Issue Brief
July 6, 2026

The Slow Death of the Russian Internet: How Russia Is Reshaping Its Digital Infrastructure

Christopher Peterstam

Photo credit: Coffeemill / Shutterstock.com

The ongoing internet restrictions in Russia have been unprecedented in scope. Never before has a country with a previously free and open internet environment attempted to build domestic barriers to block external influence by using such aggressive tactics. Through the passing of legislation, the installation of monitoring devices, and the buildup of a domestic digital services ecosystem, Russia appears to be attempting to sever itself from the global internet system, of which it has been a part since its inception. The ramifications of this effort have been reverberating across the Russian public and economy, with daily disruptions to everyday life occurring in major cities across the country. This has led to public discontent among both citizens and government officials, a phenomenon that would have been nearly unimaginable in post-2022 Russia.

Introduction

Since the beginning of the 2022 invasion of Ukraine, Russia has been gradually purging its internal digital infrastructure of foreign information platforms that it has been unable to coerce or control. Although these measures became more visible after the invasion, evidence indicates that the Russian state has been laying the groundwork for a major digital crackdown for several years before the invasion.

With early indications of state censorship emerging in the mid-2010s, this gradual encroachment was hidden by vague rhetoric and the continued allowance of foreign companies to operate, albeit with increasing rules and stipulations. Domestic internet restrictions were first documented along Russia's peripheral regions, with early experimentation with internet shutdowns occurring in the North Caucasus during periods of regional unrest. However, internet restrictions have now spread to the populated hubs in Russia's heartland that are the economic heart of the country. Urban Russians previously relatively untouched by the effects of the war in Ukraine and state restrictions have

now come under unprecedented state interference affecting their daily lives.

Compounding these problems is the Kremlin's decision to shut down widely used media platforms, the latest of which is the hugely popular Telegram messaging app. With over 100 million Russian users, Telegram is by far the most popular messaging and social media platform in Russia. The new restrictions do not solely target Telegram but are meant to isolate Russians from utilizing any kind of outside media. Thus, Virtual Private Networks (VPNs) are now being targeted in an effort to fully prevent external influences from entering the Russian media ecosystem.

The Pre-2022 Russian Internet Sphere

The Russian internet sector was created in a society that, while experiencing democratic backsliding, was relatively free. The internet, being a novel and new technology, was largely spared the regulation and state control imposed on traditional Russian media. This status quo remained until 2012. It was then that the Unified Register of Prohibited Websites was created by Roskomnadzor, the Russian communications regulator. Initially, this development was not widely viewed as cause for concern, as it mainly targeted websites with references to drugs, pornography, and suicide. However, in 2014 the so-called 'Lugovoy Law', a landmark anti-sanction legislation that allowed Russian companies to sue international entities in Russian courts, was passed, allowing certain websites deemed to contain 'extremist material' to be banned.[1] This amendment caused controversy because the definition of extremism was left intentionally vague and was often used to suppress what authorities considered unlawful protests, many of which were associated with opposition parties and figures.

> ***Following Russia's 2022 invasion of Ukraine, the true test of Russia's censorship apparatus began. Within days, several Western platforms, including Instagram and Facebook, were blocked. However, YouTube remained accessible until 2024. It was never formally blocked, but during the summer of 2024 Russian authorities slowed down video buffering speeds, essentially rendering the platform unusable.***

Access to the digital sphere remained relatively robust during this period, with the state unable to fully assert control over its citizens' ability to view and contribute to digital platforms. However, Roskmonadzor continued to cement its control over the Russian digital sphere. In 2018, it successfully pressured YouTube to remove opposition leader Alexei Navalny's ads from its platform and persuaded Google to remove his website.

