# ACCESS DENIED

## HOW THE KREMLIN CONTROLS THE INTERNET — AND HOW TO RESIST IT

ANTI-CORRUPTION FOUNDATION

Prepared by IT department

Март 2026

# Contents

# Introduction

Over the course of twenty-six years in power, **Vladimir Putin has systematically dismantled freedom of speech** and suppressed every form of horizontal self-organization among Russian citizens.

At the outset of his rule, he brought national television under state control. He subsequently destroyed the free press and, over the past fifteen years, has increasingly focused on the internet.

During this period, Russia's system of internet censorship has evolved from a relatively crude and inconsistent set of blocking mechanisms into a far more mature, **centrally managed, and technologically flexible model**.

This transformation is significant not only in technical terms, but also politically. The Russian state has gradually converted the internet from a space of relative freedom into an environment of managed access, where restrictions are imposed more quickly, more precisely, and more uniformly, while the actual mechanisms of censorship have become increasingly less visible to outside observers.

## Purpose of the Report

The purpose of this report is to **describe how Russia's system of internet restrictions has evolved**, why it became qualitatively more dangerous after the introduction of TSPU ("technical means to counter threats"), and what practical conclusions this creates for strategies aimed at circumventing internet restrictions.

The report provides historical context and proposes concrete solutions relevant today.

This report was prepared primarily to support major technology companies and other digital platforms seeking to protect their users by integrating anti-censorship and circumvention technologies into their applications.

## Scope and Sources

This memo is based on four categories of sources:

- public web reporting,
- academic literature,
- expert social and technical channels,
- internal ACF documents, expertise, and discussions.

# Executive Summary

Russia's internet blocking model has evolved from a relatively coarse system based on blacklist register, DNS (Domain Name System) interference, and IP blocking into a **distributed yet centrally managed deep packet inspection architecture built around TSPU** ("technical means to counter threats"), mandated by the 2019 Sovereign Internet law and now deployed nationwide across most providers.[1]

Rather than relying on a single national choke point like China's Great Firewall, Russia has developed **thousands of ISP-side enforcement points** — including choke-points deployed "next to eyeballs" at some data-centers and cross-border links — all operating under centralized state control.[2] This system gives Roskomnadzor (the censorship authority) significantly **finer-grained, faster, and more adaptive control over traffic**.

The failed attempt to block Telegram in 2018 marked a turning point. Roskomnadzor's earlier model, known as "Revizor", relied on provider-enforced but state-monitored IP-based blocking, as well as collateral pressure on infrastructure providers.[3] In practice, this approach proved unable to shut down a major service capable of hiding behind shared infrastructure and adapting quickly.[4] [5] Subsequent sources link the post-2018 policy shift to the deployment of TSPU under the Sovereign Internet framework.

The key implication is that a **centralized anti-censorship architecture** for any app operating in Russia would be expensive, fragile, and likely short-lived unless backed by constant protocol iteration, rapid endpoint rotation, and continuous field telemetry. Public reporting,[6] academic analysis,[7] and ACF operational data[8] all point to the same conclusion: once a circumvention method becomes uniform, visible, and widely reused, Russian censors typically identify and target it at the protocol, infrastructure, or distribution layer.

[1] Alena Epifanova, "Deciphering Russia's Sovereign Internet Law," German Council on Foreign Relations (DGAP), December 2019, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[2] Diwen Xue et al., "TSPU: Russia's Decentralized Censorship System," in *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22)* (New York: Association for Computing Machinery, 2022), 179–194, https://doi.org/10.1145/3517745.3561461.

[3] Ksenia Ermoshina and Francesca Musiani, "The Telegram Ban: How Censorship 'Made in Russia' Faces a Global Internet," *First Monday* 26, no. 5 (2021), https://doi.org/10.5210/fm.v26i5.11704.

[4] Dada Lyndell, Andrey Zayakin, and Mikhail Klimarev, "Putin's Digital Iron Curtain: Russia Bypasses Sanctions, Buys Equipment to Block YouTube and Telegram," *The Insider,* October 11, 2023, https://theins.ru/en/politics/265749.

[5] "No Country for Telegram: Russia Starts Second Attempt to Block One of Its Most Popular Messengers," *Mediazona*, February 10, 2026, https://en.zona.media/article/2026/02/10/telegram.

[6] "[Russia] Censor Has a New Method of Blocking #490," *Net4People BBS (GitHub),* https://github.com/net4people/bbs/issues/490 (accessed March 20, 2026).

[7] Xue et al., "TSPU: Russia's Decentralized Censorship System."

[8] Internal ACF documents.

**The most realistic strategy is therefore a hybrid approach:** maintain a small dedicated anti-censorship engineering function; measure real-world reachability primarily using product telemetry rather than a single external checker; avoid dependence on standard VPN protocols or static data-center ranges; and support a broader ecosystem of decentralized circumvention, rather than assuming that any single company can sustain a permanent centralized arms race.

This recommendation is grounded in several converging factors: Russia's current internet control architecture,[9] the declining effectiveness of standard VPN protocols,[10] field experience from opposition-linked projects,[11] and the recent introduction of "whitelist internet" testing in Moscow.[12]

[9] "The VLESS Protocol: How It Bypasses Censorship in Russia and Why It Works," *Habr*, February 17, 2026,
https://habr.com/en/articles/990144/.

