Russia and Eurasia Studies Programme

Russian Big Tech:
Building and Exporting a "Sovereign Internet"

Alena Epifanova

For over a decade, Russia has pursued a strategic effort to reshape the internet. Vladimir Putin views the free flow of information and people's unrestricted access to the global web as a fundamental threat to his regime. This FOI Memo examines how Russian tech companies enable domestic censorship and surveillance while projecting Russia's digital control beyond its borders.

- A "sovereign internet" policy has emerged as a central tool for preventing the free flow of information inside Russia and for consolidating power.
- Putin's vision of a "sovereign internet" is tied to his broader agenda of "reclaiming sovereignty" and concerns not only Russia's domestic control but also how it shapes Moscow's digital foreign policy.
- Both the domestic and foreign dimensions of Russia's internet policy rely on its technology companies such as Rostelecom, MTS, VK, Yandex, and other tech giants.
- These big-tech companies act not only as pillars of internal censorship and surveillance but also as conduits for exporting digital authoritarian practices abroad.

Test launch by Miranda-Media telecom service provider in the so called Lugansk People's Republic, 12 October 2023.
Source: Itar-Tass, Alexander Reka

Internet and Sovereignty

Russia's political regime has frequently invoked the necessity and assurance of "sovereignty" to justify its actions: whether to change the Constitution,[1] restrict access to information, increase repression,[2] or declare war.[3] In international relations, sovereignty is also one of the most desired qualities, as only great powers, according to Russian thinking, can be sovereign. Russia's leadership is convinced that only sovereign states can exercise genuinely independent foreign policy, be respected in the international arena and compete in shaping the global order.

Similarly, this notion of sovereignty applies to the internet. Yet, the internet and state sovereignty are in structural tension. The global internet is borderless, transnational, mostly private; it violates the principles of territoriality and undermines state authority

1 President of Russia, *Presidential Address to the Federal Assembly*, 15 January 2020, http://en.kremlin.ru/events/president/news/62582.

2 Maria Kolomychenko, "Russia's Fight Against 'Foreign Agents' and How to Prevent Its Spread," *DGAP Analysis No 3*, July 2025, https://dgap.org/en/research/publications/russias-fight-against-foreign-agents-and-how-prevent-its-spread.

3 President of Russia, *Address by the President of the Russian Federation*, 24 February 2022, http://en.kremlin.ru/events/president/news/67843.

FOI Memo 9215
Project no: A12601
Approved by: Karolina Gasinska Singh

February 2026

in information exchange. Its governance model gives nation-states just one voice among many, alongside private companies, technical experts, and civil society. The period when the internet became a truly global web and the multi-stakeholder model started to take shape, in the 1990s, is perceived in Russia as a chaotic time characterised by weak statehood following the collapse of the Soviet Union. While the Soviet Union developed projects for computer networks, none of them succeeded.[4] It was American companies that built much of the internet infrastructure that connected people into a global web. By expanding access to information and communication platforms worldwide, the internet came to be seen as a key pillar of the post-Cold War liberal international order.[5]

Against this background, Putin viewed the global internet as an expression of Western dominance, embedded in technical standards and governance norms that promoted liberal democracy. Consequently, calls for a "sovereign internet" emerged as part of a broader effort to restore state authority, reassert control over information flows, and shield domestic affairs from perceived external influence.

This ambitious endeavour is only possible to implement through controlled technologies and centralised management. While the Federal Service for Supervision of Communications, Information Technology and Mass Media (abbreviated *Roskomnadzor*) took over this latter function, Russian companies provided the necessary technologies.

Yet, Russia's "sovereign internet" policy extends beyond domestic control and functions as a key pillar of a broader ambition to shape the international digital order. Russian technology companies export digital infrastructure and services abroad, embedding surveillance capabilities and authoritarian governance practices into the information systems of other states (see below, pp. 6–8). Once a diverse and innovative sector, Russia's information technology industry has gradually become centralised and oriented toward the international diffusion of the concept of a "sovereign internet," fostering a Russian digital sphere of influence and deepening the technological dependence of primarily post-Soviet states.

