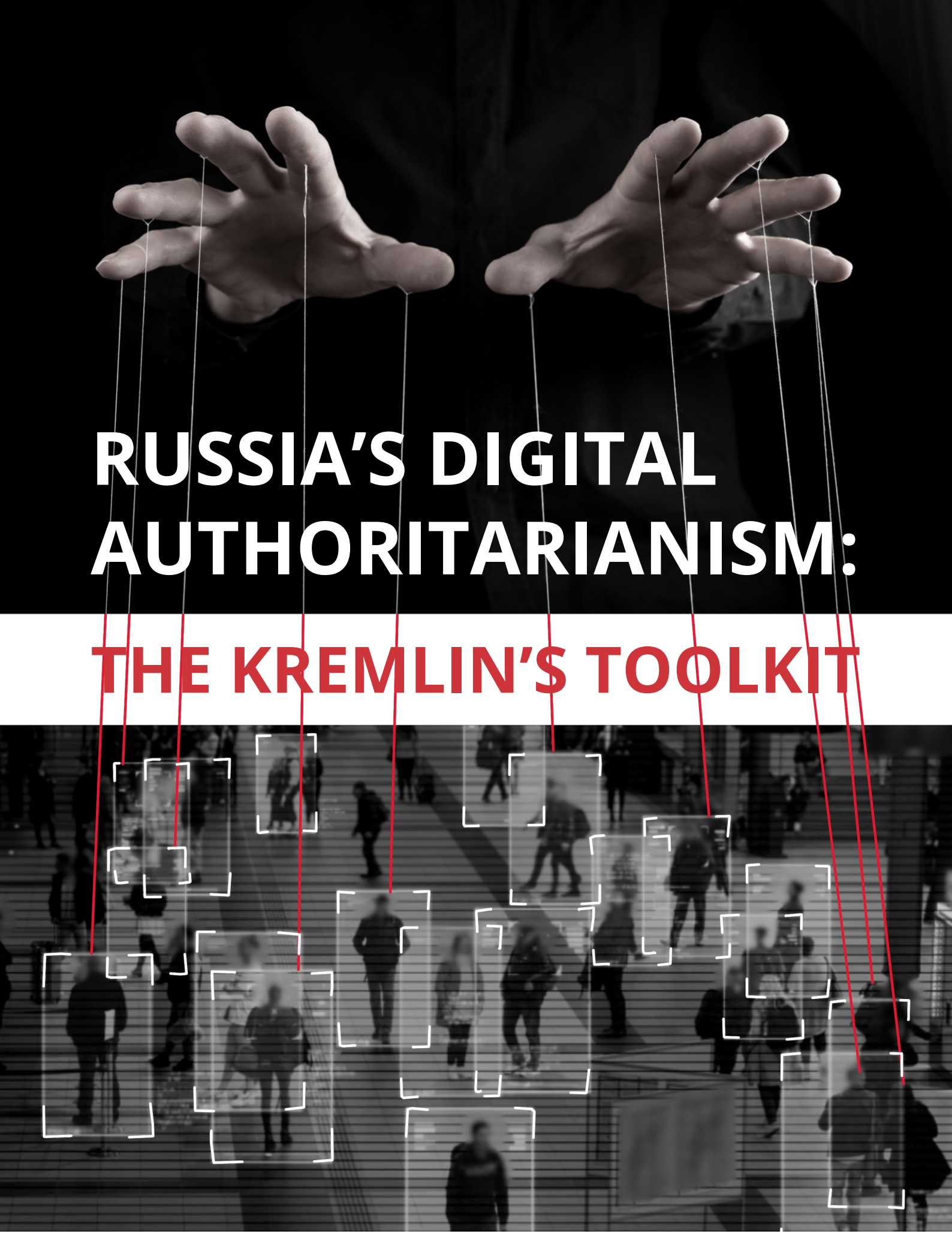

RUSSIA'S DIGITAL AUTHORITARIANISM:

THE KREMLIN'S TOOLKIT

IPHR International Partnership for Human Rights

global diligence

International Partnership for Human Rights (IPHR) is an independent, non-governmental organisation founded in 2008. Based in Brussels, with a second office in Tbilisi, IPHR works closely with civil society groups from a range of countries to raise human rights concerns at the international level and promote respect for the rights of vulnerable communities. IPHR acts to empower local civil society groups working to advance the protection of human rights in their respective countries and helps them raise human rights concerns at the international level. In cooperation with partner organisations, IPHR advocates on behalf of individuals and communities who are among those most vulnerable to discrimination, injustice, and human rights violations.

W https://IPHRonline.org/

E IPHR@IPHRonline.org

Global Diligence LLP is a partnership of established international lawyers with practical experience of living and working in high-risk areas. Global Diligence team advises and represents States, businesses, organisations, or individuals on international criminal law and human rights. Focused on challenges in unstable and conflict-affected regions, Global Diligence provides mapping, training, and project management for capacity building programs.

W https://www.globaldiligence.com/

E info@globaldiligence.com

Table of contents

Introduction

1. Digital authoritarianism is the use of digital technology by authoritarian regimes to track, repress, and manipulate domestic and foreign populations.[1] A hallmark of Vladimir Putin's regime is the use of mass surveillance technology to suppress democracy and violate human rights and freedoms.[2] The Kremlin has created a repressive law enforcement and criminal justice system that intimidates Russia's population, civil society, and businesses into silence and submission. Those who refuse to conform are severely punished.[3] Digital technologies play a major role in this repressive system – by censoring the internet and helping the authorities to identify and target critics and protesters online and on the streets.

2. Starting in the early 2000s, the Russian state began to implement a series of laws and policies that de facto criminalised criticism of the government, legalized unfettered surveillance of individuals' online activities, and increased state control over Ru.net, the Russian internet service.[4] The use of mass surveillance technologies is one of the key components of this process, along with the restriction of access to digital information. In Russia, digital authoritarianism takes many forms: the SORM system allows extensive communications monitoring, the sovereign internet (Ru.net) allows the government control and censorship over certain sectors of the internet, and facial recognition video surveillance systems enable the authorities to track and detain critics and opponents of the regime.

3. The background section of this report traces Russia's gradual descent into authoritarianism from the pro-democracy protests in 2011 through the full-scale invasion of Ukraine in February 2022. The background section describes the repressive laws the Kremlin has enacted during this period, and examples of how it has used these laws to attack and silence its opponents and critics.

4. The second part of the report discusses key digital technologies that have enabled the widening repression, namely: facial recognition and the Smart City Programme, the System of Operative Investigative Measures (SORM) and the sovereign internet or Ru.net project. The report identifies the software and hardware tools used by the Kremlin to cement its control over information and identify its detractors – and the key manufacturers and suppliers of these tools. Not only are these tools used to suppress democracy in Russia, but they likely contribute to Russia's continuing aggression in Ukraine – by censoring information on the realities of Russia's war in Ukraine and stamping out any home-grown opposition. There is also evidence that some of these technologies have been used to identify and detain Russian men in order to send them to the frontlines in Ukraine.

5. Digital technology described in this report relies heavily on the import of components, such as semiconductors, from outside Russia. The report concludes with a series of recommendations addressed to the European Union and its Members States, other western governments and their allies and partners aimed at undermining the supply chains that support the manufacture and supply of these technologies to Russian authorities.

---

1 The Russia Guy, Exporting digital authoritarianism: The Russian and Chinese models, Soundcloud (August 2019) *https://www.brookings.edu/research/exporting-digital-authoritarianism/*.

2 Anton Troianovski, They Are Watching': Inside Russia's Vast Surveillance State, The New York Times (22 September 2022) *https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html*.

3 Mariya Omelicheva, Repression Trap: The Mechanism of Escalating State Violence in Russia, Center for Strategic and International Studies (30 July 2021) *https://www.csis.org/analysis/repression-trap-mechanism-escalating-state-violence-russia*.

4 Alina Polyakova and Chris Meserole, Exporting digital authoritarianism: The Russian and Chinese models, Foreign Policy at Brookings *https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf*.

LIST OF ABBREVIATIONS USED

CMCPCN – Centre for Monitoring and Controlling Public Communications Networks

DIT – Department of Information Technologies

DNS – Domain Name System

DPI – Deep Packet Inspection

ECHR – European Court of Human Rights

FSB – Federal Security Service

FZ – Federal Law

ICCPR – International Covenant for Civil and Political Rights

ISP – Internet Service Providers

IXP – Internet Exchange Point

MRFC – Main Radio Frequency Centre

NGO – Non-Governmental Organization

Roskomnadzor – The Federal Service for Supervision of Communications, Information Technology and Mass Media

SORM – System of Operative Investigative Measures

TSPU – Technical Equipment for Counteracting Threats to Stability, Security, and the Functional Integrity of The Internet on the Territory of The Russian Federation

VPN – Virtual Private Network

Background: Russia's descent into authoritarianism

a. 2011-2013: The protests that spooked Putin

6. Protests erupted in Russia in 2011 over the handling of local and parliamentary elections.[5] By December 2011, some 60,000 demonstrators were regularly gathering in the vicinity of the Kremlin in Moscow (and in other cities across Russia) to demand fairer elections and express frustration with the lack of democracy in the country.[6] The protests intensified after Putin announced that he would be running for a third presidential term (following a four-year stint as prime minister).[7] The presidential election was held on 4 March 2012, with the Electoral Commission declaring Putin as the winner with 64 percent of the votes.[8] Following the election, protesters demanded Putin's resignation and comprehensive reforms to Russia's political system.[9]

7. The scale and intensity of the protests was unlike anything Russia had seen since the early 1990s, and represented the biggest challenge to Putin's authority since he took power.[10] This was in part due to the dominant demographic of the protesters – young, educated, middle-class urbanites dissatisfied with the lack of political representation and the sluggish services economy.[11] In many ways, the protests were a product of social media. Unlike traditional media, which Putin had consolidated under his control within his first two terms as president,[12] social media was

---

5 See Ellen Barry, Rally Defying Putin's Party Draws Tens of Thousands, The New York Times (10 Dec. 2011) *https://www.nytimes.com/2011/12/11/world/europe/thousands-protest-in-moscow-russia-in-defiance-of-putin.html*; Russian election: Biggest protests since fall of USSR, BBC News (10 Dec. 2011) *https://www.bbc.co.uk/news/world-europe-16122524*.

6 See Anti-Putin protests erupt across Russia, Al-Jazeera (11 Dec. 2011), *https://www.aljazeera.com/news/2011/12/11/anti-putin-protests-erupt-across-russia*; Timothy Heritage, Maria Tsvertkova, No Russian revolution after a year of protests, Reuters (4 Dec. 2012) *https://www.reuters.com/article/us-russia-opposition-idUSBRE8B30O220121204*; Steven Rosenberg, Mass protests in Russia put Putin under pressure, BBC News (12 Dec. 2011) *https://www.bbc.co.uk/news/world-europe-16135999*.

7 See Ellen Barry, Putin Once More Moves to Assume Top Job in Russia, The New York Times (24 Sept. 2011) *https://www.nytimes.com/2011/09/25/world/europe/medvedev-says-putin-will-seek-russian-presidency-in-2012.html*; Anti-Putin protests erupt across Russia, Al-Jazeera (11 Dec. 2011), *https://www.aljazeera.com/news/2011/12/11/anti-putin-protests-erupt-across-russia*

8 TASS, Vladimir Putin gains four million votes less than in 2004, Russian News Agency (6 Mar. 2012) *https://tass.com/russianpress/671212*.

9 Phil Black, Russia protesters demand Putin's resignation, CNN (June 12, 2012) *https://edition.cnn.com/2012/06/12/world/europe/russia-protest/index.html*.

10 More than Moscow: Protests in Russia, 1991 and 2011-2012, Carnegie Endowment for International Peace (13 Feb. 2012) *https://carnegieendowment.org/2012/02/13/more-than-moscow-protests-in-russia-1991-and-2011-2012-event-3567*; Phil Black, Russia protesters demand Putin's resignation, CNN (12 June 2012) *https://edition.cnn.com/2012/06/12/world/europe/russia-protest/index.html*.

11 Dissecting Russia's winter of protest, five years on, Open Democracy (5 Dec. 2016) *https://www.opendemocracy.net/en/odr/dissecting-russia-s-winter-of-protest-five-years-on/*.

12 Foreign Policy, "Russia's Media is Now Totally in Putin's Hands", 5 April 2022, available at: *https://foreignpolicy.com/2022/04/05/russia-media-independence-putin/*.

still largely beyond the reach of Russia's censors and law enforcement structures.[13] However, following these events, control over the internet became a key priority for the Kremlin.[14]

Having assumed presidential power, Putin immediately ordered an end to the protests by any means necessary.[15] Riot police violently suppressed protests and carried out mass arrests of protesters.[16] Police raided the homes and offices of protest leaders and opposition politicians on 11 June 2012.[17] Prosecutors initiated trumped-up criminal cases against key protest leaders, most notably Alexey Navalny.[18] At this time, Putin's regime also began the process of toughening Russian anti-protest laws.[19] Law No. 65-FZ, restricted the ability to organise and participate in public protests.[20] Law No. 65-FZ significantly increased the fines for violating the rules for organising public events.[21] On 1 July 2012, the first law on restricting internet content (Law No. 139-FZ)[22] was enacted, creating a unified register of prohibited websites that Internet Service Providers ("ISPs") were required to block[23] - with a new special agency Roskomnadzor – administering the list.[24] On 20 July, Putin signed Law No. 121-FZ (The "Foreign Agents" Law) into force – which requires non-profit organisations that receive foreign funding and engage in so-called political activity to register as foreign agents.[25] The designation of an organisation as a "foreign agent" restricts

---

13 See Katarzyna Chawrylo, The Kremlin's crackdown on Western Social networks, Centre for Eastern Studies (15 Mar. 2022) *https://www.osw.waw.pl/en/publikacje/analyses/2022-03-15/kremlins-crackdown-western-social-networks*.