[10] Human Rights Watch, "Russia: Digital Iron Curtain Falls on Internet Freedom Protection Day," March 12, 2026, https://www.hrw.org/news/2026/03/12/russia-digital-iron-curtain-falls-on-internet-freedom-protection-day

[11] Internal ACF documents.

[12] Tim Zadorozhnyy, "Moscow Citizens Turn to Pagers, Printed Maps," *The Kyiv Independent*, March 14, 2026, https://kyivindependent.com/moscow-citizens-turn-to-pagers-printed-maps/.

# Internet Blocking Before TSPU

## Brief Timeline Before TSPU

Russia's early internet blocking regime combined centralized legal authority with uneven technical enforcement. In 2012, Russia introduced a national blacklist system[13] under which Roskomnadzor maintained a unified registry of prohibited sites, and ISPs (internet service provider) were required to block listed resources.[14]

In 2015, Rozkomandzor started to implement a system known as "Revizor".[15] It worked as a simple sensor that checked whether ISPs were blocking websites on the national blacklist. If a site remained accessible, a fine was issued **automatically against the responsible** ISP.[16] This system remains in place today as a backup tool if the TSPU unit fails and needs to be bypassed.

In 2016, the Yarovaya law dramatically expanded **surveillance and compliance pressure by requiring telecom and internet companies** to retain metadata and provide information necessary for decryption on demand.[17] That law did not itself lead to the creation of TSPU, but it increased the state's leverage over network and platform operators and normalized infrastructure-level intervention in communications.[18]

In 2018, Roskomnadzor attempted to block Telegram using the existing model: legal orders, registry-based enforcement, and broad IP blocking.[19] The campaign became famous for its **large-scale collateral damage** — affecting Microsoft Store, PlayStation Network, and other major services, especially those relying on Amazon Web Services — while failing to take down Telegram.[20] This failure was widely regarded as a major catalyst for the subsequent development of the much more ambitious Sovereign Internet architecture.

[13] "Amendments to the Law on Protecting Children from Information Harmful to Their Health and Development," *Kremlin.ru,* July 31, 2012, http://en.kremlin.ru/events/president/news/16095.

[14] "Russia Internet Blacklist Law Takes Effect," *BBC News*, November 1, 2012, https://www.bbc.com/news/technology-20096274.

[15] "Revizor — Website Blocking Control System in Russia" (Ревизор — система контроля блокировки сайтов в России), *TAdviser*, https://www.tadviser.ru/index.php/Продукт:Ревизор_-_система_контроля_блокировки_сайтов_в_России.

[16] "Let's Count 'Revizor' Agents" (Сосчитаем агентов «Ревизор»), *Habr*, May 6, 2019, https://habr.com/en/articles/450362/ (accessed March 20, 2026).

[17] Danny O'Brien and Eva Galperin, "Russia Asks for the Impossible With Its New Surveillance Laws," *Electronic Frontier Foundation (EFF),* July 19, 2016, https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

[18] Human Rights Watch, "Russia: 'Big Brother' Law Harms Security, Rights — Repeal Rushed Counter-terrorism Legislation," news release, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

[19] Lyndell, Zayakin, and Klimarev, "Putin's Digital Iron Curtain."

[20] Ermoshina and Musiani, "The Telegram Ban."

In November 2019, the Sovereign Internet law gave Roskomnadzor the legal basis to require operators to install TSPU and **created the framework for centralized management of telecom networks**, a national DNS layer, and more direct state control over routing and filtering.[21]

A visible transition moment came in March 2021, when Russia **throttled Twitter in a coordinated way that researchers later linked to TSPU**.[22] By this point, the TSPU had finally been installed. This time the state demonstrated its ability to implement selective throttling at scale, rather than relying solely on blunt blocking via registries and ISP-level improvisation.

Following the start of the full-scale war in 2022, Russia's censorship regime has shifted from selective throttling to wartime, **system-wide suppression: the authorities blocked or restricted major foreign platforms** (YouTube, Facebook, Instagram, etc.),[23] expanded pressure on app stores and hosting providers, and used TSPU-backed TLS (Transport Layer Security) interference, making internet restrictions far more uniform across networks than in the pre-war period.[24]

In 2024, OONI confirmed the blocking of at least **279 news-media domains** in Russia,[25] while Human Rights Watch documented sustained throttling of services such as YouTube and a broader state push to isolate the internet in Russia both legally and technically.[26]

YouTube video stream addresses were eventually blocked, and on some Russian DNS servers the youtube.com domain became completely inaccessible.[27]

In 2025-2026, the crackdown intensified further: Roskomnadzor moved against VPNs at scale, restricted Telegram and WhatsApp calls in August 2025, **confirmed hundreds of restrictions against VPNs** (Virtual Private Network Provider) by early 2026, and then began imposing direct restrictions on Telegram itself.[28] At the same time, the authorities expanded testing of **"whitelist internet"** access models from war-affected regions to Moscow.

[21] Epifanova, "Deciphering Russia's Sovereign Internet Law."

[22] Diwen Xue et al., "Throttling Twitter: An Emerging Censorship Technique in Russia," https://doi.org/10.1145/3487552.3487858.

[23] Human Rights Watch, *Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia* (New York: Human Rights Watch, July 30, 2025), https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation.