Moscow's concept of sovereignty

The idea of Russia's sovereignty as it is understood today took shape in the early 2000s during discussions of so-called sovereign democracy and Russia's role in the world. The impetus was likely the "Rose Revolution" in Georgia in 2003, the "Orange Revolution" in Ukraine in 2004, and the "Tulip Revolution" in Kyrgyzstan in 2005, which were perceived in Moscow as Western interference and a threat to Russia and its influence in the post-Soviet countries. In 2006, a collection of articles titled *Sovereignty*, brought together, under one cover, Vladimir Putin, Dmitry Medvedev, Vladislav Surkov, Alexander Filippov, and others, and set the sovereignty discourse in motion.[6]

According to Putin, Russia "will decide for itself, taking into account its historical, geopolitical, and other specific characteristics, how to ensure the realisation of the principles of freedom and democracy,"[7] thereby distinguishing the country from liberal democracies in Europe and the United States. The then-influential ideologist of a "sovereign democracy," Surkov, argued that Russian political development must take place without foreign influence and be based on "Russian political culture," with "a strong central state" as its core.[8] Probably inspired by the controversial German political theorist Carl Schmitt and his fierce criticisms of parliamentary democracy and liberalism,[9] Russian ideologists understood sovereignty as the authority to suspend constraints of legal norms and international obligations in situations framed as exceptions and threat.[10]

Importantly, these authors highlight that a sovereign Russia does not mean an isolated Russia. "It is not a fortress," as Surkov claims; on the contrary, "it is a way out into the world, it is a participation in an open struggle," it is a bid for equal participation in decision-making "on issues of organising the world order."[11]

This conception aligns with Putin's longstanding opposition to a unipolar world led by the United

4 Benjamin Peters, *How Not to Network a Nation: The Uneasy History of the Soviet Internet* (The MIT Press, 2016), 2.

5 Johannes Thumfart, *The Liberal Internet in the Postliberal Era: Digital Sovereignty, Private Government, and Practices of Neutralization* (Palgrave Macmillan, 2024), 10–12.

6 Nikita Garadzha, *Sovereignty (Suverenitet)* (Evropa, 2006).

7 Garadzha, *Sovereignty*, 16.

8 Lewis, *Russia's New Authoritarianism*, 52.

9 David G. Lewis, *Russia's New Authoritarianism: Putin and the Politics of Order* (Edinburgh University Press, 2020), 17.

10 Garadzha, *Sovereignty*, 91.

11 Ibid., 34.

States, "one master, one sovereign."[12] Instead, Moscow advocates a multipolar world in which Russia also has "the right to dominate,"[13] alongside other powers, free from the influence of other states and international organisations.

Russia's pursuit of a "sovereign internet" is closely linked to its broader concept of sovereignty and its criticism of U.S. dominance over the internet. Core digital infrastructures and services, such as the global domain name system (DNS) and major social media platforms, originated in the United States and are seen as sources of external influence over Russia's information space. The 2013 Snowden revelations about extensive U.S. surveillance of global telecommunications reinforced the Russian leadership's belief that it needed its own "sovereign internet," independent of foreign technologies.[14]

These concerns were not unique to Russia: even liberal democracies began debating digital sovereignty and the strategic risks of dependence on foreign companies. However, while discussions in democratic countries have been held within legal, economic, and rights-based frameworks,[15] Russia's concept of a "sovereign internet" drew more heavily on the state's monopoly on control and the primacy of territoriality.[16]

As a result, the Russian government has built a robust and intricate legal and institutional framework, brought domestic technology companies under control and suppressed foreign platforms. The so-called Sovereign Internet Law from 2019 is a milestone in Russia's path to a "sovereign internet." It laid the ground for a qualitatively new transition from indirect control over content on the internet to centralised state management of the internet infrastructure within the borders of Russia.[17] The law introduces a piece of "technical equipment for counteracting threats," TSPU. This technology must be installed in the networks of internet providers at the government's expense and managed by Roskomnadzor, allowing the authority centralised blocking of undesired information.

Key Russian technology companies: Censorship and surveillance services

Russian state agencies' aspiration to control information has its roots in the early age of the internet's development in Russia. However, a vibrant development of the ICT (information and communications technologies) market in the 1990s, numerous private Internet Service Providers (ISPs) across the country and market participation by international companies established a diverse digital ecosystem in Russia. Under these conditions, censorship was hindered by decentralised infrastructure and services, owned by various actors.