In 2019, the so-called 'Sovereign Internet Law, a set of amendments added to the 2006 Federal Law "On Information, Information Technologies and the Protection of Information," mandated that all mobile providers install 'black boxes' or monitoring equipment capable of tracking internet traffic and enabling authorities to slow down or disable specific websites. The first usage of this new system occurred in 2021 against Twitter. The platform was not shut down but simply slowed,

causing images and links to take several minutes to load. It was also at this time that major tech giants removed the Navalny protest-voting app from their respective app stores at the behest of Roskmonadzor.

Following Russia's 2022 invasion of Ukraine, the true test of Russia's censorship apparatus began. Within days, several Western platforms, including Instagram and Facebook, were blocked. However, YouTube remained accessible until 2024. It was never formally blocked, but during the summer of 2024 Russian authorities slowed down video buffering speeds, essentially rendering the platform unusable.

Domestic Internet Shutdowns

A worrying new trend within Russia has been the government's usage of localized internet shutdowns, rendering mobile data effectively obsolete. The first instances of widespread internet blackouts occurred in the North Caucasus region. In 2018, in Ingushetia, following a controversial border change with Chechnya, several pro-Ingush protests were organized, and a full mobile internet blackout occurred, disrupting protestors' ability to organize. Then, in October 2023, another blackout occurred in portions of Dagestan and Chechnya following an attempt by an angry mob to accost Israeli passengers at Makhachkala airport.[2] The Dagestani internet Provider, Ellko, claimed that the blackout was part of an exercise conducted in conjunction with Roskomnadzor to 'develop scenarios for disconnecting access to the foreign segment of the internet'. As these internet disruptions occurred on the periphery of the Russian Federation, few took note of the ramifications of these actions. The shutdowns in the North Caucasus can be seen as a testing ground for a more ambitious strategy later implemented in Russia's core regions.

The first documented internet shutdowns in Russia's heartland began in the spring of 2025. During this period, several regions began reporting mobile internet blockages. In fact, in 2025 Russia had the largest number of mobile internet shutdowns than in any previous year. At the beginning of 2026, both Moscow and St. Petersburg reported restricted mobile internet and cellular access for almost three weeks. Users reported that these restrictions were extremely localized, often changing in strength from street to street. The Russian government stated that the restrictions were intended to prevent Ukrainian drone strikes, which frequently made use of Russian mobile internet infrastructure during drone operations within Russia. Dmitry Peskov, Putin's spokesperson, stated on March 11 that "all recent connection and internet restrictions in Moscow were introduced in accordance with [Russia's] legal framework and aim at ensuring the safety of Russian citizens," adding that no timeframe could be provided for the removal of restrictions. Several other cities have also reported prolonged internet shutdowns, with Nizhny Novgorod reporting restrictions since May 2025.

"In 2025, Russia had the largest number of mobile internet shutdowns than in any previous year. Then, in early 2026, both Moscow and St. Petersburg reported restricted mobile internet and cellular access for almost three weeks. Users reported that these restrictions were extremely localized, often changing in strength from street to street.

The effects of these shutdowns have greatly hindered everyday life for ordinary Russians. According to reports, sales of walkie-talkies, analog telephone lines, paper maps, and MP3 players have risen in several Russian cities as residents seek ways to avoid disruption to daily life[3] should internet be switched off unannounced. It has even been reported that workers in the Kremlin have reverted to using landline phones to bolster internal security and maintain lines of communication should internet shut offs affect the Kremlin complex. Russian businesses have also been suffering: the newspaper *Kommersant* reported that Moscow's economy lost an estimated $36 million to $65 million during a five-day shut down period.[4]

The government has attempted to improve the situation by promoting domestic services that can be monitored more effectively by the state. In August 2025, the Ministry of Digital Development, Communications, and Mass Media introduced a 'whitelist' of companies that offered "all resources essential to everyday life," according to Minister Maksut Shadayev.[5] It has been theorized that the internet shutdowns, in addition to helping prevent Ukrainian drone strikes and testing state cyber capabilities, also serve as a testing ground to ensure that the 'whitelist' system can continue operating should additional restrictions become necessary in future. This list has been expanded several times as the Russian state has dedicated itself to creating a domestic digital infrastructure capable of replacing services once provided by foreign competitors. These services include food delivery apps, taxi services, banking, and online shopping. While it is not clear how exactly these companies were able to get themselves on the list, all must be registered in Russia, maintain infrastructure within Russia, and share user information with the Russian state.