14 Russia: With War, Censorship Reaches New Heights, Human Rights Watch (28 Feb. 2022) *https://www.hrw.org/news/2022/02/28/russia-war-censorship-reaches-new-heights*; Alena Edifanova and Philipp Dietrich, Russia's Quest for Digital Sovereignty, DGAP (21 Feb. 2022) *https://dgap.org/en/research/publications/russias-quest-digital-sovereignty*.

15 Miriam Elder, Putin makes his presence felt as protesters take to Moscow's streets, The Guardian (5 Mar. 2012) *https://www.theguardian.com/world/2012/mar/05/putin-protesters-moscow*.

16 Reuters, Vladimir Putin using force to crush protests, Russian opposition fears, National Post (Mar. 6, 2012). *https://nationalpost.com/news/vladimir-putin-preparing-to-use-force-to-crush-protests-russian-opposition-fears*.

17 AP Moscow, Russians turn out in their thousands to protest against Vladimir Putin, The Guardian (12 Jun. 2012) *https://www.theguardian.com/world/2012/jun/12/russians-thousands-protest-vladimir-putin*.

18 Russia: Opposition leader Aleksei Navalny sentenced to 9 years in prison in cynical deprivation of his human rights, Amnesty International (22 Mar. 2022) *https://www.amnesty.org/en/latest/news/2022/03/russia-opposition-leader-aleksei-navalny-sentenced-to-9-years-in-prison-in-cynical-deprivation-of-his-human-rights/*.

19 Gleb Bryanski, Russia's Outin signs anti-protest law before rally, Reuters (8 Jun. 2012) *https://www.reuters.com/article/us-russia-protests-idUSBRE8570ZH20120608*.

20 Federal Law "On amendments on the Code of Administrative Offenses and the federal law 'On meetings, rallies, demonstrations, marches, and pickets," No. 65-F3, 2012, *http://www.rg.ru/2012/06/09/mitingi-dok.html*.

21 Ekaterina Vinokurova, Twenty thousand worth of walking [Нагулял на 20 тысяч], Gazeta (June 22, 2013) *http://www.gazeta.ru/politics/2012/06/22_a_4637941.shtml*; Two organizers of an unsanctioned protest in Kazan near hotel 'Bulgar' sentenced to fines [К штрафам приговорены два организатора несанкционированного митинга в Казани около отеля 'Булгар'], Tartar-inform (August 17, 2012) *http://www.tatar-inform.ru/news/2012/08/17/327757/*.

22 Crackdown on Russia's Civil Society after Putin's Return to the Presidency, Human Rights Watch (April 24, 2013) *https://www.hrw.org/report/2013/04/24/laws-attrition/crackdown-russias-civil-society-after-putins-return-presidency#_ftn198*.

23 Federal Law "On introducing changes to the federal law 'On protecting children from information harmful to their health and development' and certain legislative acts of the Russian Federation," No. 139-FZ, 2012, *http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=133282*.

24 Federal Law "On introducing changes to the federal law 'On protecting children from information harmful to their health and development' and certain legislative acts of the Russian Federation," No. 139-FZ, 2012, *http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=133282*, art. 3, para. 2.

25 The State Duma voted on the law on July 13, 2012, the Federation Council approved it on July 18, 2012, it was published on July 23, 2013, and it entered into force on November 21, 2012. Federal Law "On Making Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of Activities of Noncommercial

the organisation's ability to fundraise and allows the government to increase its monitoring of it (including online), and to apply pressure to those who openly support the group.[26] The "foreign agents" law was subsequently broadened to apply to individuals, in addition to organisations[27].

b. 2012-2021: The noose tightens

8. From 2012 onwards, the Kremlin unleashed a concerted and coordinated attack on pro-democracy and anti-corruption movements in Russia. The crackdown targeted independent media organisations, associations, activists, and opposition politicians.[28] It's key aims were to consolidate Putin's grip on power, eliminate accountability for systemic corruption, and stamp out all opposition.

9. The Kremlin's attack on democracy came to a crescendo around the 2021 parliamentary election. In the run-up to the election, polls projected poor results for the ruling United Russia party.[29] In a bid to silence its critics and retain its control over the legislature, the Kremlin intensified its crackdown on its remaining opponents.[30]

10. Relying on its powerful and flexible legal toolkit for gagging and disempowering groups and individuals, the Kremlin took down blogs and websites,[31] labelled media organisations as "foreign

---

Organisations Performing the Functions of Foreign Agents," No. 121-FZ, 2012, Rossiyskaya Gazeta, *http://www.rg.ru/2012/07/23/nko-dok.html*.

26 Crackdown on Russia's Civil Society after Putin's Return to the Presidency, Human Rights Watch (April 24, 2013) *https://www.hrw.org/report/2013/04/24/laws-attrition/crackdown-russias-civil-society-after-putins-return-presidency#_ftn198*.

27 Russia: "Foreign Agents" Bill Threatens Journalists, Human Rights Watch, (18 Nov. 2019) *https://www.hrw.org/news/2019/11/18/russia-foreign-agents-bill-threatens-journalists*

28 See Matthew Bodner, Life as a 'foreign agent': Inside Russia's crackdown on free speech, NBC News (17 Oct. 2021) *https://www.nbcnews.com/news/world/putins-russia-wages-crackdown-free-speech-political-dissent-rcna3137*; Laura Smith-Spark, Reports: Russia clamping down on free speech, CNN (24 Apr. 2013) *https://edition.cnn.com/2013/04/24/world/europe/russia-free-speech-report/index.html*.

29 WCIOM Polling, (16 July 2021) *https://wciom.ru/analytical-reviews/analiticheskii-obzor/default-402e3320c1*; Four Unknowns Ahead of Russia's 2021 Parliamentary Election, Carnagie Moscow Centre (10 June 2021) *https://carnegie.ru/commentary/84722*; In the Duma election campaign, Putin is in survival mode, Al Jazeera (6 July 2021) *https://www.aljazeera.com/opinions/2021/7/6/in-the-duma-election-campaign-putin-is-in-survival-mode*.

30 France 24, "'Not an election': Russians to vote after historic crackdown", 13 September 2021, available at: *https://www.france24.com/en/live-news/20210913-not-an-election-russians-to-vote-after-historic-crackdown*; AP, "Russia opposition stifled by unbowed as Doma election nears", 14 September 2021, available at: *https://apnews.com/article/europe-russia-elections-media-vladimir-putin-e9f4d4dde1293317ebbec028d358bd17*.

31 Consultant Plus, Federal Law of July 27, 2006 N 149-ФЗ (as amended on July 2, 2021) "On Information, Information Technologies and Information Protection", Article 15.3, *http://www.consultant.ru/document/cons_doc_LAW_61798/34547c9b6ddb60cebd0a67593943fd9ef64ebdd0/*; See also Russian Media Regulator Blocks Navalny's Website , RFE/RL (26 June 2021) *https://www.rferl.org/a/navalny-site-blocked-roskomnadzor/31377708.html*.

agents", [32] banned civil society organisations as "undesirable,"[33] and prosecuted key figures for violating restrictions,[34] or as leaders or members of "extremist organisations."[35] In March 2019 the Russian government criminalised all forms of "online disrespect" for "society, the country, Russia's official state symbols, the constitution, or the authorities", with this crime being punishable by a fine of 100,000 roubles ($1,500 USD) and/or a 15-day prison term.[36] In parallel, the Kremlin intensified its censorship of the internet.[37] On 4 June 2021, Putin signed into law a ban on the participation in elections by any members or affiliates of an entity designated as an "extremist organisation." – a designation arbitrarily applied to non-violent groups critical of the authorities. [38] In June 2021, Putin ratified a new law criminalising the participation in the activities of NGOs declared "undesirable" in Russia.[39] Under this law, individuals may face up to six years in prison if convicted of participating in the activities of an "undesirable" organisation. Activities which define an organisation as "undesirable" are deliberately vague to allow the authorities to target any civil society organisation they disagree with.

---

32 Consultant Plus, Federal Law "On Measures of Influence on Persons Involved in Violations of Fundamental Human Rights and Freedoms, Rights and Freedoms of Citizens of the Russian Federation" of 28 December 2012 N 272ФЗ (Last Edition), Article 2.1, *http://www.consultant.ru/document/cons_doc_LAW_139994/*; Pravo.Gov.ru, The Procedure for Applying the Provisions of the Federal Law of January 12, 1996 N 7-FZ "On Non-Commercial Organisations" to Foreign Mass Media Performing the Functions of a Foreign Agent, Articles 4, 9, *http://www.publication.pravo.gov.ru/Document/View/0001201804050030?index=2&rangeSize=1*; Consultant Plus, The Code of the Russian Federation on Administrative Offenses of 30 December 2001 N 195-ФЗ (as amended on 1 July 2021), Articles 19.7.5-2.; 19.7.5-4, *http://www.consultant.ru/document/cons_doc_LAW_34661/*; Consultant Plus, The Criminal Code of the Russian Federation, (as amended on 1 July 2021), Article 330.1, *http://www.consultant.ru/document/cons_doc_LAW_10699/*; See also Kremlin bears down on Moscow bureau of US-funded radio station, The Guardian (5 May 2021) *https://www.theguardian.com/world/2021/may/05/kremlin-bears-down-on-moscow-bureau-of-us-funded-radio-station-rfe-rl.*

33 Consultant Plus, Federal Law "On Measures of Influence on Persons Involved in Violations of Fundamental Human Rights and Freedoms, Rights and Freedoms of Citizens of the Russian Federation" of 28 December 2012 N 272ФЗ ((last edition), Article 3.1, *http://www.consultant.ru/document/cons_doc_LAW_139994/*; See also Andrew Osborn and Tom Balmforth, Russia bans investigative news outlet on national security grounds, Reuters (15 June 2021) *https://www.reuters.com/business/retail-consumer/russia-bans-investigative-news-outlet-proekt-national-security-grounds-2021-07-15/.*

34 Consultant Plus, The Criminal Code of the Russian Federation, (as amended on 1 July 2021), Article 284.1, *http://www.consultant.ru/document/cons_doc_LAW_10699/*; See also Six years for the "Project". Why the authorities designated the magazine of Roman Badanin as an undesirable organisation, Novaya Gazeta (19 July 2021) *https://novayagazeta.ru/articles/2021/07/16/shest-let-za-proekt*.

35 Consultant Plus, Federal Law of 25.07.2002 No. 114-ФЗ "On countering extremist activities" (Last Edition), Article 9, *http://www.consultant.ru/document/cons_doc_LAW_37867/*; Russia: Aleksei Navalny's NGOs banned as "extremist", depriving thousands of their rights, Amnesty International (10 June 2021) *https://www.amnesty.org/en/latest/news/2021/06/russia-aleksei-navalnys-ngos-banned-as-extremist-depriving-thousands-of-their-rights/*

36 Consultant Plus, Federal Law of 18 March 2019 no. 28-FZ, *https://www.consultant.ru/document/cons_doc_LAW_320403/#dst100011*; See also Russia passes law to jail people for 15 days for 'disrespecting' government, The Guardian (6 March 2019) *https://www.theguardian.com/world/2019/mar/06/russian-parliament-outlaws-online-disrespect*.

37 Russia Takes Censorship to New Extremes, Stifling War Coverage, The New York Times (4 March 2022) *https://www.nytimes.com/2022/03/04/world/europe/russia-censorship-media-crackdown.html*; Russia restricts access to DW's website, DW (4 March 2022) *https://www.dw.com/en/russia-restricts-access-to-dws-website/a-61011339*; Russia: Growing Internet Isolation, Control, Censorship, Human Rights Watch (18 June 2020) *https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship*.

38 Putin signs law banning people linked to 'extremist organisations' from running in Russian elections, Meduza (4 June 2021) *https://meduza.io/en/news/2021/06/04/putin-signs-law-banning-people-linked-to-extremist-organisations-from-running-in-russian-elections*.

39 Russian Lawmakers Approve Bill Criminalizing Links To 'Undesirable' Organisations, RFE/RL (16 June 2021) *https://www.rferl.org/a/russia-undesirable-organizations-penalties/31311067.html*.

11. Other key events during this period include:

- The poisoning and subsequent imprisonment of Alexei Navalny;[40]
- Mass arrests and prosecutions against Navalny supporters and colleagues;[41]
- Raids and arrests of other opposition politicians;[42]
- Raids, arrests, and dismantling of independent media organisations;[43]
- Raids, arrests, and elimination of human rights, pro-democracy, and other civil society organisations;[44]
- Banning of opposition politicians from standing for elected office;[45] and
- Persecuting lawyers who represent targeted activists and opposition politicians.[46]

12. The main implementers of this crackdown were the sycophantic leaders of law enforcement, state security ("FSB"), the Ministry of Justice, the Ministry of Internal Affairs, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), prosecutors, and judges.[47]

---

40 Alexey Navalny: Russia's vociferous Putin critic, BBC (21 Apr. 2021) *https://www.bbc.com/news/world-europe-16057045*.