Still, Russia's Federal Security Service (FSB) has gained access to a vast amount of information through the notorious surveillance system SORM. SORM stands for "System for Operative Investigative Activities" (*sistema operativno-rozysknykh meropriiatii*) and is designed to mirror, store, and transmit messages, voice recordings, videos, and other user-generated content from ISPs to the FSB. The system was gradually expanded and modernized throughout the 1990s, adapting to the development of communication technologies and the internet. Nowadays, SORM allows the FSB to access nearly all information transmitted via telecommunications providers without the knowledge of users and ISPs themselves, and without a court-approved warrant. SORM's stated purpose is the lawful interception of communications with the aim of combating organised crime and terrorism. However, technology experts characterise SORM as the FSB's "backdoor" to Russia's internet.[18] X-Holding, along with Citadel, have become the major suppliers of SORM.

Over time, the Kremlin has reasserted authority through consolidation and regulation of the

12 President of Russia, *Speech and the Following Discussion at the Munich Conference on Security Policy*, 13 February 2007, http://en.kremlin.ru/events/president/transcripts/24034.

13 Roland Paris, "The Right to Dominate: How Old Ideas About Sovereignty Pose New Challenges for World Order," *International Organization* 74, No 3 (2020): 453–89, https://doi.org/10.1017/S0020818320000077.

14 "Sergei Zhelezniak: My dolzhny obespechyt 'tsyfrovoi suverenitet' nashei strany", *Parlamentskaia gazeta*, 19 June 2013, https://www.pnp.ru/social/2013/06/19/sergey-zheleznyak-my-dolzhny-obespechit-cifrovoy-suverenitet-nashey-strany.html.

15 Michał Czerniawski, "EU's Digital Sovereignty and the Rights-Based Imperative," *Verfassungsblog*, 3 December 2025, https://doi.org/10.17176/20251204-172143-0.

16 Johannes Thumfart, "Digital Sovereignty in China, Russia, and India: From NWICO to SCO and BRICS," in *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*, ed. Luca Belli and Min Jiang (Cambridge University Press, 2025), 56.

17 Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law,'" *DGAP Analysis No 2*, 16 January 2020, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

18 Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's Back Door onto the Internet – Extract," *The Guardian*, 8 September 2015, https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

telecommunications sector, ISP networks, and online services. Several Russian technology companies have become key instruments in this approach.

There are more than 10,500 companies that provide mobile and broadband internet services in Russia, but market concentration under Putin has increased dramatically.[19] Four companies, namely Rostelecom, MobileTeleSystems (MTS), VimpelCom, and ER-Telecom account for 67 per cent of the broadband market in Russia.[20] The market for mobile communications services in Russia is divided between four major firms: Rostelecom, MTS, VimpelCom, and MegaFon. Together they hold over 95 per cent of the market.[21]

This consolidation is accompanied by direct state control or indirect control through loyal owners and managers. For example, Rostelecom is effectively state-controlled via the Federal Agency for State Property Management, while Kremlin-adjacent oligarchs such as Vladimir Evtushenkov and Alisher Usmanov control major tech assets of MTS and MegaFon through AFK Sistema and USM Holdings, respectively.

Yet, this direct oversight proved insufficient in preventing dissemination of undesired information in society, as the initial so-called blacklist of prohibited websites in Russia did not result in effective blocking.[22] Deep Packet Inspection (DPI) technology used by providers was inconsistent and in some places was not installed at all, so all blocking was done by IP address only. This made it impossible to block entire services; it allowed blocking only of individual websites. After attempting to block Telegram in 2018, Roskomnadzor realised that it needed a more modern system, one that could block by protocol, not just by IP address. Hence, the state moved to a system of direct technical control of the internet and installed the aforementioned TSPU on the majority of the ISPs' networks in Russia.

Two Russian companies provide the backbone for this system: servers for online content filtering and TSPU hardware come from Yadro, while RDP.ru develops software. RDP.ru was gradually acquired by Rostelecom between 2016 and 2021.[23] Yadro is Russia's leading manufacturer of data processing and storage systems, as well as telecommunications and network equipment and is reported to be affiliated with Alisher Usmanov and the X-Holding group, the same group that provides SORM.[24]

The application layer of the internet in Russia is becoming centralised as well. The state has encouraged people to switch to national social networks, while creating obstacles for foreign platforms. The main beneficiary of this policy is the Russian firm, VK Company.[25] Initially a private firm that focused on email services, VK Company has gradually become controlled by the state through three companies: the insurance company Sogaz; Gazprom Media Holding, which is Russia's largest media holding; and Rostec, a state-owned military conglomerate. The oversight of the company is through a friend of Vladimir Putin, Yurii Kovalchuk, who is a significant shareholder of Sogaz, as well as through the CEO of VK, Vladimir Kiriyenko, the son of Sergei Kiriyenko, who is first deputy chief of the Presidential Administration.