[24] RKS Global, Elizaveta Yachmeneva, Maria Xynou, Mehul Gulati, and Arturo Filastò, *Censorship Chronicles: The Systematic Suppression of Independent Media in Russia, OONI,* December 9, 2024, https://ooni.org/post/2024-russia-report/.

[25] Human Rights Watch, *Disrupted, Throttled, and Blocked.*

[26] RKS Global et al., *Censorship Chronicles.*

[27] Alexey Strelnikov, "YouTube, WhatsApp Blocked in Russia," *Deutsche Welle (DW),* February 12, 2026, https://www.dw.com/en/youtube-whatsapp-blocked-in-russia/a-75940102.

[28] Zadorozhnyy, "Moscow Citizens Turn to Pagers, Printed Maps."

## Roskomnadzor's Pre-TSPU Model

Before TSPU (pre-2021) became pervasive, Roskomnadzor mainly relied on a legal and administrative censorship stack: the centralized prohibited-sites registry, court and extra-judicial takedown orders, **pressure on hosting providers and search engines, DNS manipulation, and simple ISP-level IP blocking.**[29] This model was often inconsistent across networks as implementation quality depended on the ISP, its equipment, and its willingness or ability to comply precisely.[30]

The pre-TSPU model could still be disruptive, particularly for websites on dedicated IPs or with visible domains, but it had structural weaknesses. It was easier to evade with CDNs (Content Delivery Network), shared cloud infrastructure, domain changes, proxies, or VPNs, and it produced substantial collateral damage when authorities tried to block large address ranges.[31] Telegram's resistance in 2018 is the clearest case, but the same weakness was seen in opposition projects more broadly.[32]

[29] "Russia Internet Blacklist Law Takes Effect," *BBC News,* November 1, 2012, https://www.bbc.com/news/technology-20096274.

[30] Epifanova, "Deciphering Russia's Sovereign Internet Law."

[31] Ermoshina and Musiani, "The Telegram Ban."

[32] Internal ACF documents.

# TSPU and Its Deployment

## TSPU

TSPU stands for **“technical means to counter threats”**. In practice, it is Russia’s state-mandated ISP-side traffic filtering and manipulation layer, widely understood to be a DPI-based (Deep Packet Inspection) system, though it also includes surrounding management, control, and routing functions. Public policy analysis, academic analysis, operator testimony, and investigative reporting all describe TSPU as a combination of hardware and software supplied to operators but controlled by the state.

The most important technical distinction is architectural. Russia did not replicate China’s model. Instead of relying primarily on a small number of border choke points, since this is practically impossible, given how the internet developed in Russia, it pushed enforcement closer to end users by installing TSPU within or very near ISP access networks. Academic measurements identified over one million Russian endpoints in 650 ASes (Autonomous system) behind at least one TSPU device and concluded that 70 percent of TSPU devices were at most two hops away from the end IP.

This placement matters because it gives the system better visibility into user traffic and enables stateful, selective interference. Researchers found TSPU to be in-path and stateful, with blocking triggered by SNI (Server Name Indication), IP, and QUIC characteristics, and with behavior close enough to end users that purely remote measurement is often insufficient to observe the full mechanism.[33]

TSPU consists of a high-speed policy-checking hardware layer that either accepts/denies traffic or routes it to the low-speed CPU layer that performs complex packet analysis, segment reassembly, or traffic editing.[34] From experience, we know that the system is capable of intercepting traffic, doing real-time probing of the destination website, and depending on the outcome, accepting or denying requests.

## GRFC FSUE or Who Actually Runs the System

Roskomnadzor is the regulator and political-administrative center of the censorship system, but the General Radio Frequency Center Fed-

[33] Xue et al., “TSPU: Russia’s Decentralized Censorship System.”

[34] “How TSPU and DPI Work: An Analysis of Traffic Filtering and Blocking Mechanisms” (Как работают ТСПУ и DPI: разбор механизмов фильтрации и блокировок трафика), *Habr,* February 3, 2026, https://habr.com/en/articles/992232/ (accessed March 18, 2026)

eral State Unitary Enterprise (GRFC FSUE) functions as the technical arm of the system. The Insider's reporting, based on leaked documents, describes **GRFC as the customer and control center for TSPU supply**, installation, and operation, with the company Data Processing and Automation Center JSC acting as the system integrator and vendors such as RDP. RU. ru and Yadro involved in equipment and software supply.[35] In short, GRFC acts as the entity that manages the deployed equipment.

Operator-side materials tell a consistent story. A real-world operator account says the system is designed, installed, configured, and checked by Roskomnadzor or its contractors, that the operator cannot disable it, and that the operator still bears liability for traffic that bypasses it.[36]

An official GRFC  explanation reported by Digital Russia adds important procedural detail. Small operators with traffic up to 10 Gbps may avoid local installation only by routing through an upstream operator whose traffic already passes through TSPU; large operators and traffic exchange points must install TSPU in their own networks.[37] In other words, Russia has built policy mechanisms to minimize gaps in coverage even when a local ISP is too small to host the equipment itself.

## How TSPU Was Installed Across Russian Providers

The 2019 Sovereign Internet law **made TSPU mandatory** and put Roskomnadzor in charge of supplying it. DGAP's early analysis noted that the law required all ISPs to install TSPU and that Roskomnadzor would provide it free of charge, while giving the state centralized network-management powers in cases it defined as threats.