41 Russia: Police Detain Thousands in Pro-Navalny Protests: Mass Arbitrary Detentions, Police Brutality, Criminal Prosecutions, Human Rights Watch (25 January 2021) *https://www.hrw.org/news/2021/01/25/russia-police-detain-thousands-pro-navalny-protests*; Russian court sentences Navalny ally Lyubov Sobol for trespass, BBC (15 April 2021) *https://www.bbc.com/news/world-europe-56760173*.

42 Vladimir Isachenkov, Police detain participants in Russian opposition forum, AP (13 Mar. 2021) *https://apnews.com/article/mikhail-khodorkovsky-moscow-arrests-europe-russia-21beb0c5c6dd3e382ec4355d2efd18b8*; Two Russian Opposition Lawmakers Detained Ahead Of Elections, RFE/RL (18 June 2021) *https://www.rferl.org/a/russian-lawmaker-detained/31314388.html*.

43 Russia Labels Meduza Media Outlet As 'Foreign Agent', RFE/RL, (23 April 2021) *https://www.rferl.org/a/russia-meduza-labeled-foreign-agent-press-freedom/31219272.html*; Russia: Police searches at student magazine are a new low for press freedom, Amnesty International (14 April 2021) *https://www.amnesty.org/en/latest/news/2021/04/russia-police-searches-at-student-magazine-are-a-new-low-for-press-freedom/*; Andrew Roth, Russian news site to close over 'foreign agent' designation, The Guardian (3 June 2021) *https://www.theguardian.com/world/2021/jun/03/russian-news-site-close-foreign-agent-vtimes*; Russia Bans Independent Investigative Outlet Proekt with 'Undesirable' Label, The Moscow Times (15 July 2021) *https://www.themoscowtimes.com/2021/07/15/russia-bans-independent-investigative-outlet-proekt-with-undesirable-label-a74533*; Russian news outlet to close after being blocked by state media watchdog, Reuters (5 August 2021) *https://www.reuters.com/world/asia-pacific/russian-news-outlet-open-media-says-blocked-by-state-media-watchdog-2021-08-04/*.

44 Open Russia opposition group shuts down under pressure, DW (27 May 2021) *https://www.dw.com/en/open-russia-opposition-group-shuts-down-under-pressure/a-57693178*; Marc Bennetts, Putin critic Andrei Pivovarov hauled off Polish plane, The Times (2 June 2021) *https://www.thetimes.co.uk/article/putin-critic-andrei-pivovarov-hauled-off-polish-plane-2zxt95mjq*; Moscow court declares Navalny's organisations extremist upholding prosecutors' request , TASS (10 June 2021) *https://tass.com/russia/1301019/amp*; Zahra Ullah, Russian court declares Navalny groups 'extremist' ahead of elections, CNN (10 June 2021) *https://edition.cnn.com/2021/06/09/world/russia-navalny-groups-extremists-intl/index.html*; The official list of "undesirable organisations" as of 23 July 2021 is available on the Ministry of Justice website and accessible here: *https://minjust.gov.ru/ru/documents/7756/*.

45 Russia opposition figure says election bid blocked over Navalny support, Reuters (25 June 2021) *https://www.reuters.com/world/russia-opposition-figure-says-election-bid-blocked-over-navalny-support-2021-06-25/*.

46 AP, Russia rights group linked to Navalny closes amid prosecution fears, The Guardian (19 July 2021) *https://www.theguardian.com/world/2021/jul/19/russia-team-29-closes-navalny-links-media*.

47 See Russia's Silence Factory: The Kremlin's Crackdown on Free Speech and Democracy in the Run-up to the 2021 Parliamentary Elections, IPHR (August 2021) *https://www.iphronline.org/wp-content/uploads/2021/08/Russias-Silence-Factory_report_Aug_2021.pdf*.

13. By all accounts the crackdown was effective – the United Russia party won more than half, or 238 out of 450 seats in parliament.[48] For the first time since 1993, the Organisation for Security and Cooperation in Europe did not send election observers due to "major limitations imposed by Russian authorities."[49]

c. 2022-2023: War and authoritarianism

14. In the early hours of 24 February 2022, Putin announced that he had ordered the Russian military to commence a "special operation" for the "demilitarization" and "denazification" of Ukraine.[50] Within hours, Ukraine was subjected to a full-scale invasion from the North (Belarus), East (Donbas), and South (Crimea). Throughout the course of the war, Russian forces have bombarded civilian homes, schools, hospitals, and critical infrastructure,[51] killed and tortured civilians and committed systematic pillage, leading to accusations of war crimes and mass atrocities by the international community.[52]

15. On 1 March 2022, the Prosecutor General ordered Roskomnadzor to block access to and effectively shut down the last remaining independent media organisation in Russia, Echo Moskvy.[53] On the same day, Roskomnadzor blocked access to Twitter, Facebook and Instagram[54] and on 20 March 2022, a Moscow Court labelled Meta (which owns Facebook and Instagram) as an "extremist" organisation.[55] BBC, CNN, and other global news outlets suspended reporting from Russia, saying it was impossible to comply with Russia's anti-speech laws (see more below) and maintain journalistic integrity in the situation that evolved following the launch of Russia's full-scale war against Ukraine.[56]

---

48 Russia Votes: Final Result of the Duma Election, 4 December 2011, Centre for the Study of Public Policy (9 Dec. 2011) *https://www.russiavotes.org//duma/duma_today.php*.

49 OSCE Will Not Send Election Observers to Russia Following 'Major Limitation,' RFE/RL (4 Aug 2021) *https://www.rferl.org/a/russia-elections-osce-observers/31393760.html*.

50 Путин объявил о начале военной операции на Украине (Putin announces launch of military operation in Ukraine), EuroNews (24 February 2022,) *https://www.youtube.com/watch?v=FhQbTFmk4Qo*.

51 Ukraine: civilian casualty update 23 March 2022, UN OHCHR *https://www.ohchr.org/en/news/2022/03/ukraine-civilian-casualty-update-23-march-2022*.

52 UN Commission has found an array of war crimes, violations of human rights and international humanitarian law have been committed in Ukraine, United Nations Human Rights Office of the High Commissioner (18 Oct. 2022) *https://www.ohchr.org/en/press-releases/2022/10/un-commission-has-found-array-war-crimes-violations-human-rights-and*; Russia's War Crimes: Beyond evil, even during war, Brand Ukraine NGO and MFA Ukraine *https://war.ukraine.ua/russia-war-crimes/*; Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova, International Criminal Court (17 March 2023) *https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and*.

53 Crackdown in Russia, U.S. Department of State (2 March 2022) *https://www.state.gov/media-crackdown-in-russia/*; Ekho Moskvy, One of Russia's Last Independent Broadcasters, Closes Amid Government Crackdown, RFE/RL (3 March 2022) *https://www.rferl.org/a/russia-ekho-moskvy-closed/31733880.html*.

54 Dan Milmo, Russia blocks access to Facebook and Twitter, The Guardian (4 March 2022) *https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter*; Russian Media Watchdog Blocks Facebook After Limiting Access to Multiple Other Sites, RFE/RL (4 March 2022) *https://www.rferl.org/a/russia-rferl-bbc-facebook-google-twitter-blocked/31735597.html*.

55 Russia bans Facebook and Instagram under 'extremist' law, The Guardian (21 March 2022) *https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law*.

56 BBC, CNN and other global news outlets suspend reporting in Russia, The Guardian (5 March 2022) *https://www.theguardian.com/media/2022/mar/04/bbc-temporarily-suspending-work-all-news-journalists-russia*.

16. On 4 March 2022, a new set of laws came into force that targeted the "discreditation of the Armed Forces of the Russian Federation" and publishing "false news" (i.e., reports that divert from the official narrative) about the war in Ukraine.[57] Specifically, as a result of these amendments:

    a. According to article 20.3.3 of the Code of Administrative Offences[58], '[p]ublic actions aimed at discrediting the use of the Armed Forces of the Russian Federation for the purpose of protecting the interests of the Russian Federation and its citizens, maintaining international peace and security, including public calls to prevent the use of the Armed Forces of the Russian Federation for these purposes' are now punishable by fines of 30,000 – 100,000 roubles (330 – 1,100 USD).

    b. Article 20.3 of the Code of Administrative Offenses[59], which punishes public display of extremist symbols with fines ranging from 1,000 to 2,000 roubles or up to 15 days of administrative detention, is being used to prosecute individuals for the slogan "Glory to Ukraine", the songs "Chervona Kalina" and "Bayraktar", which the courts in Crimea found to be the attributes of extremist organizations.

    c. According to article 20.3.4 of the Code of Administrative Offences,[60] it is an offence for a Russian citizen to call for the imposition of sanctions by a foreign state against the Russian Federation, Russian nationals, or Russian legal entities. This offence is punishable by fines of 30,000 – 500,000 roubles (330 – 5,515 USD). The new offences set out by articles 20.3.3 and 20.3.4 of the Code of the Administrative Offences are primarily aimed at protesters on the streets and online.

    d. Article 280.3 of the Criminal Code[61] prohibits "public actions aimed at discrediting the use of the Armed Forces … including public calls to prevent their use" and is applicable to any person convicted under Article 20.3(3) of the Code of Administrative Offences in the preceding 12 months. The offence is punishable by a fine of up to 300,000 roubles (3,300 USD), or up to three years of imprisonment or forced labour.

---

57 Consultant Plus, Federal Law of 4 March 2022 N 31-FZ (as amended on 16 April 2022) On Amendments to The Code of the Russian Federation on Administrative Offenses *https://www.consultant.ru/document/cons_doc_LAW_410886/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100036*; Consultant Plus, Federal Law of 4 March 2022 N 32-FZ "On Amendments to the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedure Code of the Russian Federation", *https://www.consultant.ru/document/cons_doc_LAW_410887/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100023*; See also Kremlin.ru, Установлена уголовная ответственность за публичное распространение под видом достоверных сообщений заведомо ложной информации, содержащей данные об использовании Вооружённых Сил России, (4 March 2022) *http://kremlin.ru/acts/news/67908*.

58 Consultant Plus, The Code of the Russian Federation on Administrative Offenses of 30 December 2001 No. 195-FZ (as amended on 27 April 2022), Article 20.3.3 *http://www.consultant.ru/document/cons_doc_LAW_34661/df67f6386f3aa5253a89bbfbe63fca1b2315988c/*.

59 Consultant Plus, The Code of the Russian Federation on Administrative Offenses of 30 December 2001 No. 195-FZ (as amended on 10 July 2023) *https://www.consultant.ru/document/cons_doc_LAW_34661/e3620d183bd6d1fe2ab8b0c912809857217325a2/*

60 Consultant Plus, The Code of the Russian Federation on Administrative Offenses of 30 December 2001 N 195-ФЗ (as amended on 27 April 2022), Article 20.3.4 *http://www.consultant.ru/document/cons_doc_LAW_34661/a4b1349770e40880151df67e188220a736115ff8/*.

61 Consultant Plus, The Criminal Code of the Russian Federation of 13 June 1996, (as amended on 25 March 2022), Article 280.3 *http://www.consultant.ru/document/cons_doc_LAW_10699/4618fd95c30a6fbe7717ceaebf64f082e735c9ad/*.

e. Article 280.3(2) of the Criminal Code[62] applies where the above-mentioned 'public actions' have led to mass disruptions of public order or disruptions of infrastructure – in these instances, the punishment is increased up to a million roubles (11,000 USD) or up to 5 years of imprisonment.

f. Article 284.2 of the Criminal Code[63] prohibits calls for the imposition of sanctions by a foreign state against the Russian Federation and is applicable to any person convicted under Article 20.3(4) of the Code of Administrative Offences in the preceding 12 months. The offence is punishable by a fine of up to 500,000 roubles (5,515 USD) or up to three years of imprisonment or forced labour.

g. Article 207.3 of the Criminal Code[64] prohibits the "public dissemination, under the guise of a truthful message, of knowingly false information including facts on the use of the Armed Forces of the Russian Federation for the purpose of protecting the interests of the Russian Federation and its citizens, maintaining international peace and security". This crime is punishable by a fine of up to 5,000,000 roubles (55,150 USD), or a prison term ranging from three to 15 years (depending on undefined "circumstances" and "consequences").

h. Several articles of the criminal code were adopted on 6 July 2022 criminalizing activities related to national security. A new article 275.1 of the Criminal Code (Cooperation on a confidential basis with a foreign state, international or foreign organization) introduced criminal liability for "confidential" cooperation with foreign states and organizations, as well as international organizations, with a penalty of two to eight years' imprisonment. At least two criminal cases have already been initiated. Article 280.4 of the Criminal Code introduced liability for public calls for actions against the security of the state. Article 283.2 of the Criminal Code criminalized the violation of requirements for the protection of state secrets.

i. On 29 December 2022 State Duma introduced several articles of the Criminal Code related to sabotage: 281.1 (Facilitating sabotage activities), 281.2 (Training for sabotage activities) and 281.3 (Organization of a sabotage community and participation in it). These articles now allow for punishment of individuals that propagandize, justify or endorse activities that are considered by the Russian government as sabotage.