In recent years, VK Company has consolidated major services into one ecosystem, replacing foreign services, such as YouTube. One of the key services of the company is VKontakte, the largest social network in Russia with around 50 million daily users. Additionally, VK owns Odnoklassniki (OK.ru)– a popular social network with around 21 million daily users. With both networks, the company harvests an enormous amount of data from their users that can be passed to the authorities and security services.

Both social media platforms are listed in the register of "organisers of information dissemination" (*organizator rasprostraneniia informatsii, ORI*). According to the Law on Information Technologies and Information Protection of 2014, any person or legal entity who owns a website on which users can leave comments and reviews

19 Maria Kolomychenko, "The Impact and Limits of Sanctions on Russia's Telecoms Industry," *DGAP Analysis No 3*, March 2024, https://dgap.org/en/research/publications/impact-and-limits-sanctions-russias-telecoms-industry.

20 Anastasiia Gavryliuk, "Schastlivo ostavatsia na sviazi: spros na podkliuchenie domashnego interneta vyros na 20%", *Forbes.ru*, 11 August 2025, https://www.forbes.ru/tekhnologii/543601-scastlivo-ostavat-sa-na-svazi-spros-na-podklucenie-domasnego-interneta-vyros-na-20.

21 "Obzor industrii telekomov v Rossii. Chast 1", *T-Bank*, 18 February 2025, https://www.tbank.ru/invest/social/profile/T-Investments/15b8f670-8d28-4993-9973-0a54f89e981b/.

22 The law on 'blacklists' was originally introduced in 2012 and then expanded.

23 Dada Lyndell et al., "Putin's Digital Iron Curtain: Russia Bypasses Sanctions, Buys Equipment to Block YouTube and Telegram," *The Insider*, 10 October 2023, https://theins.ru/en/politics/265749.

24 Andrey Zayakin, "Sovereign Cyberpunk: Despite Sanctions, Western Components Are Still Being Used to Build Russia's Cyberwar Machine," *The Insider*, 8 January 2025, https://theins.press/en/inv/277733.

25 Philipp Dietrich, "The Key Player in Russia's Cybersphere," *DGAP Analysis No 4*, September 2023, https://dgap.org/en/research/publications/key-player-russias-cybersphere.

or chat in forums or chat rooms can be included in this register.[26] The law obliges ORIs to store a range of information about users in Russia; metadata must be stored for one year, and users' chat messages for six months. Above all, the ORIs must hand over the data to state agencies such as the FSB upon request and decrypt electronic messages if they are encrypted. Roskomsvoboda, a digital rights NGO (nongovernmental organisation), estimates that over 419 ORIs are listed in this register.[27]

Additionally, VK has developed the application "Max." Max is intended to become the main state messenger in Russia, following Vladimir Putin's signing of a decree "on a multifunctional information exchange service" and the authorities' aggressive promotion of the app, including administrative pressure on schools, universities, and public institutions to install it.[28] Moreover, from 1 September 2025, Max must be preinstalled on all new smartphones sold in Russia. To force people in Russia to switch to the state messenger, Roskomnadzor has been blocking voice and video calls on WhatsApp and Telegram, the most popular messengers in the country.

Although there is no confirmed evidence of built-in surveillance of users,[29] the messenger Max is designed in a way that enables third parties and security services to access users' data: the messenger does not provide end-to-end encryption, and all information and correspondence are stored on servers in Russia.

Another Russian tech giant, Yandex, was once the flagship company of Russian innovation. But state control of the domestic IT market and the full-scale invasion of Ukraine have put significant pressure on it. The company's market capitalisation collapsed, stock trading was halted, and Western sanctions hit Yandex's top management, as well as its projects on emerging technologies.[30] In the summer of 2022, two flagship services, Yandex Dzen and Yandex News, were sold to VK Company and became part of its ecosystem. As both relied heavily on traffic from Yandex.ru, Russia's largest search engine, the homepage was included in the sale to ensure their continued visibility and user reach.