Investigative reporting later filled in the procurement side. The Insider reported a 2020 contract phase **worth 4.3 billion rubles and planned 2022-2024 spending of 24.7 billion rubles for supply and operation**, including EcoFilter DPI devices, Huawei servers, and other network components, with TSPU placed at junctions between operators and the wider internet.[38]

Public reporting in 2024 and 2026 indicates that deployment became close to universal among major operators. Habr's January 2026 reporting, sum-

[35] Lyndell et al., "Putin's Digital Iron Curtain."

[36] Pavel Vasilyev, "TSPU Installation" (Установка ТСПУ), https://pavel.su/internet/setting-up-tspu/ (accessed March 18, 2026).

[37] "Traffic Routing Schemes Through TSPU — GRFC" (О схемах пропуска трафика через ТСПУ — ГРЧЦ), *Digital Russia,* February 16, 2024, https://d-russia.ru/o-shemah-propuska-trafika-cherez-tspu-grchc.html.

[38] Lyndell et al., "Putin's Digital Iron Curtain."

marizing Roskomnadzor statements, said that since August 2023 all connection nodes at major providers had been equipped with TSPU and that the regulator now focused on installation compliance and constant modernization.[39]

The same Habr reporting states that operators must provide space, power, and remote access for GRFC, Roskomnadzor, and manufacturers, and must not obstruct remote management. As a result, the Russian state does not merely require operators to buy equipment — it embeds state-managed equipment into provider networks and reserves operational control over it.

The operator-side accounts are even more direct. The installation process begins when Roskomnadzor or its contractor contacts the operator, requests topology and load information, agrees the insertion scheme, and then places TSPU on uplinks so that all traffic, including transit traffic, passes through it.

## How TSPU continuously evolving

The situation as of 2026 shows that TSPU is not just a fixed censorship appliance but a continuously updated platform.

Habr's January 2026 reporting adds that already-installed TSPU kits require constant modernization because of traffic growth and that additional equipment is being installed at nodes to keep up.

Roskomnadzor goes further, describing an explicitly software-evolving anti-circumvention layer. TAdviser reported in January 2026 that Roskomnadzor planned a 2.27 billion ruble machine-learning-based traffic filtering system designed to expand TSPU's functionality and enable more targeted degradation of specific traffic types.[40]

Reuters reported in September 2024 that Russia planned to allocate almost 60 billion rubles over five years to strengthen the censorship system.[41] More recent reporting by TechRadar in 2026, citing experts and VPN operators, indicates that AI-assisted traffic analysis is already part of the current enforcement environment.[42]

[39] "Roskomnadzor Identified Violations in TSPU Installation at 33 Telecom Operators in Russia" (Роскомнадзор в ходе проверок выявил у 33 операторов связи в РФ «нарушения правил установки ТСПУ»), *Habr*, February 12, 2026, https://habr.com/en/news/984470/ (accessed March 20, 2026).

[40] "Roskomnadzor's Policy on Internet Control," *TAdviser*, March 25, 2026, https://tadviser.com/index.php/Article:Roskomnadzor%60s_policy_on_Internet_control.

[41] Gleb Stolyarov and Lucy Papachristou, "Russia to Spend Over Half a Billion Dollars to Bolster Internet Censorship System," *Reuters*, September 11, 2024, https://www.reuters.com/world/europe/russia-spend-over-half-billion-dollars-bolster-internet-censorship-system-2024-09-10/.

[42] Chiara Castro, "Russia's Battle Against VPNs Is Entering a New Phase: Here's What to Expect in 2026,"

This means that **treating TSPU as a static list of signatures would be a mistake**. The system is increasingly iterative: signatures, heuristics, active probing, and infrastructure-level rules are continuously updated over time.

## Why Centralized Circumvention Has Become So Difficult

Russia's old censorship regime could often be outmaneuvered by hiding behind shared infrastructure or shifting domains. Current TSPU changes the game because it enables **uniform, near-real-time policy enforcement across many ISPs without depending on each ISP's technical sophistication**. The 2022 TSPU measurement paper explicitly argues that the new architecture gives Roskomnadzor the ability to impose uniform censorship nationally in real time without relying on ISP technical capabilities or the blocking registry alone.

This makes centralized circumvention especially vulnerable. If you were to deploy a small number of common fallback transports, a narrow set of relay endpoints, or a stable signature shared by a very large Russian user population, this pattern would be unusually easy for the censor to observe and classify.[43] The system is designed precisely to identify repeated protocol fingerprints, suspicious SNI patterns, and traffic flows associated with known circumvention infrastructure.[44]

Our own experience points to the same operational conclusion from practice rather than research. The Smart Vote app was built specifically to withstand Roskomnadzor's restrictions, using service discovery through unconventional methods and automatically redirecting users away from blocked servers.[45]

In other words, the most resilient pattern combines decentralized distribution, configuration agility and protocol camouflage. This is the opposite of a simple global fallback switch inside a mainstream messenger.

*TechRadar*, January 24, 2026, https://www.techradar.com/vpn/vpn-services/russias-battle-against-vpns-is-entering-a-new-phase-heres-what-to-expect-in-2026.

[43] "[Russia] Censor Has a New Method of Blocking #490," *Net4People BBS (GitHub)*, https://github.com/net4people/bbs/issues/490 (accessed March 20, 2026).