17. As a consequence of these new measures and their enforcement since February 2022:

- 310 journalists, human rights defenders, lawyers and others have been declared "foreign agents;"[65]
- At least 504 journalists have fled Russia in fear of persecution;[66]
- All remaining independent Russian media outlets have shut down, moved to other countries or have been unable to cover the war in Ukraine; [67]

---

62 ConsultantPlus, The Criminal Code of the Russian Federation of 13 June 1996, (as amended on 25 March 2022), Article 280.3 *http://www.consultant.ru/document/cons_doc_LAW_10699/4618fd95c30a6fbe7717ceaebf64f082e735c9ad/*.

63 ConsultantPlus, The Criminal Code of the Russian Federation of 13 June 1996, (as amended on 25 March 2022), Article 284.2 *http://www.consultant.ru/document/cons_doc_LAW_10699/6a1e4076a95264b0f02fe733b710cc7e03e02b18/*.

64 ConsultantPlus, The Criminal Code of the Russian Federation of 13 June 1996, (as amended on 25 March 2022), Article 207.3 *http://www.consultant.ru/document/cons_doc_LAW_10699/65e0c88a157ad970eb20e97979647f03c0cd927d/*.

65 The official list of "foreign agents" is available on the Ministry of Justice website and accessible here: *https://minjust.gov.ru/ru/documents/7755/.This* link does not work (Error 404) I suggest we use this one *https://minjust.gov.ru/ru/activity/directions/998/*

66 Около 500 журналистов покинули Россию после репрессий и начала войны, Проект (15 August 2022) *https://t.me/proektproekt/761*.

67 Crackdown in Russia, U.S. Department of State (2 March 2022) *https://www.state.gov/media-crackdown-in-russia/*; Ekho Moskvy, One of Russia's Last Independent Broadcasters, Closes Amid Government Crackdown, Radio Free

- 45 organisations have been banned as "undesirable;"[68]
- 13 organisations have been labelled as "extremist;"[69]
- More than 19,700 persons have been arbitrarily arrested at anti-war rallies, more than 7,100 persons were charged with discrediting armed forces, 636 persons are under criminal investigation or have already been sentenced for their antiwar stance;[70]
- Russians have lost regular, unrestricted access to western-based social media;[71]
- Key opposition figures have been prosecuted, imprisoned or forced to flee Russia.[72]
- According to different estimates, between 400,000 to 800,000 Russians left the country after 24 February 2022.[73]

18. A serious impact of the measures described above is that most people living in Russia have lost access to independent sources of information about the conduct of Russian authorities in Russia, Ukraine and beyond. As such, the Kremlin's crackdown on critics and opponents has been effectively deployed to manufacture consent for the war in Ukraine – a prerequisite for the continual deployment and mobilization of military reserves and by extension the continuation of the war itself.

Europe (3 March 2022) *https://www.rferl.org/a/russia-ekho-moskvy-closed/31733880.html*; Russian news outlet Novaya Gazeta to close until end of Ukraine war, The Guardian (28 March 2022) *https://www.theguardian.com/world/2022/mar/28/russian-news-outlet-novaya-gazeta-to-close-until-end-of-ukraine-war*.

68 The official list of "undesirable organisations" is available on the Ministry of Justice website and accessible here: *https://minjust.gov.ru/ru/documents/7756/*.

69 The official list of "extremist organisations" is available on the Ministry of Justice website and accessible here: *https://minjust.gov.ru/ru/documents/7822/*.

70 Преследование за антивоенные взгляды, ОВД-Инфо, (28 July 2023), *https://antiwar.ovdinfo.org/*

71 Russia blocks access to Facebook and Twitter, The Guardian (4 March 2022) *https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter*; Russian Media Watchdog Blocks Facebook After Limiting Access to Multiple Other Sites", RFE/RL (4 March 2022) *https://www.rferl.org/a/russia-rferl-bbc-facebook-google-twitter-blocked/31735597.html*; 'I'm writing this post now and crying': Russians bid farewell to Instagram before midnight ban, The Washington post (13 March 2022) *https://www.washingtonpost.com/world/2022/03/13/russia-instagram-ukraine-war/*.

72 Prominent Russian opposition activist jailed in Moscow, The Guardian (12 April 2022) *https://www.theguardian.com/world/2022/apr/11/prominent-russian-opposition-activist-detained-in-moscow*; Alexei Navalny sentenced to 9 more years in prison after fraud conviction, The Guardian (22 March 2022) *https://www.theguardian.com/world/2022/mar/22/alexei-navalny-13-years-more-jail-fraud*; Washington Post contributor arrested in Moscow after criticizing Putin, The Washington Post (12 April 2022) *https://www.washingtonpost.com/media/2022/04/12/kara-murza-arrest/*; Valerie Hopkins and Misha Friedman, Leader of Pussy Riot Band Escapes Russia, With Help From Friends, The New York Times (10 May 2022) *https://www.nytimes.com/2022/05/10/world/europe/pussy-riot-russia-escape.html*; Russian Opposition Activist Flees Russia After Serving Jail Term Over Anti-War Rally, RFE/RL (29 March 2022) *https://www.rferl.org/a/activist-luzin-flees-russia-ukraine-war/31776594.html*.

73 The Bell came to a conclusion that at least 500,000 persons emigrated from Russia (*https://thebell.io/skolko-rossiyan-v-2022-godu-uekhalo-iz-strany-i-ne-vernulos*); Forbes Russia estimates this number to be more than 700,000 persons (*https://www.forbes.ru/society/478827-rossiu-posle-21-sentabra-pokinuli-okolo-700-000-grazdan*); Demographers Yulia Florinskaya and Alexei Raksha estimated emigration in 2022 at 400-800 thousand people (*https://novayagazeta.eu/articles/2023/02/03/rossiiane-pobili-piatiletnii-rekord-po-vyezdam-v-sredniuiu-aziiu-armeniiu-i-mongoliiu-news*).

The Kremlin's tech toolkit: technology supporting authoritarianism

19. As mentioned above, starting in the early 2000s, the Russian authorities began to implement a series of laws that de facto criminalised online criticism of the government, legalized unfettered surveillance of individuals' online activities, and increased state control over Ru.net, the Russian internet.[74] As examined in detail below, in the last two decades, the Kremlin has effectively put in place a system of digital authoritarianism whereby it has used digital technology to carry out surveillance, repression and manipulation of both domestic and foreign populations.[75] Russian digital authoritarianism is implemented through an integrated system of repressive technologies, including SORM, which allows extensive communications monitoring; a sovereign internet, which gives the government complete control over certain sectors of the internet; and facial recognition video surveillance systems (including the Safe Cities programme), which enable the authorities to track individuals' movements in urban areas.

a. Facial Recognition and Safe City Programmes

I. WHAT IS IT AND HOW DOES IT WORK?

20. Since 2018, Russian authorities have begun to integrate facial recognition capabilities into the country's extensive video surveillance system. These algorithms compare data obtained from surveillance cameras with a database of open-source images and data held by authorities (such as ID card photos and online government services). The result of the algorithm is an indication of image matches in percentage terms.[76]

21. In the last decade, Russia has consistently ranked first in the world both in terms of the number of street video surveillance cameras and the rate of increase in the number of such cameras.[77] Facial recognition technology was first tested during the 2018 World Cup.[78] Its use was further expanded during the COVID-19 pandemic, when the authorities used the technology to identify violators of quarantine restrictions in the Moscow Metro.[79]

---

74 Alina Polyakova and Chris Meserole, Exporting digital authoritarianism: The Russian and Chinese models, Foreign Policy of Brookings, *https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf*.

75 Alina Polyakova and Chris Meserole, Exporting digital authoritarianism: The Russian and Chinese models, Foreign Policy of Brookings, *https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf*.

76 Facial Recognition, PI *https://privacyinternational.org/learn/facial-recognition*.

77 В цифрах не значился: Могут ли высокие технологии помочь найти подлежащих мобилизации граждан (The figures did not include: Can high technology help find citizens to be mobilized), Kommweant (30 Sept. 2022) *https://www.kommersant.ru/doc/5583949?from=doc_vrez*.

78 Как власти используют камеры и распознавание лиц против протестующих (How authorities are using cameras and facial recognition against protesters), *https://www.vedomosti.ru/politics/news/2018/07/26/776624-sistema-raspoznavaniya-na-chm-2018*.

79 Корона доказательств. Как устроено «санитарное дело» (Crown of evidence. How is the «sanitary business»), Media Zona (7 July 2021) *https://mediazona.online/article/2021/07/07/korona-236*.

22. The pandemic also led to an intensification of the roll-out of Russia's Safe City programme, notably in Primorsk,[80] Yuzhno-Sakhalinsk,[81] and St. Petersburg.[82] The stated aim of the Safe City programme was to increase public safety by giving law enforcement the technological means to monitor and prevent potential threats.[83] Safe City programmes consist of government-installed surveillance camera systems, data storage systems, and software for analysing the information collected. Central to Safe City is the installation of cameras equipped with facial recognition capabilities and video analytics platforms. The system allows the automatic transfer of information to government authorities, including facial/moving objects recognition.[84] This information is available to any executive or presidential body.[85] The programme is most developed in Moscow,[86] which has among the highest number of CCTV cameras in any city in the world – over 217,000.[87]

23. The operation of video surveillance systems lies in a grey zone in which the application of national law is unclear. Court materials often only make indirect references to the use of facial recognition technology.[88] As such, while the technology is actively used as the basis for arrests and prosecutions, its use is rarely acknowledged by law enforcement authorities, making it difficult to challenge it in the courts.

II. HOW IT IS USED AND BY WHOM?

24. The overall authority over facial recognition cameras and the Safe City Programme lies with the Ministry of Digital and Mass Communications.[89] Moscow has the highest number of facial-recognition enabled cameras of all cities in Russia – in excess of 100,000.[90] These cameras cover streets, public transport, the entrances of residential buildings, and other public places such as yards, entranceways, parks, schools, and medical clinics.[91] Moscow's Department of Information

---

80 Primorsky region video surveillance system, Netris *https://www.netris.ru/en/projects/primorie/*.

81 Yuzhno-Sakhalinsk video surveillance system, Netris *https://www.netris.ru/en/projects/yuzhno-sakhalinsk/*.

82 Saint Petersburg video surveillance system, Netris *https://www.netris.ru/en/projects/saint-petersburg/*.

83 "Временные единые требования к техническим параметрам сегментов аппаратно-программного комплекса "Безопасный город" (Temporary unified requirements for the technical parameters of the segments of the hardware-software complex "Safe City"), *https://bit.ly/3gx12m2*.

84 Россия под наблюдением – 2017: как власти выстраивают систему тотального контроля над гражданами (Russia under surveillance 2017: How the Russian state is setting up a system of total control over its citizens), Fig Share (15 Dec. 2017) *https://figshare.com/articles/journal_contribution/2017-pdf/5705131*.

85 Alina Polyakova and Chris Meserole, Exporting digital authoritarianism: The Russian and Chinese models, Foreign Policy of Brookings, *https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf*.

86 Victoria Ryabikova, Are you safe from Big Brother's prying eye in Moscow?, Russia Beyond (22 July 2019) *https://www.rbth.com/science-and-tech/330697-how-real-big-brother-operates-in-moscow*.

87 Wired, "Inside Safe City, Moscow's AI Surveillance Dystopia", 6 February 2023, available at: *https://www.wired.com/story/moscow-safe-city-ntechlab/*. Surveillance cities, Surf Shark *https://surfshark.com/surveillance-cities*.

88 How Authorities Use Cameras and Facial Recognition against Protesters, OVD Info (17 Jan. 2022) *https://reports.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters*.

89 "Временные единые требования к техническим параметрам сегментов аппаратно-программного комплекса "Безопасный город" (Temporary unified requirements for the technical parameters of the segments of the hardware-software complex "Safe City"), *https://bit.ly/3gx12m2*.

90 CPA Magazine, "Moscow's 105,000 Facial Recognition Cameras Here to Stay as Country's Court System Entrenches Video Surveillance", 19 March 2020, available at: *https://www.cpomagazine.com/data-privacy/moscows-105000-facial-recognition-cameras-here-to-stay-as-countrys-court-system-entrenches-video-surveillance/*.

91 Damir Kamaletdinov, Система распознавания лиц в Москве теперь ищет протестующих. Как она устроена

Technologies (DIT) is responsible for the city's information systems and for implementing facial recognition programmes. The head of DIT, Eduard Lysenko, the Head of the DIT Department of Urban Video Surveillance, Dmitry Golovin, and the DIT official responsible for implementing digital surveillance through facial recognition technology, Alexander Gorbatko, are the principal actors in the rollout of this technology in Moscow. The DIT shares surveillance data with law enforcement and state security authorities on request.