Finally, in February 2024, Yandex was split into two companies: a Russia-based firm including maps, taxi, and food delivery services and a Dutch-based firm focusing on emerging technologies for the international market. The Russian business was transferred to a consortium of Russian investors with close ties to the Kremlin, while the Dutch Yandex N.V. remained with its founder Arkady Volozh abroad, was renamed Nebius, and resumed trading on NASDAQ, thereby completing the integration of the Russia-based Yandex services into the state's surveillance system, making it easier for authorities to access citizens' data.[31]

This consolidation of technology companies and services has become decisive since Putin started the full-scale invasion of Ukraine on 24 February 2022. Roskomnadzor started to block and restrict access to foreign platforms to prevent dissemination of independent reporting about Russia's cruelties in Ukraine: Facebook, Instagram, and finally YouTube have become almost unavailable to people in Russia.[32] This, in turn, sparked a high demand for VPNs (virtual private networks) among Russian internet users to circumvent censorship.[33] Roskomnadzor's next target is therefore VPNs, expanding the block to tools that allow access to the blocked websites and services.

As the war persists, state control over digital connectivity has progressively intensified, justified by newly declared "threats," and has culminated in widespread internet shutdowns. One of the latest threats cited by authorities involves Ukrainian drones operating through mobile networks. Under the pretext of countering these attacks and "to ensure the safety of Russian citizens," the government has increasingly imposed mobile internet blackouts, effectively cutting off large segments of the population from online access. Since the summer

26 Russian Federation, *Federal Law On Amendments to the Federal Law On Information* 05.05.2014 N 97-FZ, https://www.consultant.ru/document/cons_doc_LAW_162586/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100010.

27 Monitoring of registry, accessed 17 December 2025, https://blockedin.org/en/.

28 "Prinuzhdenie k MAXu. Kak v Rossii vsekh perevodiat v gosudarstvennyi messendzher", *Sever.Realii,* 16 December 2025, https://www.severreal.org/a/prinuzhdenie-k-maxu-kak-v-rossii-vseh-perevodyat-v-gosudarstvennyy-messendzher-/33612662.html.

29 RKS Global, "Testing for Surveillance in MAX on Android and iPhone," https://rks.global/en/research/max.

30 Anna Ustinova et al., "Nekhvatka chipov Nvidia mozhet zatormozit proekty 'Yandeksa' po bespilotnikam i II", *Vedomosti*, 6 February 2023, https://www.vedomosti.ru/technology/articles/2023/02/06/961756-nehvatka-chipov-nvidia-mozhet-zatormozit-proekti-yandeksa.

31 Peter Mironenko, "Yandex: The End of an Era for Russia's Most Innovative Firm," *The Bell,* 12 February 2024, https://en.thebell.io/yandex-the-end-of-an-era-for-russias-most-innovative-firm/.

32 Alena Epifanova, "Throttling of YouTube Shows That Russia Is Getting Better at Online Censorship," *Carnegie Endowment for International Peace*, 12 February 2025, https://carnegieendowment.org/russia-eurasia/politika/2025/02/russia-youtube-block-attempt?lang=en.

33 Daria Talanova, "Russia Leads Globally in VPN Service Expansion despite Government Crackdown," *Novaya Gazeta Europe*, 18 May 2023, https://novayagazeta.eu/articles/2023/05/18/russia-leads-globally-in-vpn-service-expansion-despite-government-crackdown-en.

of 2025, such measures have become normalised and geographically widespread, affecting most of the country, with disruptions reported in 58 regions.[34]

This radical intervention in connectivity across the country has become possible due to domestic technology companies, which help maintain access to essential services during shutdowns and thereby mitigate the risk of public backlash. Yandex and VK's services, including Max, along with the e-government portal Gosuslugi, Russian Post, major online marketplaces, and several state-controlled media outlets form a so-called "whitelist" of state-approved websites and services that remain accessible during internet shutdowns.[35] The introduction of such whitelists has been documented in 64 regions, and their number continues to grow. This approach is supposed to simulate the continuity of everyday life while simultaneously steering society into state-controlled digital ecosystems, effectively excluding any sources deemed to represent "foreign influence."