> ***Compounding these problems is the Kremlin's decision to shut down widely used media platforms, the latest of which is the hugely popular Telegram messaging app. With over 100 million Russian users, Telegram is by far the most popular messaging and social media platform in Russia. The new restrictions do not solely target Telegram but are meant to isolate Russians from utilizing any kind of outside media.***

Significant anger has risen from both the general populace and from well-known political actors. Several requests to hold protests have been registered across Russia, although none have been granted, to voice concerns over growing censorship. The Governor of the Ukrainian-bordered Belgorod Oblast, which has experienced significant air raids during the war, warned that internet disruptions could lead to 'needless deaths' because internet connectivity plays a critical role in civilian warning systems.

The Kremlin vs. Telegram

The most dramatic and longstanding feud between the Russian government and a tech company has been the battle between the Kremlin and Telegram. The encrypted messaging app, led by entrepreneur Pavel Durov, has repeatedly refused requests from several governments to provide a mechanism for decrypting chats deemed to be

used by terrorist and/or criminal networks. This refusal led to Durov's arrest in Paris in August 2024 after he allegedly failed to comply with the Elysee's demand for access. French authorities cited complicity in the distribution of child exploitation material and drug trafficking.

The first salvo of attacks against Telegram began in 2018 when the Federal Security Service (FSB), Russia's domestic security apparatus, demanded that Telegram hand over encryption keys allowing authorities to access chats deemed to be used by extremist elements. Durov refused, prompting Roskomnadzor to block millions of internet protocol (IP) addresses in an attempt to intercept those used by Telegram. As a result, everything from supermarket digital scanning systems to ticket bookings, and even government websites failed, while Telegram continued to operate largely unimpeded. In 2020, because of the difficulties of stopping Telegram and the ongoing disruption to Russian digital services, the ban was lifted, and the authorities learned a valuable lesson: IP blocking was not a viable solution for shutting down the platform.

Telegram is now back in Moscow's sights, as, with over 100 million Russian users, it has been deemed a major threat to the Kremlin's centralized information hegemony. Beginning in early 2026, Roskomandzor once again targeted Telegram. In February, officials claimed that the platform had violated Russian law by failing to protect its users' personal data, stop fraud, and prevent its use by terrorists and criminals.[6] As with other platforms the Kremlin wished to marginalize, the authorities responded by throttling Telegram's service to discourage its use.

Significant pushback was seen from all levels of society. Within Russia's parliament, known for 'rubber stamping' nearly all legislation put before it, there was dissent over the ban. Due to Telegram being an essential tool for Russian soldiers coordinating operations in Ukraine, Sergei M. Mironov, the leader of the party A Just Russia and a supporter of the war, stated that Telegram was the "only reliable means of communication [between Russian soldiers]…What are you doing, you idiots?"[7]

> ***"The Russian state has also recognized the risk Virtual Private Networks or VPNs pose to its information sector and has begun instructing private companies to prevent their users from accessing these services. By mid-January 2026, it was reported that Russia had blocked over 400 VPNs, representing a 70 percent increase since autumn 2025.***

This dissent extended into the Duma, Russia's parliament, where in a rare display of opposition, 77 deputies voted in favor of a motion demanding that federal authorities appear before parliament to explain the measure. Although the motion failed, it demonstrated the influence and importance of Telegram within Russian society. This opposition has gone unacknowledged by Putin, who still maintains the need to 'strangle' foreign tech firms.