[44] Internal ACF documents.

[45] See the Smart Voting section below for further detail.

# Successful Cases of Resistance to Roskomnadzor

## Telegram as a Successful Circumvention Case

In 2018, Roskomnadzor decided to block the Telegram messenger. But the attempt failed: although the service was officially unblocked only in 2020, restrictions had ceased to be effective much earlier.

Telegram's resilience became a turning point: it exposed the weakness of the old approach to internet control and helped explain the subsequent shift in policy. Users and service operators relied on proxies, VPNs, infrastructure maneuvering, and other bottom-up tactics, while Roskomnadzor's legal and technical efforts remained incomplete and costly.

Experts directly connect the failed 2018 Telegram campaign to the later policy decision to install DPI equipment across providers at government expense and formalize the program under the Sovereign Internet law.[46]

This is important because **it means Telegram's success is not a strong precedent for any kind of app today, unless one also accounts for the pre-TSPU timing**. What worked against IP-heavy blocking in 2018 cannot be assumed to work against distributed state-controlled DPI in 2026.

As of February 2026, the contrast is clear: the current effort against Telegram relies on TSPUs installed across all major Russian providers, allows targeted throttling of specific traffic types such as encrypted voice calls, and is harder to circumvent than the earlier brute-force block.[47] The State now **has the necessary tools and means to block Telegram completely**.[48]

## Smart Voting: A Closer Relevant Case Study

Smart Voting was an electoral strategy designed to reduce the vote share of pro-government candidates at elections of different levels through coordinated tactical voting. In 2021, the Navalny app was used to deliver the names of recommended candidates as part of this strategy.

This case is highly relevant because it demonstrates the **full escalation ladder of Russian pressure**: domain blocking, DPI-based interference, infrastructure adaptation by the target, pressure on app stores, and ultimately coercive pressure on distribution itself.

[46] Ermoshina and Musiani, "The Telegram Ban."

[47] Lyndell, Zayakin, and Klimarev, "Putin's Digital Iron Curtain."

[48] Mediazona, "No Country for Telegram."

Internal retrospective material from our team states that, once TSPU had been deployed broadly across providers, there was much less point in keeping the website itself alive because the site was already Roskomnadzor-blocked and accessible primarily through VPNs, prompting the team to use Android and iOS apps and a Telegram bot as alternative delivery channels.

The most important technical lesson is that the Navalny app did not rely on a single static backend or a normal app-update cycle to stay reachable. The app needed near real-time backend synchronization because Smart Voting recommendations were published only shortly before the election and depended on address-based candidate lookup, while delays in Google Play and App Store review made store-driven updates too slow for an active censorship environment. To solve this, the team built a custom discovery mechanism based on signed JSON configuration, low-TTL endpoint rotation, DNS-over-HTTPS resolution, and SNI-faking, allowing the application to learn fresh backend addresses without requiring a new store release every time Roskomnadzor blocked an endpoint.

Our circumvention strategy then evolved into aggressive "**preemptive rotation**". The team cycled through third-level subdomains, App Engine subdomains, large pools of pre-registered second-level domains, and later CDN-backed domains on providers such as Bunny, Fastly, and Amazon CloudFront, exploiting the fact that Roskomnadzor often needed minutes rather than seconds to discover and suppress each new endpoint. The ACF public report describes how some of these approaches forced the censor into increasingly costly choices: either keep chasing individual endpoints or escalate toward broader regex-, zone-, or platform-level blocking that risked collateral damage. The team monitored this battle operationally through a distributed probe network based on more than 50 Raspberry Pi vantage points across Russian ISPs, with Zabbix and Grafana used to watch block propagation and decide when to rotate again. Later, the monitoring network system could no longer continue working due to the risks of persecution by Russian authorities, as it required the installation and maintenance of equipment.

The app also experimented with stronger fallback layers than ordinary proxying. The client-side domain fronting, DoH-based fallback discovery through cloud storage, and even experimental integration of NewNode-style peer-to-peer transport concepts aimed to reduce dependence on ordinary DNS and conventional direct connectivity.

This is precisely why this case is relevant: Smart Voting was already converging on a model in which resilience came from transport agility, discovery agility, and distribution **outside normal web flows**, rather than from any single "working proxy" or stable domain.

Public reporting shows how the state responded. Apple and Google removed the Smart Voting app under Russian pressure on the eve of the September 2021 election, and Telegram also limited associated distribution channels.[49] This demonstrated that once network-level measures proved insufficient, the Russian authorities moved to choke the delivery ecosystem around the product.[50] Internal team assessments went further, suggesting that if store removal had failed, the state was prepared to escalate toward broader short-term disruption. While this should be treated as an internal operational judgment rather than a fully documented public fact, it is consistent with the technical and political trajectory of Russia's internet governance.

For any actor willing to resist the censorship, the conclusion is not that their app faces exactly the same app-store vulnerability profile as Smart Voting. The more important lesson is that, if the Russian state comes to view a censorship-resistant app as **sufficiently politically dangerous**, it may be willing to accept **very high collateral damage and escalate from service-specific blocking to much broader network disruption in order to degrade availability**. In this sense, Smart Voting is best understood not merely as a case of an opposition app being suppressed, but as **an early warning of how far the Russian state is prepared to go** when adaptive circumvention technology is perceived as a direct political threat.