25. At least 122sixty-two decisions issued by Russian courts in 2020-2022 referred to the use of facial recognition. Most of these cases concerned participation in peaceful protests deemed unlawful by authorities.[92] The fact that protesters often were arrested only several days after the protests took place shows that authorities increasingly used facial recognition technology to identify protest participants. One example that illustrates the use of such technology is the detention of a total of 363 protestors following a peaceful rally opposing the detention of Alexei Navalny on 21 April 2021.[93] In another case, on 12 June 2022, the police detaining 43 people in the Moscow Metro using facial recognition technology ahead of a planned anti-war protest .[94] The individuals arrested were journalists and activists known for their anti-war rhetoric.[95] The same system has also been used to identify individuals eligible for military mobilisation for the purpose of enabling the police to hand over draft letters to them.[96] In July 2023, OVD-Info reported that there have been 595 cases of facial recognition being used against protesters, 141 of which were cases of preventive detention and that facial recognition was also used for the purposes of mobilisation[97].

и что сделать для защиты (A facial recognition system in Moscow is now looking for protesters. How it works and what to do to protect), TJournal (4 Feb. 2021) *https://tjournal.ru/tech/333457-sistema-raspoznavaniya-lic-v-moskve-teper-ishchet-protestuyushchih-kak-ona-ustroena-i-chto-sdelat-dlya-zashchity*; Victoria Ryabrikova, Are you safe from Big Brother's prying eye in Moscow?, Russia Beyond (22 July 2019) *https://www.rbth.com/science-and-tech/330697-how-real-big-brother-operates-in-moscow*.

92 List of decisions of the courts of the city of Moscow 2021.

93 How Authorities Use Cameras and Facial Recognition against Protesters, OVD Info (17 Jan. 2022) *https://reports.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters*.

94 67 человек задержали в День России, 43 из них задержали в московском метро с помощью системы распознавания лиц (67 people were detained on Russia Day, 43 of them were detained in the Moscow metro using a facial recognition system), OVD Info (13 June 2022) *https://t.me/ovdinfo/14935*. В московском метро по камерам распознавания лиц задерживают участников антивоенных акций (Participants of anti-war actions are detained in the Moscow metro using facial recognition cameras), OVD News (22 Aug. 2022) *https://ovd.news/express-news/2022/08/22/v-moskovskom-metro-po-kameram-raspoznavaniya-lic-zaderzhivayut-uchastnikov*.

95 67 человек задержали в День России, 43 из них задержали в московском метро с помощью системы распознавания лиц (67 people were detained on Russia Day, 43 of them were detained in the Moscow metro using a facial recognition system), OVD Info (13 June 2022) *https://t.me/ovdinfo/14935*; В московском метро по камерам распознавания лиц задерживают участников антивоенных акций (Participants of anti-war actions are detained in the Moscow metro using facial recognition cameras), OVD News (22 Aug. 2022) *https://ovd.news/express-news/2022/08/22/v-moskovskom-metro-po-kameram-raspoznavaniya-lic-zaderzhivayut-uchastnikov*.

96 Ksenia Churmanova, Из метро - на фронт. Как власти Москвы следят за «уклонистами» с помощью системы распознавания лиц (From the subway to the front. How the authorities of Moscow monitor the "evaders" using a facial recognition system), BBC New (24 Oct. 2022) *https://www.bbc.com/russian/features-63346138*; Russia Uses Facial Recognition to Hunt Down Draft Evaders: Moscow Police Detain Draftees, Peaceful Protest Participants, Human Rights Watch (26 Oct. 2022) *https://www.hrw.org/news/2022/10/26/russia-uses-facial-recognition-hunt-down-draft-evaders*.

97 Государство-сталкер: как власти используют систему распознавания лиц против несогласных и что про это думает ЕСПЧ, ОВД-Инфо (21 July 2023) *https://data.ovdinfo.org/gosudarstvo-stalker-kak-vlasti-ispolzuyut-sistemu-raspoznavaniya-lic*

26. In November 2022, in its Concluding Observations on the eighth periodic report submitted by the Russian Federation under the International Covenant for Civil and Political Rights (ICCPR), the UN Human Rights Committee expressed concern about the widespread practice of preventive detention in Russia, facilitated by using facial recognition systems not regulated by law. The Committee also expressed concern over procedures for storing and reviewing data relating to such systems.[98] The Committee recommended that the Russian Federation refrains from using facial recognition systems and cease the practice of using preventive detention to hamper participation in peaceful assemblies.[99]

III. KEY SUPPLIERS

27. Moscow City authorities use the municipal Electronic Moscow joint stock company for the procurement of IT goods and services.[100] Electronic Moscow has published four contracts that demonstrate that local authorities procured four brands of facial recognition technology for deployment in the capital: FindFace, Luna Platform, Kipod, and Tevian FaceSDK.[101] These four contracts cost the city 130 million USD in total.[102]

28. FindFace is owned and operated by NTech Lab LLC, which was established in Russia in 2015.[103] It develops FindFace facial recognition, specialising in matching social media profiles with photos taken and reportedly does so successfully 70 percent of the time.[104] In January 2020, Moscow's DIT announced that NTech Lab would be the city's primary facial recognition software provider.[105] The company is owned by a Cypriot entity (NTech Lab LTD) whose shareholders are a consortium

---

98 Concluding observations on the eighth periodic report of the Russian Federation, Office of the High Commissioner of Human Rights (3 Nov. 2022) *https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/RUS/CCPR_C_RUS_CO_8_50614_E.pdf*.

99 Concluding observations on the eighth periodic report of the Russian Federation, Office of the High Commissioner of Human Rights (3 Nov. 2022) *https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/RUS/CCPR_C_RUS_CO_8_50614_E.pdf*.

100 Svetlana Yastrebova, Мэрия Москвы выбрала технологии для системы поиска и распознавания лиц: одним из поставщиков властей станет компания, среди владельцев которой «Ростех» и фонд Варданян (The Moscow City Hall has chosen technologies for the face search and recognition system: one of the suppliers of the authorities will be a company whose owners include Rostec and the Vardanyan Foundation), Beiomoctn (29 Jan. 2020) *https://www.vedomosti.ru/technology/articles/2020/01/29/821677-algoritm-opredelyaet*.

101 Official portal of public procurement of the Russian Federation (contract Information), (30 June 2022) *https://zakupki.gov.ru/epz/contractfz223/card/contract-info.html?id=14098697*; Official portal of public procurement of the Russian Federation (contract Information), (30 June 2022) *https://zakupki.gov.ru/epz/contractfz223/card/contract-info.html?id=14098715*; Official portal of public procurement of the Russian Federation (contract Information), (30 June 2022) *https://zakupki.gov.ru/epz/contractfz223/card/contract-info.html?id=14098714*; Official portal of public procurement of the Russian Federation (contract Information), (30 June 2022) *https://zakupki.gov.ru/epz/contractfz223/card/contract-info.html?id=14098729*.

102 *https://reestr.digital.gov.ru/reestr/*.

103 Russian Unified State Register of Legal Entities-NTech Lab LLC.

104 FindFace is a new facial recognition app that could end public privacy, Digital Trends (18 May 2016) *https://www.digitaltrends.com/photography/findface-social-networks-detect-people-public-with-70-reliability/*.

105 Svetlana Yastrebova, Мэрия Москвы выбрала технологии для системы поиска и распознавания лиц: одним из поставщиков властей станет компания, среди владельцев которой «Ростех» и фонд Варданян (The Moscow City Hall has chosen technologies for the face search and recognition system: one of the suppliers of the authorities will be a company whose owners include Rostec and the Vardanyan Foundation), Beiomoctn (29 Jan. 2020) *https://www.vedomosti.ru/technology/articles/2020/01/29/821677-algoritm-opredelyaet*.

of investment funds. NTech Lab LLC reportedly received a grant from the Russian Foundation for the Development of Information Technologies in 2021 for 78.3 million roubles.[106] It is also reported that Russia's sovereign wealth fund has invested more than 1 billion roubles (approx. USD 11 million) in NTech Lab LLC to expand its operations outside Russia, including in the Middle East and Latin America. [107]

29. Luna Platform is one of several biometric recognition technologies developed by VISION LABS LLC.[108] VISION LABS is 100 percent owned by VISIONLABS BV, a company that was incorporated in the Netherlands on 25 August 2017.[109] INTEMA SARL, a Luxembourg company that invests in and develops artificial intelligence products on international markets on behalf of MTS AI LLC, is the sole shareholder in VISIONLABS BV.[110] MTS AI LLC, an international subsidiary of Russia's largest telecom operator, MTS,[111] owns 100% of the shares in INTEMA SARL.[112] MTS's majority shareholder in turn is AFK Sistema PAO, whose biggest shareholder is Vladimir Yevtushenkov.

30. Kipod is owned and operated by Synesis LLC. Until July 2021, Nikolai Ptitsin and Peter and Alexander Shatrov jointly owned Synesis Russia and Synesis Belarus.[113] Alexander Shestakov replaced Nikolai Ptitsin on the board in 2021, and he remains Synesis's sole director and owner.

31. Tevian FaceSDK is owned and operated by Video Analysis Technologies LLC, and is co-owned by Anton and Vadim Konushin.[114] Vadim Konishin is also the general director.[115]

b. SORM

I. WHAT IS IT AND HOW DOES IT WORK?

32. The System of Operative Investigative Measures (SORM) is a legal and technological architecture that allows the authorities to monitor, store, and filter information from commercial, mobile, internet, and phone traffic across Russian telecommunications networks.[116] In other words, SORM is a form of wiretapping of mobile and internet activity.[117] The latest generation of

106 N-Tech Lab, 2022, *https://bit.ly/3gNR02y*.

107 N-Tech Lab, 2022, *https://bit.ly/3gNR02y*.

108 Extract from the register of Russian software-Luna Platform Enterprise.

109 VisionLabs BV-Uittreksel 31Oct2022. Russian Unified State Register of Legal Entities-VisionLabs LLC (14 Dec. 2022).

110 Luxembourg Register of Trade and Companies-Intema Sarl. Intema Sarl has not filed more recent documents confirming its shareholder. VisionLabs BV-Uittreksel (31 Oct 2022).

111 Alix Pressley, MTS AI Center launches US$100 million Artificial Intelligence fund and global accelerator, Intelligentcio (13 Sept. 2021) *https://www.intelligentcio.com/eu/2021/09/13/mts-ai-center-launches-us100-million-artificial-intelligence-fund-and-global-accelerator/*.

112 Luxembourg Register of Trade and Companies-Intema Sarl. Intema Sarl has not filed more recent documents confirming its shareholder.

113 U.S. Treasury Targets Belarusian Support for Russian Invasion of Ukraine, 24 February 2022, *https://home.treasury.gov/news/press-releases/jy0607*.

114 Russian Unified State Register of Legal Entities-Videoanalysis Technologies.

115 Russian Unified State Register of Legal Entities-Videoanalysis Technologies.

116 Private Interests: Monitoring Central Asia, Privacy International (Nov. 2014) *https://privacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf*.

117 Pavel Ivleev, DigitalOcean.ru, "СОРМ – «родина слышит, родина знает...» как и зачем работает государственная система контроля трафика" (SORM – "The Motherland, Hears, The Motherland Knows..." How and Why the State Traffic Control System Works), Business Digital Ocean (11 June 2016) *https://business.digitalocean.ru/n/sorm-*

SORM allows for monitoring, recording and storing extensive information relating to users of telecommunications networks. Thus, its current capabilities make it possible to digitally trace any user of telecommunication services in Russia.

33. SORM includes three components: (1) hardware and software installation at the telecommunication operation site; (2) a remote-control panel managed by law enforcement agencies; and (3) data transmission devices that internet providers must install to connect to the control panel.[118] SORM equipment is installed in all Russian data centres and at all internet traffic communication points, major search engines, and major social infrastructure facilities.[119] SORM engineers then work with each of these centres and points to install a backdoor in the systems to enable the government to wiretap them.[120] After installation, all incoming and outgoing traffic passes through the SORM equipment, making it easy for law enforcement to intercept it.[121] The State fines any telecommunication or internet provider that does not comply with the requirement to install SORM and they risk losing their operating licenses.[122]

II. HOW IS IT USED AND BY WHOM?

34. As a result of the 2016 legislation dubbed the "Yarovaya package," Russian telecommunication operators are required to record and store all text messages, voice calls and images for six months and to store metadata (including time, location, and sender and recipient information) for three years. Telecommunications companies are required to purchase and maintain the necessary equipment to operate this system.[123]

35. SORM is not implemented by regular law enforcement authorities but rather by the infamous Federal Security Service ("FSB"), the main repressive agency in the country. Although the FSB in theory is required to obtain an eavesdropping warrant from a court to access SORM data, the FSB is not legally obliged to show the warrant to anyone, not even the internet company whose

---

rodina-slyshit-rodina-znaet.

118 Alyona Sokolova, SecretMag.ru, "Что такое «пакет Яровой». Объясняем простыми словами" (What is «Yarovaya Package». Explained in simple words), (13 Nov. 2021) *https://secretmag.ru/enciklopediya/chto-takoe-paket-yarovoi-obyasnyaem-prostymi-slovami.htm*.

119 Ministry of Communications and Mass Media of the Russian Federation, Order of the Ministry of Information Technology and Communications of the Russian Federation of 16.01.2008 No. 6 "On approval of the Requirements for telecommunication networks for operational and investigative activities. Part I. General requirements", Order No. 6, (25 June, 2010) *https://digital.gov.ru/ru/documents/3923/?utm_referrer=https%3a%2f%2fwww.google.com%2f*; *https://digital.gov.ru/uploaded/files/prikaz_16-01-2008_N6_1.pdf*.

