of 1937 has allowed the regime to restrict the space for political activism even further, raising the cost of political activism significantly, as the collective memory has multiplied the feelings of fear and uncertainty.

Another pattern that is evident in our analysis is that, despite the success of the application of physical coercion and repression tools, the Russian state has been developing digital repression tools such as information control techniques, and it has heavily invested in information channeling. The use of history for political purposes and the export of digital repression technologies and playbooks (that is, digital surveillance technologies, election meddling, troll factories, etc.) to the near abroad are the few of Russia's rather recent advances in information control.[96] Moscow's

[93] Anita R. Gohdes, "Repression in the Digital Age: Communication Technology and the Politics of State Violence," (Oxford: Oxford University Press, 2014); Gohdes, "Reflections on Digital Technologies, Repression, and Resistance: Epilogue," *State Crime Journal* vol. 7 no. 1 (Spring 2018), 141; Feldstein, *The Rise of Digital Repression*; Bushwick, "Russia Is Using 'Digital Repression' to Suppress Dissent: An Interview with Jennifer Earl."

[94] James C. Pearce, *The Use of History in Putin's Russia* (Wilmington, Del.: Vernon Press, 2020).

[95] Kathleen E. Smith, *Remembering Stalin's Victims: Popular Memory and the End of the USSR* (Ithaca, NY: Cornell University Press, 1996); Khlevnyuk, "Narrowcasting Collective Memory Online"; Antony Kalashnikov, "Stalinist Crimes and the Ethics of Memory," *Kritika: Explorations in Russian and Eurasian History* 19, no. 3 (Summer 2018): 599–626, https://muse.jhu.edu/pub/28/article/701568/summary; Theodore P. Gerber and Michael E. Van Landingham, "Ties That Remind: Known Family Connections to Past Events as Salience Cues and Collective Memory of Stalin's Repressions of the 1930s in Contemporary Russia," *American Sociological Review* 86, no. 4 (August 2021): 639–669, https://doi.org/10.1177/00031224211023798; Orlando Figes, "Private Life in Stalin's Russia: Family Narratives, Memory and Oral History," *History Workshop Journal*, vol. 65 (Oxford: Oxford University Press, 2008), 117–137, https://academic.oup.com/hwj/article-abstract/65/1/117/640511.

[96] Anastassiya Mahon, James C. Pearce, Andrei Korobkov, Rashid Gabdulhakov, Nino Gozalishvili, Revaz Topuria, Natalia Stercul, and Marius Vacarelu, "Russia's Invasion of Ukraine: What Did We Miss?" *International Studies Perspectives* (May 2023), https://doi.org/10.1093/isp/ekad006; Pearce, *The Use of History in Putin's Russia*; Polyakova and Meserole, "Exporting Digital Authoritarianism."

desire to control information flows has intensified since the beginning of the Ukraine War, but the heavy focus on this digital repression tool category is consistent with Russia's long tradition of disinformation going back to the early Soviet years. During the Bolshevik era, Vladimir Lenin and Joseph Stalin employed propaganda as a powerful tool to shape public perception and control information.[97] The state-controlled media became a vehicle for disseminating carefully crafted narratives that served the ideological goals of the Communist Party. Modern Russia takes a similar approach to the media, ensuring control over information flows.[98] While not all media resources in Russia are directly controlled by the state, the current climate of the state's freedoms repression, surveillance, and heavy consequences for political dissent create an environment of mistrust and self-censorship that still has echoes of the Soviet era. The Russian state's use of repressive technologies builds on the collective memory of the Soviet state's repression and propaganda, multiplying the effect of modern repression technologies used to control information.

The collective memory of the Cold War and the rivalry between Russia and the West can also be seen in Moscow's instrumentalization of history, especially regarding disinformation campaigns. As a tool used in its competition with the West, the Soviet Union employed disinformation to advance its geopolitical interests and ideological agenda. Active measures, such as spreading false information through state-controlled media outlets and covert influence operations, became integral elements of Soviet foreign policy, preceding the modern techniques of information control.[99] This era witnessed the amplification of conspiracy theories, the creation of false narratives about the West, and the promotion of disinformation to undermine confidence in democratic institutions.[100] The legacy of this longstanding tradition continues to manifest in contemporary Russia, where disinformation remains a prominent feature of statecraft and a tool for shaping narratives both domestically and on the global stage.