[49] Steve Feldstein and Andrew S. Weiss, "Sideswiped: Apple, Google, and the Kremlin's Make-Believe Election," *Carnegie Endowment for International Peace,* September 23, 2021, https://carnegieendowment.org/russia-eurasia/posts/2021/09/sideswiped-apple-google-and-the-kremlins-make-believe-election.

[50] Navalny Team, "RKN vs. the Navalny App: The Fight for Accessibility" (РКН против приложения «Навальный»: борьба за доступность), *Dev.to,* September 14, 2023, https://dev.to/navalnyteam/rkn-protiv-prilozhieniia-navalnyi-borba-za-dostupnost-2gg6.

# The Current State of Internet Censorship in Russia

## The State of VPN Blocking in 2025–2026

The evidence now strongly supports the conclusion that **Russia can block or substantially degrade most mainstream VPN protocols**. Human Rights Watch reported in March 2026 that Roskomnadzor had blocked 469 VPN services and had been blocking the three most popular VPN protocols since December 2025.

Expert social and technical channels documented earlier waves. SecurityLab's Telegram archive reported mass disruption of OpenVPN in May 2023, major blocking of OpenVPN and WireGuard in August 2023, and wider failures of OpenVPN, IKEv2, IPsec, and WireGuard shortly afterward across both mobile and fixed operators.

By 2026, the public operational consensus has shifted from "use a VPN" to "**use the right family of transports, configured carefully, and expect continuous churn**". TechRadar's January 2026 reporting, citing Amnezia and other operators, says that most VPN protocols are blocked and that the more resilient options are protocols that disguise themselves as **ordinary traffic**, including XRay transports such as VLESS, plus NaiveProxy, Hysteria, and AmneziaWG when properly configured.[51]

The Habr VLESS article makes a similar, more opinionated claim: that OpenVPN, WireGuard, Shadowsocks, Trojan, and VMess have all been significantly degraded or detected, while VLESS with TLS, WebSocket, and CDN fronting remains one of the few relatively durable approaches.[52] Even if one treats some of the article's percentages cautiously, its technical direction is consistent with broader reporting and field practice.

Internal ACF documentation and discussions independently reach the same conclusion. Most protocols are blocked, and VPN providers play constant cat and mouse with Roskomnadzor's GRFC.

[51] Chiara Castro, "Russia's Battle Against VPNs Is Entering a New Phase: Here's What to Expect in 2026," *TechRadar*, January 24, 2026, https://www.techradar.com/vpn/vpn-services/russias-battle-against-vpns-is-entering-a-new-phase-heres-what-to-expect-in-2026.

[52] "The VLESS Protocol: How It Bypasses Censorship in Russia and Why It Works," *Habr*, February 17, 2026, https://habr.com/en/articles/990144/.

## Suspicious Subnets and Data-Center Reputation Now Matter

Russian internet censorship is also no longer limited to protocol fingerprints. It increasingly appears to incorporate **infrastructure reputation, destination heuristics, and region-specific rules**.

A June 2025 Net4People report describes a method in which TCP connections to "suspicious" foreign data-center IPs are frozen after roughly 15-20 KB of server response data, especially on mobile networks, even when the connection is being an HTTPS traffic, looks like HTTPS or VLESS, Reality over TLS 1.3. The examples explicitly include Hetzner, DigitalOcean, Cloudflare, OVH, Oracle, and AWS.

Independent discussion in the Tor Project forum documented similar real-world breakage for Hetzner IP ranges: TCP to all ports stops receiving SYN responses, UDP fails, ICMP still works, the block is temporary but retriggerable, and the effect may extend to other data-center networks such as OVH.[53]

Internally, our IT team also noticed multiple situations with this exact behavior from Russian ISPs, and we reached the same conclusion as stated above.

In this case, the operational implication is clear: a circumvention plan that concentrates heavily on a few well-known foreign cloud providers or stable data-center ASNs is unusually vulnerable. Even if the protocol layer is obfuscated, the **infrastructure layer may still be scored as suspicious and degraded**.

## Encrypted Client Hello (ECH): Blocked and Ineffective

Encrypted Client Hello (ECH) is a TLS 1.3 extension that encrypts the ClientHello message, including the SNI (Server Name Indication) field traditionally used by DPI systems to identify which domain a connection targets. While ECH was intended as "the last puzzle piece to privacy" in TLS, it has proven **highly vulnerable to state censorship in Russia**.

In October 2024, Cloudflare enabled ECH by default for its customers. Within a month, on November 5, 2024, Russia's Roskomnadzor began **blocking ECH connections through TSPU**. The blocking triggers when a ClientHello contains both the ECH extension and the SNI value. Matching packets are silently dropped, affecting both TLS and QUIC traffic, but only

[53] "Tor and Hetzner Block in Russia," *Tor Project Forum*, December 2024, https://forum.torproject.org/t/tor-and-hetzner-block-in-russia/16134 (accessed March 20, 2026).

to Cloudflare's advertised IP ranges. Thousands of Cloudflare-hosted websites became inaccessible to Russian users. Roskomnadzor stated that ECH "**violates Russian legislation and is restricted by TSPU**."[54]

ECH fails as a censorship circumvention tool for several reasons. Cloudflare remains virtually the only major provider supporting it. The fixed outer Cloudflare SNI makes filtering trivial. ECH depends on encrypted DNS to retrieve server configurations, so **blocking DNS resolvers alone is sufficient to prevent ECH usage**. ECH was designed as a privacy mechanism, not a censorship circumvention tool, and it does not fulfill the latter role. It may complement DPI-bypass tools like Zapret or GoodbyeDPI, but as a standalone solution against state-level filtering it is ineffective.