120 Pavel Ivleev, DigitalOcean.ru, "СОРМ – «родина слышит, родина знает...» как и зачем работает государственная система контроля трафика" (SORM – "The Motherland, Hears, The Motherland Knows..." How and Why the State Traffic Control System Works), (11 June 2016) *https://business.digitalocean.ru/n/sorm-rodina-slyshit-rodina-znaet*.

121 Pavel Ivleev, DigitalOcean.ru, "СОРМ – «родина слышит, родина знает...» как и зачем работает государственная система контроля трафика" (SORM – "The Motherland, Hears, The Motherland Knows..." How and Why the State Traffic Control System Works), (11 June 2016) *https://business.digitalocean.ru/n/sorm-rodina-slyshit-rodina-znaet*.

122 Pavel Ivleev, DigitalOcean.ru, "СОРМ – «родина слышит, родина знает...» как и зачем работает государственная система контроля трафика" (SORM – "The Motherland, Hears, The Motherland Knows..." How and Why the State Traffic Control System Works), (11 June 2016) *https://business.digitalocean.ru/n/sorm-rodina-slyshit-rodina-znaet*; Consultant.ru, Code of Administrative Offenses of the Russian Federation, Art. 13(46), *https://www.consultant.ru/document/cons_doc_LAW_34661/82fd5dfb3e959c3cc3cfa39795e12cb51c701c9e/*.

123 СОРМ-1, СОРМ-2, СОРМ-3: особенности и отличия (SORM-1, SORM-2, SORM-3: features and differences), (1 Nov. 2016) *https://vasexperts.ru/blog/osobennosti-i-otlichiya-sorm/*; Как устроен СОРМ? (How is SORM organized?), (17 May 2019) *https://rspectr.com/articles/515/kak-ustroen-sorm*.

equipment is being tapped. Further, companies are required to disclose user data and metadata to the Russian authorities upon request and without a court order.[124]

36. The fact that the SORM infrastructure provides a wide opportunity for extrajudicial access to private content has been condemned by the European Court of Human Rights. The Court has ruled that Russian legal provisions "do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance."[125] The European Court of Human Rights also came to the conclusion that Russian laws in this area fail to meet the "quality of law" criteria and are "incapable of limiting" the use of covert surveillance methods (in particular phone tapping) to situations where it is "necessary in a democratic society."[126]

37. On 4 July 2023, The European Court of Human Rights in the case of Glukhin v. Russia ruled that the utilization of facial recognition technology to identify and apprehend a protester during his commute on the Moscow metro violated his right to freedom of expression and privacy. Mr Nikolay Glukhin, the applicant, was apprehended by the police on a train within the Moscow metro system. The authorities informed him that he was identified through the wanted persons list due to his participation in a solo protest without prior notification to the authorities. Identification was made possible through facial recognition cameras present in the metro, with still images from the footage being utilized as evidence in the subsequent legal proceedings. Mr Glukhin was ultimately found guilty of an administrative violation, specifically failing to follow the notification protocol for public event organization[127].

III. KEY SUPPLIERS

38. CITADEL LLC is the largest manufacturer and reportedly the most important supplier of SORM hardware, software, and other related equipment in Russia. As of 8 November 2022, Citadel's ownership information disappeared from the public register of legal entities operating in Russia. This is likely due to a Russian government decree adopted in September 2022, which excluded companies subjected to western sanctions from this register.[128] Citadel occupied 50 percent of the SORM equipment market in Russia in 2017 and its share further increased to over 80 percent in 2019.[129] Up to November 2022, 99.5 percent of CITADEL LLC's shares were owned by Russian

---

124 Russia: 'Big Brother' Law Harms Security, Rights: Repeal Rushed Counterterrorism Legislation, Human Rights Watch (12 July 2016) *https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights#*.

125 Mass surveillance (The ECtHR), ECHR (Sept. 2022) *https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf*.

126 Judgment of the European Court in the case "Moskalev against the Russian Federation" (Moskalev v. Russia) dated March 5, 2018, complaint No. 44045/05 // Bulletin of the European Court of Human Rights. 2018. No. 5; Judgment of the European Court in the case "Radzhab Magomedov v. Russia" (Radzhab Magomedov v. Russia) of March 20, 2017, complaint No. 20933/08 // Bulletin of the European Court of Human Rights. 2018. No. 4.

127 Judgement of the European Court in the case "Glukhin against the Russian Federation" (Glukhin v. Russia) dated July 4, 2023, complaint No. 11519/20

128 Consultant.ru, Government of the Russian Federation, Order No. 1625, On the Definition of Cases in Which Access To Information (Data), Contained In The State Information Resource Accounting (Financial) Statements and Unified State Register of Legal Entities, May Be Limited, on Amending the Ordinance of the Government of the Russian Federation of June 6 2019 No. 729 and Invalidation Certain Provisions of Certain Acts of the Government of the Russian Federation, (16 Sept. 2022)

https://www.consultant.ru/document/cons_doc_LAW_426986/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/.

129 Andrey Kaganskikh, Proslushka.baza.io, "кто такой sneg1 и как он прослушивает россию" (Who is SNEG1 and How He Listens to Russia), *https://proslushka.baza.io/9/*; TAdviser.ru, The structure of VTB Capital purchased 25.1% of the supplier of IT systems for the Yarovaya Law, TAdviser *https://tadviser.com/index.php/Company:Citadel_of_group_of_companies*.

company X Holding LLC. Until June 2022, X Holding LLC was owned by Alisher Usmanov's USM-Telecom LLC – a company with a wide-ranging tech portfolio. X-Holding's revenue doubled from 42 billion to 91 billion roubles (1bn USD) between 2021 and 2022.[130]

39. According to available records, until October 2022, Citadel also owned MFI Soft LLC.[131] MFI Soft LLC is a supplier of SORM software and hardware to the private Russian telecommunications industry, as well as to the public Rostelecom, the FSB, and other government-affiliated agencies.[132] MFI Soft's net income has grown 298 percent since 2018.[133]

40. Signatek is another crucial player in the SORM supply chain, as it produces the telecommunications equipment needed for SORM to operate.[134] Reportedly, Signatek supplies SORM equipment to many regional departments of the Ministry of Internal Affairs, the Investigative Committee of the Russian Federation, Rostelecom, and the Russian Customs Service.[135] Citadel acquired 90% of Signatek in 2018 and, since July 2022, it has been the sole owner.[136]

c. Sovereign Ru.net

I. WHAT IS IT AND HOW DOES IT WORK?

41. The global internet plays a crucial role in ensuring access to independent information for people across the world. However, it only functions properly when it is decentralised and made freely available to all those looking to use it.[137] The Russian government has made it its goal to restrict access to the internet, and the war against Ukraine has further reinforced this trend.[138] Therefore, it is no surprise that the Russian government has attempted to create an isolated network under the guise of the world wide web that controls the information ordinary citizens can access.[139]

---

130 "Годовая выручка "ИКС Холдинга" выросла в 2,2 раза - до 91 млрд рублей" (The annual revenue of X-Holding increased by 2.2 times - up to 91 billion rubles), Interfax (11 Apr. 2023) *https://www.interfax.ru/business/895392*; Kontur Focus_report HC-X LLC. Interfax, USM closes deal to sell back IKS Holding and its assets to Cherepennikov, Interfax (9 June 2022) *https://www.interfax.ru/business/845596* .

131 Kontur focus data public procurements MFI Soft LLC; Maria Kolomychenko, Rbc.ru, "Производители прослушки раскрыли свои доходы от "закона Яровой" (Wiretapping manufacturers have disclosed their revenues from the "Yarova Law"), RBC (7 Aug. 2019) *https://www.rbc.ru/technology_and_media/07/08/2019/5d49925e9a79473386b2d28d*.

132 "Годовая выручка "ИКС Холдинга" выросла в 2,2 раза - до 91 млрд рублей" (The annual revenue of X-Holding increased by 2.2 times - up to 91 billion rubles), Interfax (11 Apr. 2023) *https://www.interfax.ru/business/895392.*

133 Kontur focus data public procurements MFI Soft LLC.

134 SPARK-Report_MFI_Soft_LLC; MFI-Soft 10Oct2023

135 Svetlana Yastrebova, Vedomosti.ru, "Партнер Усманова продолжает скупать производителей систем для закона Яровой" (Usmanov's Partner Continues to Buy Up System Manufacturers for Yarovaya Law), Beiomoctn (27 Sept. 2018) *https://www.vedomosti.ru/technology/articles/2018/09/27/782237-partner-usmanova-prodolzhaet-skupat-zakona-yarovoi*.

136 Kontur focus data public procurements SIGNATEK_LLC

137 Tech Target, Definition of "Internet", *https://www.techtarget.com/whatis/definition/Internet#:~:text=The%20Internet%2C%20sometimes%20called%20simply,to%20users%20at%20other%20computers*.

138 Gavin Wilde and Justin Sherman, Putin's internet plan: Dependency with a veneer of sovereignty, Brookings Tech Stream (11 May 2022) *https://www.brookings.edu/techstream/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/*; Understanding Russia's 'Sovereign Internet': What Happens if Russia Isolates Itself from the Global Internet, Flashpoint (11 Mar. 2022) *https://flashpoint.io/blog/russian-runet-sovereign-internet/*.

139 See e.g., Alena Epifanova, Deciphering Russia's "Sovereign Internet Law," German Council on Foreign Relations

The government refers to this sovereign internet as "Ru.net," and it allows the state to restrict information and punish those who spread information that contradicts the Kremlin's narrative.

II. HOW IS IT USED?

42. There are several components, both technical and legal, which are needed to implement a fully sovereign internet. First, it is necessary to install equipment used to filter internet content.[140] Filter equipment allows the government to control and restrict information crossing its "digital borders" and to divert traffic from specific websites.[141] For example, if protests break out in one region of the country, the government can prevent access to websites reporting on protests from the relevant geographical area to prevent the mobilisation of more people. Content filtering was initially carried out by internet service providers (ISPs) in accordance with a list of blocked websites maintained by Roskomnadzor. However, this model changed in 2021 when Roskomnadzor provided ISPs with "technical equipment for counteracting threats to stability, security, and the functional integrity of the internet on the territory of the Russian Federation" ("TSPU").[142] TSPU enables Roskomnadzor to filter internet traffic directly without any further assistance of ISPs.[143] Roskomnadzor can blacklist websites without a court order – if their content is deemed to call for unsanctioned public actions, is deemed extremist, includes materials that violate copyright, information about juvenile victims of crime, child abuse imagery, information encouraging the use of drugs, and descriptions of suicide.[144]

43. Data sent over the internet consists of so-called "packets," which contain the source of information, the destination IP address, and port numbers.[145] Additionally, the packets contain information revealing its origin. For example, a packet that originates from Telegram features different information than a packet that originates from Facebook Messenger.[146] TSPU uses a deep packet inspection (DPI) technique that looks past immediately accessible information such as the IP address and delves into additional information that makes it easier to identify the content and purpose of data.[147] DPI is being abused to check if individual packets originate

---

(January 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*.

140 See e.g., Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*.

141 Andrei Soldatov and Irina Borogan, The New Iron Curtain, CEPA (7 June 2022) *https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/*.

142 Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*; Evgenia Chernyshova, RBC Trends, Зачем власти создают «суверенный Рунет»: от чего он защитит и чем грозит (Why do the authorities create a 'sovereign Runet'), (28 Feb. 2022) *https://trends.rbc.ru/trends/industry/609a52329a79471fba0f0837*; Gotta block 'em all (but can't), Mediazona (14 June 2022) *https://en.zona.media/article/2022/06/14/ruvpn*; Andrei Soldatov and Irina Borogan, The New Iron Curtain, CEPA (7 June 2022) *https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/*.

143 Diwen Xue, et al, TSPU: Russia's Decentralised Censorship System, (27 Oct. 2022) *https://ensa.fi/papers/tspu-imc22.pdf*; Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*.

144 Roskomnadzor, Powers of Roskomnadzor, available at: *https://eng.rkn.gov.ru/about/powers_of_roskomnadzor/*.

145 Ericka Chickowski, Deep packet inspection explained, AT&T Cybersecurity Blog (2 Oct. 2020), *https://cybersecurity.att.com/blogs/security-essentials/what-is-deep-packet-inspection*.

146 Evgenia Chernyshova, Зачем власти создают «суверенный Рунет»: от чего он защитит и чем грозит (Why do the authorities create a 'sovereign Runet'), RBC Trends (28 Feb. 2022).

147 Ericka Chickowski, Deep packet inspection explained, AT&T Cybersecurity Blog (2 Oct. 2020), *https://cybersecurity.att.com/blogs/security-essentials/what-is-deep-packet-inspection*.

from a flagged source and to prevent it from passing through in that case – an effective tool for internet censorship.[148] For example, in summer 2019, the Russian authorities used DPI to interrupt internet access during mass protests throughout Moscow.[149] In another example, Roskomnadzor used DPI equipment to throttle the loading speeds for Twitter when the platform failed to comply with removal requests.[150] Thus, in these two cases, DPI was used for two different purposes: in the first case, to restrict public access to certain types of information in a particular geographical area during a particular event and, in the second case, to interfere with a platform's operating performance as a means to pressure it into complying with requests to remove information.