Exporting digital authoritarianism beyond Russia

Russia's efforts to expand its digital authoritarian model abroad are hard to trace due to opaque ownership structures of the involved companies and participation of shell firms and proxies. Still, investigative journalists and researchers have revealed several cases that exemplify the spread of Russian surveillance technologies to other countries with the help of key tech giants.

Since 2014, the company Miranda Media has played a central role in extending Russian telecommunications infrastructure into occupied territories first in Crimea and, in 2022, to parts of southern Ukraine. Originally established in 2004, Miranda was activated by its then-owner Rostelecom shortly after Russia's annexation of Crimea to build and operate network infrastructure. In 2015, Rostelecom divested 80.001 per cent of Miranda's shares to a group of inhouse managers, likely to shield itself from international sanctions.[36] Still, Rostelecom has remained closely connected to Miranda Media through operational ties, including zero-interest loans and infrastructure sharing.[37]

Miranda has since been implicated in surveillance and censorship in Crimea, operating SORM and internet filtering equipment. Its activities expanded further following Russia's invasion of southern Ukraine, with evidence indicating it has rerouted internet traffic from occupied Kherson through its networks.[38] In 2023–2024, Miranda Media launched telecom services in Russian-occupied parts of other Ukrainian regions, Donetsk[39] and Luhansk.[40]

Another Russian company, K-Telecom, has significantly contributed to a "digital annexation" of Ukraine and established a state-controlled telecommunications system. Nominally independent, K-Telecom has maintained deep ties to AFK Sistema-owned MTS.[41] K-Telecom began providing mobile services in Crimea shortly after Russia's annexation in 2014, following the handover of MTS Ukraine's frequencies.[42] Investigations reveal that MTS was involved in K-Telecom's establishment, asset transfers, and ongoing operations, often through opaque ownership structures in Armenia. After the full-scale invasion of Ukraine in 2022, K-Telecom, similarly to Miranda Media, expanded into occupied Kherson and Zaporizhzhia. In 2024, +7Telecom, a brand under K-Telecom, started to provide telecommunications services in occupied Luhansk.

Beyond Ukraine, Russian technology companies such as Citadel, MFI Soft (Citadel's subsidiary), and Protei play a crucial role in exporting SORM to Central

34 Monitor Runeta, "Ogranicheniia sviazi 16 dekabria", Telegram, 17 December 2025, 12:37, https://t.me/monitor_runet/198.

35 Maria Kolomychenko, "How Far Will the Kremlin Take Its Internet Crackdown?," *Carnegie Endowment for International Peace*, 16 December 2025, https://carnegieendowment.org/russia-eurasia/politika/2025/12/russia-internet-restrictions?lang=en.

36 Rostelecom stated publicly that the divestment was a routine management buy-out. However, a more plausible explanation is that Rostelecom reduced its shareholding to mitigate exposure to sanctions, which had been expanded to Russian state-owned enterprises and the telecommunications sector. The company reduced its shareholding in Miranda to just below 20 per cent, i.e., under the threshold that defines a controlling party under Russian law.

37 Andrei Fedoseev, "Rostelekom soedinitsia s Mirandoi-Media", 2 April 2015, https://www.comnews.ru/content/90940/2015-04-02/rostelekom-soedinitsya-s-mirandoy-media.

38 Ksenia Ermoshina, "'Voices from the Island': Informational Annexation of Crimea and Transformations of Journalistic Practices," *Journalism* 25, no 3 (2024): 528–46, 529, https://doi.org/10.1177/14648849231152359.

39 Anna Ustinova, "'Miranda-media' ofitsialno zarabotala v DNR", *Vedomosti*, 4 May 2023, https://www.vedomosti.ru/technology/articles/2023/05/04/973685-miranda-media-ofitsialno-zarabotala-v-dnr.

40 "Iz LNR poidet trafik", *Kommersant*, 18 January 2024, https://www.kommersant.ru/doc/6455439.

41 "Ukraine: Mobile Network Faces 'Crimean Freeze-Out,'" *BBC News*, 6 August 2014, https://www.bbc.com/news/blogs-news-from-elsewhere-28677323.