The collective memory legacy is reflected in the ways the Kremlin has been using its information control techniques, especially the tools for information channeling, as many of the underlaying messages from the state resemble those of the Cold War (for example, the "othering" of the West, the enhanced juxtaposition of Russian values vs. Western capitalism and liberalism, and the recurring argument of Russia being "encroached upon" by the evil forces). The combination of the geopolitical choices of leading political actors since the mid-2010s, combined with the collective memory of living in the constant disinformation and propaganda environment in the Soviet Union, influence the Russian public's understanding and perception of Moscow's usage of digital repression technologies. This perception through the collective memory lens accounts for much of the misunderstanding of what is perceived as the political inertia of the Russian people by publics in Western democracies.

[97] Ralph Carter Elwood, "Lenin and Pravda, 1912–1914," *Slavic Review* 31, no. 2 (June 1972): 355–380, https://doi.org/10.2307/2494339; Vladimir Shlapentokh, "Perceptions of Foreign Threats to the Regime: From Lenin to Putin," *Communist and Post-Communist Studies* 42, no. 3 (September 2009): 305–324, https://doi.org/10.1016/j.postcomstud.2009.07.003; Gerber and Van Landingham, "Ties That Remind."

[98] Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: Perseus Books, 2017).

[99] McLaughlin, *Russia and the Media*; Adrian Hänni, Thomas Riegler, and Przemyslaw Gasztold, *Terrorism in the Cold War: State Support in Eastern Europe and the Soviet Sphere of Influence* (London: Bloomsbury Publishing, 2022).

[100] George Soroka and Félix Krawatzek, "When the Past Is Not Another Country: The Battlefields of History in Russia," *Problems of Post-Communism* 68, no. 5 (September 2021): 353–367, https://doi.org/10.1080/10758216.2021.1966989; David L. Hoffmann, *The Memory of the Second World War in Soviet and Post-Soviet Russia* (Abingdon: Routledge, 2022), https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.4324/9781003144915&type=googlepdf.

However, after noting the regime's reliance on physical coercion and information channeling, one question remains: why does the regime generally prefer physical channeling over information coercion? While Moscow does not extensively employ physical channeling, the state is gradually coming to rely more on overt physical channeling tactics. Notably, there are online platforms in Russia addressing grievances—provided not by the state, but by dissent-supportive nongovernmental organizations (NGOs), such as OVDinfo. These NGOs, along with independent media outlets, offer guides, manuals, and online consultations to address legal and administrative challenges related to online activism and dissent (such as Holod).[101]

It is noteworthy that the Kremlin may not fully understand that, although the Russian public tolerates but does not actively engage in the state's overt physical control strategies, NGOs are very active in providing support for political dissent. These NGOs primarily support anti-regime activities, helping people evade surveillance, secure their devices, and participate in protests. The parts of the Russian society that such NGOs' engagement can reach might be seen as the regime's semi-loyal audiences, and therefore, as potential target audiences for Russia's democratization.[102] This is particularly important for any Western attempts to reach Russian audiences while official Western media channels have been expelled from Russia. There is potential for reaching the audiences of the NGOs who support the remaining dissent in Russia as a way to circumvent the Kremlin's clampdown on Russia's civil society and political opposition.

The apparent limited interest of the Kremlin in physical channeling may be explained by the substantial advancements in Russia's information channeling tools, representing a more sophisticated approach to suppressing dissent than physical channeling. Information channeling proves to be cost-effective, cultivating persistent doubt among the Russian populace and fostering fear and distrust in both the government and fellow citizens.[103] This strategic use of information channeling harkens back to the collective memory of Soviet repressions, creating a pervasive atmosphere of uncertainty and apprehension.

The government's involvement in information coercion is evident through diverse means, including content regulation, internet shutdowns aligned with governmental needs, and the establishment of content-filtering systems. Russia has actively employed both overt and covert information coercion strategies to restrict potential dissent. Nevertheless, when juxtaposed with physical coercion and information channeling, information coercion tools have not attained a high level of political embeddedness. This suggests that the regime's capacity to invest in the category of digital repression tools specifically related to information coercion is not as pronounced as its investment in information channeling techniques. In contrast to information channeling, the deployment of information coercion demands a significant degree of technological development across the country, a milestone Russia has yet to achieve.[104] When considering the associated costs of developing information coercion tools, it is plausible to posit that the financial prioritization of

[101] Holod is an independent media outlet founded by Taisia Bekbulatova, a renowned Russian journalist, in the summer of 2019. For more information, see https://holod.media/en/about-us/.