## Moscow's "Whitelist Internet" Tests

The March 2026 reports from Moscow are strategically important because they suggest that Russia is experimenting with a still more restrictive mode: **not merely blocking selected destinations, but allowing access only to an approved** subset of sites and services during shutdowns or exceptional conditions.[55]

According to these reports, the whitelist model initially allowed access mainly to pro-government social platforms, state media, and official government resources, which represents a qualitative shift from earlier phases of censorship, which were centered on blocklists and throttling alone. In practical terms, this kind of regime is especially hostile to centralized circumvention, because a global relay, a stable fallback domain, or any persistent alternative control plane can simply be excluded from the approved set at the network layer.

At the same time, early field practice already shows that even **whitelist-style restrictions can be bypassed** in some cases by tunneling traffic through infrastructure that remains reachable because it belongs to approved domestic services. One illustrative example is **vk-turn-proxy**, an openly published tool that proxies WireGuard or Hysteria traffic through TURN servers used by VK Calls, and previously also Yandex Telemost, rather than sending that traffic directly to a foreign VPN endpoint. As described in its documentation, the tool generates TURN credentials from a VK call link, encapsulates packets with DTLS 1.2, sends them over parallel TCP or UDP streams using STUN ChannelData, and has the TURN server forward the traffic by UDP

[54] "Encrypted Client Hello Didn't Solve Censorship, but Still May Have a Role to Play," *AdGuard DNS Blog*, November 25, 2024, https://adguard-dns.io/en/blog/encrypted-client-hello-misconceptions-future.html.

[55] Zadorozhnyy, "Moscow Citizens Turn to Pagers, Printed Maps."

to the user's own server, where it is decrypted and handed to WireGuard. The same project also documents integration paths for V2Ray/Xray-style clients, allowing SOCKS or HTTP proxying on top of the same transport rather than only a plain WireGuard-style tunnel.[56]

This is an important proof of concept because it shows that **even a whitelist regime is not necessarily absolute**: if a censor leaves a domestic real-time communications platform reachable, its media-relay or TURN infrastructure may potentially be repurposed as a transport substrate for censorship circumvention. But it would be a mistake to overgeneralize from that fact. The repository itself documents practical constraints, including the closure of Yandex Telemost support, VK-related speed limits, the need for manual TURN selection in some cases, MTU tuning, routing tricks, and the risk that less obfuscated modes can lead to bans or rapid breakage.

In this case, the key implication is that while whitelist bypass may be technically possible at the edge, it is **far less clear how such an approach could be translated into a centralized, productized "bigtech app"-scale system**: a mass deployment would be much more visible, would depend on third-party Russian infrastructure that you do not control, and would almost certainly **trigger rapid countermeasures** once Russian authorities recognized it as a generalized bypass channel. In other words, even if whitelist circumvention remains possible in principle, turning it into a durable centralized app strategy would require **substantial ongoing engineering effort, constant adaptation, and acceptance of a fast-moving escalation cycle with the censor**.

## The Monitoring Problem: Why You Cannot Rely on a Simple External Checker

One of the hardest practical problems is **observability**. We still do not have a simple, comprehensive, and reliable way to test "is this service reachable from Russia right now?" from outside the country. The TSPU measurement paper is explicit that answering such questions is hard because researchers need local Russian vantage points on networks where TSPU is deployed, and because the asymmetric nature of TSPU restrictions makes standard remote measurement insufficient for many cases. The same conclusions were reached by our team during internal development of some of our applications.

OONI is the most important open network-measurement effort here, and it remains valuable, but **even OONI does not eliminate the problem**.

[56] "vk-turn-proxy," *GitHub*, https://github.com/cacggghp/vk-turn-proxy (accessed March 20, 2026).

Its data relies on volunteer-run probes, coverage varies by network and time, and Russia **blocked OONI Explorer in 2024** specifically because it contained circumvention-related information.[57]

OONI's own recent analysis confirms both the value and the limitation of open measurement. It finds **strong evidence of widespread TLS-based interference across many Russian networks** and argues that censorship appears centrally managed through **decentralized TSPU deployment**, but this conclusion still depends on distributed volunteer vantage points, rather than on a simple universal checker.

Our team also previously operated a multi-provider monitoring network inside Russia used to test the availability of internet resources from different providers, and that network was later dismantled under state pressure, forcing some participants to leave the country. Similar monitoring capacity associated with several other projects has also become degraded or unavailable. This shows that the Russian state sees those efforts as a threat to their censorship process.

Thus, the practical consequence is that external probes are necessary but insufficient. The more scalable signal is likely product telemetry: **connection success rates, handshake failure types, latency shifts, transport fallback rates, geographic and ASN-level anomaly detection, and comparative success across transport variants**.

[57] Maria Xynou, "Russia Blocked OONI Explorer, a Large Open Dataset on Internet Censorship," *OONI*, September 25, 2024, https://ooni.org/post/2024-russia-blocked-ooni-explorer/.