42 Oleg Salmanov, "MTS iz Kryma ushla, no delo ee zhivet", *Vedomosti*, 5 April 2016, https://www.vedomosti.ru/technology/articles/2016/04/06/636599-mts-krima.

Asia, Eastern Europe, Africa, Latin America, and the Middle East, expanding their global presence and most likely facilitating access to these systems for Russian intelligence services.

As in Russia, telecommunications operators in Kazakhstan, Kyrgyzstan, Uzbekistan,[43] and Belarus are obliged to install SORM-compliant technology by law or decree, opening the countries' markets to Russian companies. While official information about the market share and the scope of SORM coverage remains opaque and largely inaccessible to the public, investigative reports and threat intelligence assessments indicate that Citadel, MFI Soft, Protei, and VAS Experts are among the principal SORM suppliers to several telecom operators in the Central Asian countries, as well as in Belarus.[44]

Several of Protei's customers have been identified far beyond the post-Soviet countries and include Ariantel (Iran),[45] Comores Telecom (Comoros), ETECSA (Cuba), Safaricom (Kenya), Niger Telecoms (Niger), Tunisie Télécom (Tunisia), and Umniah (Jordan).[46] A recent hack of Protei's web server, involving around 182 gigabytes of files, revealed data on the SORM provider operating in Bahrain, Italy, Mexico, Pakistan, and much of Central Africa, among other locations.[47] In Latin America, Protei's surveillance technology was traced in Venezuela, Nicaragua, and Cuba.[48]

Apart from telecom infrastructure and surveillance equipment, Russia has been gradually expanding its national social media platforms and online services through its major technology companies, VK and Yandex. However, the role of VK Company and its services abroad remains rather limited. Its social media platforms VK and Odnoklassniki are used in former Soviet republics such as Belarus, Kazakhstan, and Armenia as well as among Russian-speaking communities in Germany and the United States.

Yet, the bulk of traffic using these social media platforms is Russia-based (see Table 1), while traffic from abroad accounts for single-digit percentages.

Table 1. Russian social media traffic distribution: Russia and top traffic sources, November 2025 (mobile and desktop, %)

	vk.ru	ok.ru
Russia	90.05	78.24
Belarus	2.13	3.68
Germany	0.86	1.77
Kazakhstan	0.85	2.28
Armenia	0.54	0.29
US	0.54	1.52

Source: Based of data of Similarweb.com.

While the scope of Russia's information control abroad via VK Company remains limited, its surveillance capabilities are bolstered by Yandex services, which are more popular than VK across several countries. In a global context, Yandex ranks as the third-largest search engine, but its market share remains around two per cent.[49] Yet, it has a significant presence in specific countries: apart from its dominant market in Russia, Yandex search has strong positions in Turkey, Central Asia, and Belarus.

Another of Yandex's services is even more popular abroad: its taxi service (under the brand Yandex Go) dominates Central Asia, controlling around 90 per cent of the taxi markets in Kazakhstan and Uzbekistan.[50] In 2024, Kyrgyzstan's Antimonopoly Regulation designated

43 Dylan Welch, "Russia and China in Central Asia's Technology Stack," *The German Marshall Fund of the United States*, 5 June 2025, 22, https://www.gmfus.org/news/russia-and-china-central-asias-technology-stack.

44 Insikt Group®, "Unveiling Russian Surveillance Tech Expansion in Central Asia and Latin America," 7 January 2025, https://www.recordedfuture.com/research/tracking-deployment-russian-surveillance-technologies-central-asia-latin-america.

45 Gary Miller et al., "You Move, They Follow: Uncovering Iran's Mobile Legal Intercept System," *Citizen Lab, University of Toronto*, 16 January 2023, https://citizenlab.ca/2023/01/uncovering-irans-mobile-legal-intercept-system/.

46 Insikt Group®, "Unveiling Russian Surveillance Tech Expansion in Central Asia and Latin America,"

47 Zack Whittaker, "Surveillance Tech Provider Protei Was Hacked, Its Data Stolen, and Its Website Defaced," *TechCrunch*, 17 November 2025, https://techcrunch.com/2025/11/17/surveillance-tech-provider-protei-was-hacked-its-data-stolen-and-its-website-defaced/.

48 Doug Farah, "How Russian Surveillance Tech Is Reshaping Latin America," *Research Publications*, 27 September 2024, https://digitalcommons.fiu.edu/jgi_research/67.