44. Roskomnadzor also uses this technology to target specific individuals, as was seen when the authorities accused websites and organisations affiliated with Alexei Navalny of carrying out "extremist activities."[151] DPI was an easy and effective way to block Navalny's websites from operating.[152] In total, Roskomnadzor reportedly blocked 610,654 web pages in 2022, including foreign media, human rights websites, Facebook, Instagram, and Twitter.[153]

45. Roskomnadzor also uses Ru.net to blacklist, ban and block individual sites. Roskomnadzor maintains a list of sites, which have been prohibited because they allegedly have published unlawful information on suicides, drugs, child pornography, "extremism" and other issues. ISPs are required to block access to the sites prohibited by Roskomnadzor.[154] Because of the lack of a clear definition of "extremism" in national law, basically any information critical of the Kremlin can be deemed "extremist".[155] Since its creation, Roskomnadzor has blacklisted over a million websites.[156] The blocking procedures of Roskomnadzor lack transparency and affected website owners are not given any opportunity to rectify alleged violations.[157]

---

148 Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*; Alexandra Propokenko, Закон о суверенном рунете. Как он возник и к чему приведет" (Law on the sovereign runet. How did it come about and what will it lead to?), (18 April 2019) *https://carnegiemoscow.org/commentary/78928*.

149 Freedom on the Net 2022: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2022*.

150 Freedom on the Net 2022: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2022*; Andrei Soldatov and Irina Borogan, The New Iron Curtain, CEPA (7 June 2022) *https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/*.

151 Russia Blocks 49 Navalny-Linked Websites, Allies Say, The Moscow Times (26 July 2021) *https://www.themoscowtimes.com/2021/07/26/russia-blocks-49-navalny-linked-websites-allies-say-a74618*.

152 Freedom on the Net 2022: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2022*.

153 Roskomsvoboda, "'Сетевые свободы' выпустили доклад об уровне свободы Рунета в 2022 году" ('Network Freedoms' released a report on the level of freedom of Runet in 2022), (2 Feb. 2023) *https://roskomsvoboda.org/post/doklad-2va-runeta-2022/*.

154 From 'protecting children' to 'discrediting the army' – A brief history of 10 years of Russian Internet censorship, Meduza (6 Nov. 2022) *https://meduza.io/en/feature/2022/11/06/from-protecting-children-to-discrediting-the-army*; Andrei Soldatov and Irina Borogan, The New Iron Curtain, CEPA (7 June 2022) *https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/*.

155 Andrei Soldatov and Irina Borogan, The New Iron Curtain, CEPA (7 June 2022) *https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/*.

156 Roskomsvoboda, "Monitoring of Registry", *https://reestr.rublacklist.net/en/?status=1&gov=all&date_start=&date_end*; "Роскомнадзор в 2022 году внес более 384 тыс. ссылок в Единый реестр запрещенной информации" (Roskomnadzor added more than 384,000 links to the Unified Register of Prohibited Information in 2022), Tass (16 February 2023) *https://tass.ru/obschestvo/17071733*.

157 Freedom on the Net 2022: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2022*.

46. The authorities employ several additional methods to restrict speech on Ru.net. The network uses a state-controlled domain name system (DNS) to register a text-based URL address as a numerical IP address.[158] Normally, domain names are assigned to a number of servers and lack a central database.[159] However, the Russian DNS, which is currently being rolled out, will enable the authorities to control internet users' access to information as it will feature a centralised list of all IP addresses on the network and allow for determining the address provided to an ISP when a user carries out a search on its system.[160] The sovereign Russian internet, which is being created, will also require Russian-owned domains to obtain a security certificate through the Russian-owned DNS. This means that sites will not work on Western browsers such as Google Chrome but only on Russian browsers such as Yandex or Atom, resulting in further isolation of Russian internet users.[161]

47. Russia has banned most virtual private networks (VPNs), which allow anonymous internet browsing by hiding a user's IP address[162] and enables users to bypass local restrictions on accessing websites.[163] Similarly, the government has required ISPs to block the installation of Tor, a well-known tool for masking online activity.[164] These measures have decreased the ability of people in Russia to use the internet anonymously and have simultaneously cut off Russia from the rest of the world by reducing external traffic.[165]

48. The process of creating the closed Ru.net network began in 2010 when the government passed content regulations.[166] Once Roskomnadzor was set up, the mechanisms were in place to begin banning sites and controlling online information.[167] Restrictions were first imposed on sites featuring information on widely disfavoured topics such as child pornography and drugs, but the list soon broadened to include websites accused of promoting rioting, disseminating "extremist"

---

158 Understanding Russia's "Sovereign Internet": What Happens If Russia Isolates Itself from the Global Internet?, Flashpoint (11 Mar. 2022) *https://flashpoint.io/blog/russian-runet-sovereign-internet/*.

159 Roman Goncharenko, Is Russia building its own internet?, Deutsche Welle (17 Jan. 2018) *https://www.dw.com/en/russia-moves-toward-creation-of-an-independent-internet/a-42172902*; Kieren McCarthy, Russia threatens to set up its 'own internet' with China, India and pals, The Register (1 Dec. 2017) *https://www.theregister.com/2017/12/01/russia_own_internet/*; P. Mockapetris, Domain Names-Implementation and Specification, Network Working Group (Nov. 1987) *https://datatracker.ietf.org/doc/html/rfc1035*.

160 Russia: Growing Internet Isolation, Control, Censorship: Authorities Regulate Infrastructure, Block Content, Human Rights Watch (18 June 2020) *https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship*.

161 D-Russia, "Чем российским онлайн-ресурсам грозит отзыв SSL-сертификатов" (What threatens Russian online resources with the revocation of SSL certificates), (2 Mar. 2022) *https://clck.ru/3444Pw*.

162 Russia: Growing Internet Isolation, Control, Censorship: Authorities Regulate Infrastructure, Block Content, Human Rights Watch (18 June 2020); Freedom on the Net 2022: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2022*.

163 SkillFactory.ru, "VPN", (27 Mar. 2023) *https://clck.ru/346mr7*.

164 Russia is trying to build its own great firewall, The Economist (19 Feb. 2022) *https://www.economist.com/business/russia-is-trying-to-build-its-own-great-firewall/21807706*.

165 Freedom on the Net 2022: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2022*: Andrei Soldatov and Irina Borogan, The New Iron Curtain, CEPA (7 June 2022) *https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/*.

166 iFreedomLab, "Полная история регулирования интернета в России: от 80-х и до наших дней" (A Complete History of Internet Regulation in Russia: from the 80s to the present day), *https://ifreedomlab.net/campaignes/istoriya-regulirovaniya-svyazi/#2*.

167 iFreedomLab, "Полная история регулирования интернета в России: от 80-х и до наших дней" (A Complete History of Internet Regulation in Russia: from the 80s to the present day).

content, and calling for protests.[168] Ru.net goes as far as banning access to informative sites regarding illegal or illicit subjects, such as a Wikipedia page about drugs.[169]

49. Ru.net is more than just a tool for controlling access to information; it also is used to collect data.[170] Since 2015, all domestic and foreign internet companies operating in Russia have been required to store users' data on servers physically located within Russia.[171] In 2016, this obligation was extended to telecommunication companies, which are now required to store text messages, phone conversations, images, videos, and metadata in similar servers.[172]

50. Ru.net was further expanded in 2019 when the authorities passed regulations to monitor international communication lines and Internet Exchange Points (IXPs).[173] While IXPs are used to communicate with the global internet, the 2019 regulations required that all internet traffic into Russia be routed through IXPs included in the Russian IXP register, managed by Roskomnadzor.[174] The regulation allowed Roskomnadzor to restrict traffic through these IXPs in the event of an "external threat," a term not fully defined, giving Roskomnadzor overly broad authority.[175]

51. Since there are no clear rules regarding oversight of Roskomnadzor's decisions and the judicial branch lacks powers to review them, the government can block internet content and restrict access to sites and IXPs unfettered.[176] Additionally, the government still has to release the full list of websites banned by Roskomnadzor; without a publicly available list, internet restrictions are immune from public scrutiny.[177]

---

168 Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*.

169 Alexander Isavnin, The Russian Sovereign Internet and Number Resources, RIPE Labs (31 Mar. 2022), *https://labs.ripe.net/author/alexander-isavnin/the-russian-sovereign-internet-and-number-resources/*.

170 "Processing and storage of personal data in the Russian Federation. Changes from September 1, 2015" [in Russian], Ministry of Digital Development, Communications and Mass Media of the Russian Federation, (12 Feb. 2016); See also Regulation of personal data in the Russian Federation changes from September 1, 2015, TAdvisor (10 Apr. 2023) *https://tadviser.com/index.php/Article:Processing_of_personal_data_in_Russia*.

171 "Processing and storage of personal data in the Russian Federation. Changes from September 1, 2015" [in Russian], Ministry of Digital Development, Communications and Mass Media of the Russian Federation, (12 Feb 2016); See also Regulation of personal data in the Russian Federation changes from September 1, 2015, TAdvisor (10 Apr. 2023) *https://tadviser.com/index.php/Article:Processing_of_personal_data_in_Russia*.

172 Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*; Alexander Tabachnik, The Yarovaya Law as an Example of Ill-conceived Legislation, University of Haifa, Center for Cyber Law and Policy Blog *https://cyber.haifa.ac.il/index.php/all-posts/yarovaya-law*.

173 Max Seddon, Putin signs law to isolate Russian internet, Financial Times (1 May 2019) *https://www.ft.com/content/9ba46770-6c36-11e9-80c7-60ee53e6681d*; Maxim Edwards, What lies ahead for the RuNet in 2020?, Global Voices (26 Dec. 2019) *https://globalvoices.org/2019/12/26/what-lies-ahead-for-the-runet-in-2020/*; Freedom on the Net 2019: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2019*.

174 Freedom on the Net 2019: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2019*.

175 Vasilisa Strizh, Morgan Lewis, Sovereign Runet Law: Russia Considers Taking Control of Internet in Emergency Situations, (29 April 2019); Freedom on the Net 2019: Russia, Freedom House *https://freedomhouse.org/country/russia/freedom-net/2019*; Putin Signs 'Sovereign Internet' Law, Expanding Government Control of Internet, RFE/RL (1 May 2019) *https://www.rferl.org/a/putin-signs-sovereign-internet-law-expanding-governmentcontrol-of-internet/29915008.html*.

176 Vasilisa Strizh, Morgan Lewis, Sovereign Runet Law: Russia Considers Taking Control of Internet in Emergency Situations, (29 April 2019); Freedom on the Net 2019: Russia, Freedom House, *https://freedomhouse.org/country/russia/freedom-net/2019*; Putin Signs 'Sovereign Internet' Law, Expanding Government Control of Internet, RFE/RL (1 May 2019) *https://www.rferl.org/a/putin-signs-sovereign-internet-law-expanding-governmentcontrol-of-internet/29915008.html*.

177 Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP

52. The measures taken by the government to date shows that the goal of the Kremlin is to create a highly controlled version of the internet.[178] Putin recognises that the isolation of the Russian people is his greatest ally and that the more the free flow of information is restricted, the stronger his foothold becomes.[179] That is why there has been a ten-year campaign to expand the reach of the information security section of the National Security Strategy.[180] As currently worded the National Security Strategy suggests that any information that the authorities cannot verify has been channelled through untrustworthy international tech companies, represents historical facts distorted for political reasons, constitutes a breach of Russia's territorial sovereignty, or originates from terrorist and extremist organisations calling for civil unrest.[181] The National Security Strategy further suggests that online anonymity leads to an increase in crimes and that the use of foreign information technologies and equipment has increased the influence in Russia of institutions based abroad.[182]

53. These policy objectives are clearly aimed at controlling all sources of public information in Russia – with the view to indefinitely retaining the economic and political levers of power in Russia.[183] As eloquently summarised by George Orwell in his seminal work 1984, "Those who control the present, control the past and those who control the past control the future".

III. KEY USERS AND SUPPLIERS

54. Roskomnadzor and its head Andrey Lipov oversee the entire sovereign internet project.[184] Roskomnadzor was established in 2008 to implement laws regulating internet use in Russia.[185] Roskomnadzor also oversees the Main Radio Frequency Centre (MRFC) and the Centre for

---

(Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*; Alexandra Propokenko, Закон о суверенном рунете. Как он возник и к чему приведет (Law on the sovereign runet. How did it come about and what will it lead to?", Carnegie Moscow (18 Apr. 2019), at para. 13, *https://carnegiemoscow.org/commentary/78928*.

178 Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*; Alexandra Propokenko, Закон о суверенном рунете. Как он возник и к чему приведет (Law on the sovereign runet. How did it come about and what will it lead to?", Carnegie Moscow (18 Apr. 2019), at para. 13, *https://carnegiemoscow.org/commentary/78928*.

179 Russia, Blocked From the Global Internet, Plunges Into Digital Darkness, New York Times (7 Mar. 2022) *https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html*.

180 What you need to know about Russia's 2021 national security strategy, Meduza (5 July 2021) *https://meduza.io/en/feature/2021/07/05/what-you-need-to-know-about-russia-s-2021-national-security-strategy*.