[102] Lührmann, "Disrupting the Autocratization Sequence."

[103] Pop-Eleches and Way, "Censorship and the Impact of Repression on Dissent."

[104] Anna Gladkova and Massimo Ragnedda, "Exploring Digital Inequalities in Russia: An Interregional Comparative Analysis," *Online Information Review* 44, no. 4 (June 2020): 767–786, https://doi.org/10.1108/OIR-04-2019-0121.

the war in Ukraine takes precedence over investments in information coercion.[105] This prioritization is influenced by the perception that information channeling yields more successful and enduring results in altering people's behavior compared to information coercion.

Conclusion

This paper has analyzed Russia's employment of digital repression, reflecting on the complex interplay of political realities and Moscow's illiberal path of stifling dissent and gaining more control over the public. By examining the landscape of digital repression, we have identified key patterns, trends, and directions in the Kremlin's illiberal strategies, offering insights into the multifaceted dynamics that shape political phenomena in the country. Two primary trends have emerged from our analysis, each offering distinct insights into the Kremlin's approach to digital repression. Firstly, the convergence of traditional forms of repression with digital technologies reflects the regime's responsiveness to both external and internal challenges. Moscow's paying more attention to addressing domestic dissent, particularly following the onset of the Ukraine War, highlights the evolving priorities of the Russian government.

The historical trajectory of Russia's information control, dating back to pre-revolutionary tsarist times and persisting through the Soviet era, forms a crucial backdrop to understanding the continuity in the Kremlin's repressive tactics. Our analysis has demonstrated that the Putin regime, far from being fixated solely on past Soviet achievements, actively addresses contemporary political challenges, particularly those arising from dissent in the online space. The paper's findings challenge prevailing Western narratives, such as Putin-centrism and Russia's imperial ambitions, which may oversimplify the regime's approach, thus highlighting the regime's adaptive capacity to navigate shifting sociopolitical landscapes.

However, we have also shown that the regime actively uses history and builds on the collective memory of traumatic events during the Soviet period to manipulate information flows and intensify the system of digital repression. Rooted in historical practices, traditional repression mechanisms remain indispensable tools for the regime. Moreover, the strategic integration of covert physical coercion, grounded in the collective memory of Soviet-era repressions, has proven effective in deterring anti-government sentiment. This approach cultivates doubt, fear, and distrust among the public, effectively suppressing dissent in a cost-effective manner. The legacy of Soviet-era disinformation campaigns persists in the Kremlin's current narrative-shaping efforts, reflecting an amalgamation the collective-memory agenda and the regime's increasing reliance on digital repression technologies.

In considering why certain digital repression tools are prioritized over others, our analysis points to a variety of factors. The regime's reliance on physical coercion methods is attributed to the proven efficacy of established mechanisms and the enduring impact of historical collective memory. In contrast, the regime's limited interest in physical channeling may stem from the sophistication of information-channeling tools, which are deemed more cost-effective and politically embedded. Additionally, financial prioritization according to the Kremlin's cost-benefit analysis

[105] Marina G. Petrova, "Is It All the Same? Repression of the Media and Civil Society Organizations as Determinants of Anti-Government Opposition," *International Interactions* 48, no. 5 (September 2022): 968–996, https://doi.org/10.1080/03050629.2022.2068541; Eleonora La Spada, "Costly Concessions, Internally Divided Movements, and Strategic Repression: A Movement-Level Analysis," *International Studies Quarterly* 66, no. 4 (December 2022), https://academic.oup.com/isq/article-abstract/66/4/sqac052/6695167.

and influenced by its ongoing invasion of Ukraine, shapes the regime's investment in information coercion tools. These advances in digital repression tools that Russia has achieved should be analyzed in relation to the role that Russia plays both globally and regionally, taking into account the potential for the creation of a digital repression technology-sharing space between Russia and the near abroad.