The contradictions in the Kremlin's position were highlighted in a meeting between Putin and a Russian military officer, When Putin asked the officer about the danger of using foreign information systems, the officer replied that they were extremely dangerous and even

claimed that Telegram was an "enemy form of communication". Russian journalists later reported that the same officer had a premium Telegram account.[8]

The opposition did not have any major effect and on April 10 a nationwide ban on the platform came into effect. Users reported that access to Telegram without the use of a VPN became all but impossible.[9] While Telegram has become the latest victim of Russia's online censorship, many other platforms, such as South Korea's KakaoTalk, Turkey's BiP, and even China's WeChat, have seen a rise in user usage within Russia.

The War on VPNs

Virtual Private Networks (VPNs) have long allowed the Russian population to circumvent state censorship and access foreign media platforms. VPNs operate by encrypting internet traffic and routing connections through secure remote servers, allowing users to bypass national systems and appear as though they are accessing the internet from outside their own country.[10]

> ***Concerns have grown over the risks of fully adopting MAX, the new messaging app being promoted by the Russian state, due to privacy concerns. As Russian legislation already requires companies to store and, if needed, share sensitive private data with the state, many users have developed tactics, such as maintaining multiple devices with different messaging platforms on each, to evade state control.***

However, the Russian state has recognized the risk VPNs pose to its information sector and has begun instructing private companies to prevent their users from accessing these services.[11] By mid-January 2026, it was reported that Russia had blocked over 400 VPNs, representing a 70 percent increase since autumn 2025.[12] Authorities issued a list of banned VPNs to Russian telecommunication companies, as well as a guide on how to identify and block them. These businesses were also required to report any new VPN activity to Roskomnadzor. Failure to comply could lead to the loss of their IT accreditation, tax benefits, and, most dangerously, removal from the state's whitelist.

Experts point out that these measures could further hinder the Russian telecommunication industry. With no international competition or viable alternatives, Russian telecommunication companies risk becoming complacent in their protected market, potentially reducing efficiency and creating a system in which user choice is eliminated. For the corporate sector, however, the state must exercise considerable care in identifying which VPNs to block. In attempting to limit the general public's access to VPNs, authorities risk inadvertently disrupting corporate VPNs that businesses rely on for secure communications, causing further trouble for the Russian economy.

The Rise of MAX

As nearly all previously popular messaging platforms in Russia have been, or are in the process of being rendered unusable, the state has been quick to offer the population a monitored alternative. This has given rise to the MAX

messaging app. Developed by VKontakte (VK), the Russian social networking company co-founded by Telegram founder Pavel Durov, MAX can be seen as a continuation of Russia's broader strategy of developing domestic alternatives across sectors including banking, social media networks, video hosting services, and cloud platforms. Across Russian society, from government institutions and schools to neighborhood chats, the government has been encouraging citizens to use MAX as their primary communication platform.

Concerns have grown across Russia over the risks of fully adopting MAX due to privacy concerns. As Russian legislation already requires companies to store and, if needed, share sensitive private data with the state, many users have developed tactics, such as maintaining multiple devices with different messaging platforms on each, to evade state control.

The Future

Russia's May 9, 2026, Victory Day Parade was emblematic of the security concerns the country continues to face. Usually an event full of pomp, this year's parade was notably subdued, with no armored vehicles, tanks, or missiles displayed through Red Square.[13] Reports indicated that anti-aircraft batteries had been redeployed from across Russia to form a defensive ring around Moscow, and internet shutdowns were reported before and during the event in central Moscow.

Indications point to Russia continuing to expand its internet restrictions, with the ultimate goal of creating a sovereign internet ecosystem that is domestically based and subservient to the state. Currently, the restrictions have been met with growing concern among citizens and political officials alike. One notable example was an eighteen-minute video posted by Russian social media influencer Victoria Bonya, who resides in Monaco, in which she criticized the internet blackouts while explicitly calling out President Putin.[14] In a rare public statement, the Kremlin acknowledged the ongoing challenges Russia was facing and stated that work was under way to address these issues. While large-scale protests are unlikely to break out, the disruption to daily life and the erosion of everyday conveniences are likely to add to a growing sense of war fatigue that will become increasingly difficult for the Kremlin to ignore.