181 What you need to know about Russia's 2021 national security strategy, Meduza (5 July 2021) *https://meduza.io/en/feature/2021/07/05/what-you-need-to-know-about-russia-s-2021-national-security-strategy*.

182 What you need to know about Russia's 2021 national security strategy, Meduza (5 July 2021) *https://meduza.io/en/feature/2021/07/05/what-you-need-to-know-about-russia-s-2021-national-security-strategy*.

183 Alena Epifanova, German Council on Foreign Relations, Deciphering Russia's "Sovereign Internet Law," DGAP (Jan. 2020) *https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf*; Alexandra Propokenko, Закон о суверенном рунете. Как он возник и к чему приведет (Law on the sovereign runet. How did it come about and what will it lead to?), Carnegie Moscow (18 Apr. 2019), at para. 13, *https://carnegiemoscow.org/commentary/78928*.

184 Austrian Red Cross & Accord, Russian Federation: Political protests and dissidence in the context of the Ukraine invasion, (May 2022) *https://www.ecoi.net/en/file/local/2073690/ACCORD-2022-05-Russian_Federation_Protesters_and_Dissidents.pdf*; Roskomnadzor, "Statute of Roskomnadzor", Article 1, *https://eng.rkn.gov.ru/about/statute_of_roskomnadzor/*; Government.ru, "Ministries and Agencies" *http://government.ru/en/ministries/#federal_ministries*.

185 Government.ru, "Ministries and Agencies" *http://government.ru/en/ministries/#federal_ministries*; About Roskomnadzor: Historical Reference, Rkn.gov.ru *https://rkn.gov.ru/about/p530/*

Monitoring and Controlling Public Communications Networks (CMCPCN).[186] Roskomnadzor and its two sub-units monitor the internet to identify sites that fail to comply with information-blocking laws and issue fines and bans to ensure compliance.[187] Andrey Lipov has led Roskomnadzor since March 2020 and was a key initiator of the sovereign internet project.[188] As chief architect of Ru.net, Lipov has been responsible for establishing and supervising the network and the banning of websites.[189]

55. The CMCPCN, headed by Sergey Khutortsev, was established in 2019. It was tasked with blocking banned content and monitoring and reporting on threats to the stability and security of Ru.net.[190] The MRFC, under the lead of its head Ruslan Nesterenko and senior manager Alexander Fedotov, is primarily responsible for monitoring the internet in order to identify information considered offensive to the Russian state or President Putin.[191] For example, information about the president's health issues, critical comments by residents in regions that he recently visited, or negative information about other government officials might be deemed offensive.[192] The MRFC also monitors public discussion about the mobilisation of protests or social tension.[193]

56. Palitrum Lab LLC provides Brand Analytics, the social media and media monitoring system used by the MRFC.[194] Brand Analytics collects and organises social media comments and analyses this information to better understand public reactions to certain products.[195] Thus, when used by MRFC, the system allows Putin to find out what people are saying about him or his competitors and protect his "brand" against threats from his competitors.[196]

---

186 Diwen Xue, et al, TSPU: Russia's Decentralised Censorship System, (27 Oct. 2022) *https://ensa.fi/papers/tspu-imc22.pdf*; Runet Sovereignty. How the Kremlin is building a national web with censorship even a VPN won't defeat, The Insider (11 Mar. 2022) *https://theins.ru/en/politics/249095*; Freedom on the Net 2022: Russia; Freedom House, *https://freedomhouse.org/country/russia/freedom-net/2019*.

187 Roskomnadzor, "Statute of Roskomnadzor" – Article 5, *https://eng.rkn.gov.ru/about/statute_of_roskomnadzor/*; Freedom on the Net 2022: Russia, Freedom House, *https://freedomhouse.org/country/russia/freedom-net/2019*.

188 Freedom on the Net 2022: Russia, Freedom House, *https://freedomhouse.org/country/russia/freedom-net/2019*.

189 Runet Sovereignty. How the Kremlin is building a national web with censorship even a VPN won't defeat, The Insider (11 Mar. 2022) *https://theins.ru/en/politics/249095*.

190 Center for Monitoring and Control of the Public Communications Network, TAdvisor, ("Центр мониторинга и управления сетью связи общего пользования"), *https://clck.ru/33KML3*.

191 Alesya Marokhovskaya , Irina Dolinina , Sonya Savina , Editorial staff , Polina Uzhvak , Katya Bonch-Osmolovskaya, Important Stories, "Как Роскомнадзор власть Путина бережет (How Roskomnadzor protects Putin's power), (8 Feb. 2023); ФГУП 'ГРЧЦ' (Federal State Unitary Enterprise "GRChTs"), Meduza (8 Feb. 2023).

192 Alesya Marokhovskaya , Irina Dolinina , Sonya Savina , Editorial staff , Polina Uzhvak , Katya Bonch-Osmolovskaya, Important Stories, "Как Роскомнадзор власть Путина бережет (How Roskomnadzor protects Putin's power), (8 Feb. 2023).

193 Alesya Marokhovskaya , Irina Dolinina , Sonya Savina , Editorial staff , Polina Uzhvak , Katya Bonch-Osmolovskaya, Important Stories, "Как Роскомнадзор власть Путина бережет (How Roskomnadzor protects Putin's power), (8 Feb. 2023); see also Brand Analytics website, *https://br-analytics.ru/en_RU/*.

194 Alesya Marokhovskaya , Irina Dolinina , Sonya Savina , Editorial staff , Polina Uzhvak , Katya Bonch-Osmolovskaya, Important Stories, "Как Роскомнадзор власть Путина бережет (How Roskomnadzor protects Putin's power), (8 Feb. 2023); see also Brand Analytics website *https://br-analytics.ru/en_RU/*.

195 Brand Analytics website *https://br-analytics.ru/en_RU/*.

196 Alesya Marokhovskaya , Irina Dolinina , Sonya Savina , Editorial staff , Polina Uzhvak , Katya Bonch-Osmolovskaya, Important Stories, "Как Роскомнадзор власть Путина бережет (How Roskomnadzor protects Putin's power), (8 Feb. 2023).

57. E.Soft is the largest IT supplier of Roskomnadzor and MRFC.[197] It is the sole developer of the group's IT systems, provides technical support, and fulfils other government contracts.[198] Valeria Prohortseva is the CEO of E.Soft. and Dmitry Bulatov is the sole shareholder of both Inforser Engineering LLC and E.soft.[199] Both companies have contracts for billions of roubles with the Russian Ministry of Defence.[200] E.Soft has also helped develop the Registry of Information Resources of Foreign Agents and the Registry of Prohibited Internet Resources, which is used to block prohibited content.[201]

58. RDF.RU, headed by Dmitry Nikiforov, provides Roskomnadzor with TSPU. TSPU includes URL-filtering services and DPI technology.[202] Additionally, NTC Vulkan, another IT company, develops software to monitor the internet and block websites.[203] Its clientele includes the Russian Ministry of Defence, FSB, and the Foreign Intelligence Service.[204] The company's founders are Anton Markov and Alexander Irzhavsky, and its director is Roman Vinokurov.[205] Vulkan's main development is a programme called Amezit, which the Ministry of Defence reportedly uses to monitor all internet users in a geographical area, block access to unwanted sites, and redirect them to approved content.[206] Another programme called Fraction was reportedly developed by Vulkan for the FSB. This programme scans social media sites to identify potential opposition figures.[207]

---

197 The Russian government's Internet blacklist is managed by a private company whose main client is the military, Meduza (19 Apr. 2018) *https://meduza.io/en/feature/2018/04/19/the-russian-government-s-internet-blacklist-is-managed-by-a-private-company-whose-main-client-is-the-military*; Alesya Marokhovskaya, et al, Important Stories, Inside the Censorship Machine, (8 Feb. 2023) *https://istories.media/en/stories/2023/02/08/inside-the-censorship-machine/* and, in Russian, at *https://meduza.io/feature/2018/04/19/uchet-dannyh-o-blokirovkah-dlya-roskomnadzora-vedet-storonnyaya-kompaniya-ee-osnovnoy-zakazchik-struktury-minoborony*.

198 The Russian government's Internet blacklist is managed by a private company whose main client is the military, Meduza (19 Apr. 2018).

199 E.Soft_Register Extract; Rusprofile.ru, "Prohortseva Valeria Sergeevna" *https://www.rusprofile.ru/person/prokhorceva-vs-110374261215*.

200 The Russian government's Internet blacklist is managed by a private company whose main client is the military, Meduza (19 Apr. 2018); See also INFORSER ENGINEERING LLC_Kontur-Focus.

201 E.Soft_interaction with foreign agents_Cyber-Partisans; E.Soft_Registry of Information Resources of Foreign Agents (2)_Cyber-Partisans; E.Soft_Registry of Information Resources of Foreign Agents_Cyber-Partisans.

202 RocketReach, Rdp.Ru Information, *https://rocketreach.co/rdp-ru-profile_b4510b79fc738d68*.

203 Важные истории»: малоизвестная IT-компания по заказу Минобороны РФ создает программы для изоляции интернета, кибератак и управления «фабрикой троллей» ("'Important Stories': a little-known IT company"), Meduza (30 Mar. 2023) *https://meduza.io/news/2023/03/30/vazhnye-istorii-maloizvestnaya-it-kompaniya-po-zakazu-minoborony-rf-sozdaet-programmy-dlya-izolyatsii-interneta-kiberatak-i-upravleniya-fabrikoy-trolley*.

204 Важные истории»: малоизвестная IT-компания по заказу Минобороны РФ создает программы для изоляции интернета, кибератак и управления «фабрикой троллей» ('Important Stories': a little-known IT company), Meduza (30 Mar. 2023) *https://meduza.io/news/2023/03/30/vazhnye-istorii-maloizvestnaya-it-kompaniya-po-zakazu-minoborony-rf-sozdaet-programmy-dlya-izolyatsii-interneta-kiberatak-i-upravleniya-fabrikoy-trolley*.

205 NTC VULKAN_Registry Extract; NTC VULKAN_Kontur-Focus; Важные истории»: малоизвестная IT-компания по заказу Минобороны РФ создает программы для изоляции интернета, кибератак и управления «фабрикой троллей» ('Important Stories': a little-known IT company), Meduza (30 Mar. 2023) *https://meduza.io/news/2023/03/30/vazhnye-istorii-maloizvestnaya-it-kompaniya-po-zakazu-minoborony-rf-sozdaet-programmy-dlya-izolyatsii-interneta-kiberatak-i-upravleniya-fabrikoy-trolley*.

206 Важные истории»: малоизвестная IT-компания по заказу Минобороны РФ создает программы для изоляции интернета, кибератак и управления «фабрикой троллей» ('Important Stories': a little-known IT company), Meduza (30 Mar. 2023) *https://meduza.io/news/2023/03/30/vazhnye-istorii-maloizvestnaya-it-kompaniya-po-zakazu-minoborony-rf-sozdaet-programmy-dlya-izolyatsii-interneta-kiberatak-i-upravleniya-fabrikoy-trolley*.

207 'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics, The Guardian (30 Mar. 2023) *https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics*.

Conclusions and recommendations

59. This report argues that digital authoritarianism plays a major role in Putin's attack on democracy and human rights in Russia. It also facilitates Russia's war in Ukraine both directly (by assisting the authorities to identify men subject to mobilization) and indirectly (by enabling the authorities to maintain public support for the war by silencing criticism, suppressing anti-war protests and restricting access to information about Russian war crimes in Ukraine).

60. In particular the SORM and sovereign internet programmes have given the Kremlin control over the last remaining platform for free information exchange in Russia, i.e., the internet. These tools have enabled the Russian authorities to wiretap the internet. The Facial Recognition and Safe City Programme have allowed the regime to track physical movements of activists, journalists and opponents of the regime, thereby turning major cities into de facto open prisons. Both technologies have reportedly began to appear in Russian-occupied regions of Ukraine and are being exported to prop up other authoritarian regimes.

61. The supply, maintenance and operation of digital authoritarianism systems depend on imports of hardware and software from abroad. Thus, the continued export of these components to Russia – either directly or through regional proxies helps to preserve Putin's regime and protects the Russian authorities from public scrutiny and accountability for their aggression and war crimes in Ukraine.

62. For these reasons, and based on the information provided in this report, IPHR would like to make the following recommendations to the European Union and its Members States, governments of the United Kingdom, United States, Canada and their allies and partners:

    a. Designate all key manufacturers, suppliers, procurers and users of digital authoritarian technologies in Russia for sanctions;

    b. Tighten trade restrictions and other measures to prevent third party states and corporate entities from acting as proxies for Russian importers of key technology and components required for the manufacture, operation and maintenance of digital authoritarian technologies;

    c. Prevent Russia from exporting its brand of digital authoritarianism to other states;

    d. Incentivise former Soviet Union states and other regional neighbours with closer trade links and other economic incentives to turn away from Russia's sphere of malign influence;

    e. Invest in technological solutions, cyber security and capacity building to help the Russian opposition, civil society activists, journalists and human rights defenders to defend themselves against the Kremlin's digital authoritarianism;

    f. Step up political and economic pressure on the Russian government to roll back repression at home and to end its war of aggression against Ukraine.