49 StatCounter Global Stats, "Search Engine Market Share Worldwide," https://gs.statcounter.com/search-engine-market-share.

50 Azattyk Azia and Bolot Kolbaev, "Ne prosto taksi. Kak Yandex zanial rynok izvoza y dostavki v Tsentralnoi Azii, no ne ves", *Radyo Azattyk*, 19 February 2025, https://rus.azattyk.org/a/ne-prosto-taksi-kak-yandeks-zanyal-rynok-izvoza-i-dostavki-v-tsentralnoy-azii-no-ne-ves/33318959.html.

Table 2. Yandex search market share in November 2025 (%)

	Yandex search
Russia	73.75
Turkey	50.93
Belarus	33.47
Kazakhstan	32.47
Uzbekistan	26.73
Kyrgyzstan	16.00

Source: Based on data of StatCounter Global Stats.

Yandex Taxi a monopoly,[51] as it effectively suppressed all competitors in the capital and several regions, holding up to 70 per cent of the cab market in the country. Yandex Taxi also operates in Israel, Norway, Finland, and several other countries. Most rides are arranged through the Yandex app, and the data generated is stored on servers within Russia, which poses a significant risk for its users. From 1 September 2023, new legislation granted the Russian FSB full access to data about cab rides facilitated by Yandex services. This data includes the user's name, phone number, e-mail address, banking information, user comments, and trip addresses. Media reports indicate that there is no separation between domestic and international user data in Yandex's Russian databases.[52] While Yandex has denied that the FSB has access to customer data from abroad, it remains unclear how such access could be technically prevented.

Conclusions

Russia's concept of a "sovereign internet" should be discussed within Vladimir Putin's broader notion of "sovereignty" and his challenge to the liberal international order. By exploiting a permanent narrative of threat, the Russian state apparatus, together with domestic technology companies, has built an increasingly centralised system of information control. While the system does not fully isolate Russia from the global internet and foreign services remain accessible via VPNs, censorship and surveillance have expanded significantly.

A number of prominent Russian technology companies play a central role in developing this infrastructure domestically and exporting digital control systems abroad, though further research is needed to capture the full scope of actors involved and assess the related risks.

These companies provide complementary technologies ranging from telecommunications infrastructure and surveillance hardware to content-blocking systems, social media platforms, and mobility services. These technologies are designed to grant Russian security services access to user data, enabling extensive monitoring of communications. Contrary to its name, the "sovereign internet" reduces individual and national autonomy by creating dependencies on Russian providers and exposing foreign users' data to potential exploitation, thereby expanding Russia's intelligence-gathering capacity.

Although the market for SORM and other hardware-based surveillance systems is opaque, available evidence points to a significant presence of Russian SORM suppliers across multiple regions, especially in Central Asia and Belarus, opening access to data in these countries for the FSB. Additionally, Yandex has gained significant popularity in several countries through its search and taxi services, potentially creating surveillance risks. By contrast, the international reach of Russian social media platforms remains limited, largely confined to Russian-speaking populations. However, in non-democratic countries aiming to suppress free access to information, Russian social networks may emerge as attractive alternatives. ■

Alena Epifanova is a research fellow at the German Council on Foreign Relations (DGAP) in Berlin, exploring digital authoritarianism, internet governance, international order, and democracy.

This FOI Memo builds on a paper presented in a joint panel "Russian Strategy in the Information Spacen" at the XI ICCEES World Congress, London, 25 July 2025. The author wishes to thank Carolina Vendil Pallin and Emil Wannheden for review and valuable comments in support of this FOI Memo.

51 "Yandex Taksi v Kyrgyzstane vnesli v spisok monopolistov", *Radyo Azattyk,* 4 April 2024, https://rus.azattyk.org/a/32890706.html.

52 Svetlana Reiter, Denis Dmitriev, and Jussi Konttinen, "Sovsem skoro FSB poluchit kruglosutochnii dostup k dannim servisa Yandex po zakazu taksi", *Meduza*, 8 August 2023, https://meduza.io/feature/2023/08/08/sovsem-skoro-fsb-poluchit-kruglosutochnyy-dostup-k-dannym-servisa-yandeksa-po-zakazu-taksi-kak-vyyasnila-meduza-v-tom-chisle-k-poezdkam-za-predelami-rossii.