Author –

Christopher Peterstam *is a Project Manager at ISDP's Asia Program. His work focuses on contemporary political and security developments across Asia, with particular attention to state narratives, regional power dynamics, and transnational issues. He contributes to the program's analytical output through research, writing, and engagement in ongoing projects.*

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

www.isdp.eu

Endnotes

1 Human Rights Watch, "Russia: Halt Orders to Block Online Media," March 24, 2014, https://www.hrw.org/news/2014/03/23/russia-halt-orders-block-online-media.

2 Elizaveta Chukharova, "As Russia Further Restricts the Internet, What Does the Future Hold for the North Caucasus?" OC Media, March 30, 2026, https://oc-media.org/as-russia-further-restricts-the-internet-what-does-the-future-hold-for-the-north-caucasus/.

3 Aisha Down, "Russia Slowly Trying to Splinter Its Internet from Rest of World, Analysts Say," *Guardian*, March 31, 2026, https://www.theguardian.com/world/2026/mar/31/russia-splinter-internet-blackouts-telegram-analysts.

4 Niko Vorobyov, "'My Phone Is a Brick': Russians Scramble for Information as Data Blocked," *Al Jazeera*, March 26, 2026, https://www.aljazeera.com/features/2026/3/26/my-phone-is-a-brick-russians-scramble-for-information-as-data-blocked.

5 Human Rights Watch, "Russia: Internet Shutdowns Escalate," March 31, 2026, https://www.hrw.org/news/2026/03/31/russia-internet-shutdowns-escalate.

6 Veronika Sukhanych, "Russia Introduces Full Telegram Ban Nationwide," *Kyiv Post*, April 10, 2026, https://www.kyivpost.com/post/73690.

7 Ekaterina Bodyagina, "A Superpower Goes Offline," Politico, March 14, 2026, https://www.politico.com/news/2026/03/14/russias-self-inflicted-communication-crisis-00827197.

8 Paul Sonne, Valerie Hopkins, and Oleg Matsnev, "Putin's Internet Blackout: A Chaotic Drive to Cut off Russians from the World," *New York Times*, March 31, 2026, https://www.nytimes.com/2026/03/31/world/europe/russia-putin-telegram-internet.html.

9 Veronika Sukhanych, n. 6.

10 "Russia's Digital Ministry Declares War on VPNs," *Moscow Times*, March 31, 2026, https://www.themoscowtimes.com/2026/03/31/russias-digital-ministry-declares-war-on-vpns-a92384.

11 Guy Faulconbridge, "Russia Goes after VPNs as 'Great Crackdown' Gathers Pace," *Reuters*, March 31, 2026, https://www.reuters.com/technology/russia-goes-after-vpns-great-crackdown-gathers-pace-2026-03-31/.

12 Chiara Castro "Russia Moves to 'Reduce VPN Usage' with New Blocking, Fines and Fees," TechRadar, March 31, 2026, https://www.techradar.com/vpn/vpn-privacy-security/russia-moves-to-reduce-vpn-usage-with-new-blocking-fines-and-fees.

13 Steve Rosenberg, "Rosenberg: Russia's Victory Day Parade with No Tanks a Sign Ukraine War Not Going to Plan," *BBC*, May 7, 2026, https://www.bbc.com/news/articles/cwy2gj2jlr8o.

14 Pjotr Sauer, "Russian Blogger's Fierce Critique of Kremlin Goes Viral: 'People Are Afraid of You,'" *Guardian*, April 18, 2026, https://www.theguardian.com/world/2026/apr/18/russian-blogger-fierce-kremlin-critique-goes-viral.