# Conclusions and Recommendations

## DPI Circumvention

When a full VPN is unavailable or undesirable, tools such as Zapret and GoodbyeDPI can be used as a fallback option. Both solutions work locally, do not require connecting through third-party servers, and are designed to bypass TSPU DPI; Zapret is described as an autonomous multi-platform DPI bypass tool, while GoodbyeDPI provides a similar approach for Windows systems.

In practice, this means they can still help **restore access to services such as Telegram or WhatsApp when direct connections fail**. GoodbyeDPI supports techniques such as packet fragmentation, HTTP/TLS request modification, fake packet injection, and dedicated handling for QUIC/HTTP3, while Zapret includes DPI desynchronization methods, fake packet retransmission, and specialized profiles for protocols and services including QUIC and Discord; for that reason, it makes sense to add comparable **client-side fallback logic and automatically switch to DPI bypass behavior** when the client cannot reach target hosts through a normal connection path.[58] However, some of those methods require low-level network APIs that are normally restricted on Android and iOS, making **cooperation with OS vendors necessary**.[59]

## Implications for a circumvention strategy

Based on the evidence outlined above, our team recommends the following:

### 1. A centralized circumvention program is viable only as a permanent engineering function

The evidence suggests that a centrally managed circumvention layer can maintain reachability for some users, but only if it is treated as an **ongoing operational function rather than as a one-off feature**. Russia’s system updates signatures, scales infrastructure, targets app distribution, and increasingly scores both protocols and hosting environments.

In practical terms, this would require a dedicated team working daily on transport changes, endpoint diversification, telemetry analysis, and incident response. Without this, any fixed solution is likely to decay quickly.

[58] ValdikSS, “goodbyeDPI,” *GitHub,* https://github.com/ValdikSS/goodbyeDPI (accessed March 20, 2026).

[59] bol-van, “zapret,” *GitHub,* https://github.com/bol-van/zapret (accessed March 23, 2026).

### 2. Avoid standard VPN assumptions

App circumvention layer should not assume that OpenVPN, IKEv2, IPsec, or vanilla WireGuard are dependable building blocks in Russia. Public reporting and operational evidence show repeated mass failures for these protocols.

More resilient approaches currently include VLESS, XRay-style transports, AmneziaWG, NaiveProxy, Hysteria, and other camouflage-heavy protocols, but even these should be treated as **moving targets rather than permanent solutions**.

### 3. Distribution and discovery are part of the threat model

If circumvention features depend on **obvious settings pages, app-store updates, a single domain, or a stable published list of endpoints**, those surfaces will become **targets**.

You should therefore assume the need for **silent server-side activation, remote configuration, multiple discovery paths**, piggybacking on services that are unlikely to be blocked in their entirety, and also consider out-of-band bootstrap methods that do not depend on a single public domain. This recommendation follows directly from the distribution failures observed in Smart Voting.

### 4. Measure availability primarily through telemetry, not through one external monitoring stack

Since TSPU is **close to end users** and standard remote measurement is incomplete, You should treat its own **telemetry as the primary availability oracle**. Probes from inside Russia would still help, but they should be only one layer of evidence.

### 5. A grassroots strategy may be more realistic than a purely centralized arms race

The most realistic medium-term option may be a **grassroots or ecosystem strategy rather than a fully centralized circumvention system**. Public communication encouraging VPN use, support for circumvention projects, interoperability with resilient transports, and selective P2P or peer-assisted delivery features may yield **more durable outcomes than a single transport** that the state can classify as one more target.

However, peer-to-peer delivery may be complicated by the fact that you potentially can be **designated as an extremist by Russia**. Addressing this may require **non-trivial solutions**, such as ensuring that communication links remain cross-border and implementing informed-consent mechanisms for peers, in order to avoid "surprises" if, for example, a person travels to Russia while using a hypothetical "App P2P relay" application. Therefore, additional legal analysis is required to assess the risks for cooperating peers and the potential impact on your reputation should these risks materialize. Notable examples of users being prosecuted for using software include, first, the prosecution of ByLock messenger users in Turkey in 2016 (see the Yalçınkaya v. Türkiye ruling by the European Court of Human Rights). Second, users of BitTorrent software have been prosecuted not for downloading copyrighted material but for distributing it ("seeding").

### Recommended Near-Term Actions

1. **Establish a dedicated anti-censorship function focused on Russia**, with protocol, infra, SRE, and measurement ownership.
2. **Build an internal reachability dashboard** for Russia, based primarily on your app telemetry by ASN, network type, app version, handshake type, and fallback path success.
3. **Avoid standard VPN protocols and static data-center concentration**; diversify infrastructure away from easily scored subnets and **expect recurrent endpoint burn**.
4. **Prototype pluggable, obfuscation-heavy transports and configuration agility mechanisms** that can be updated without forcing obvious user actions.
5. **Explore whether limited peer-assisted or store-and-forward components** can reduce dependence on a small set of centrally visible relays during acute blocking periods.
6. **Consider an ecosystem approach**, including support for external circumvention projects and user education, because the strongest surviving pattern in Russia is distributed adaptation rather than one stable central bypass.

## Conclusion

Russia's system of internet restrictions can **no longer be described as a set of isolated blocks that can be bypassed through a single, universal technical workaround**. In recent years, the state has built a distributed yet centrally managed censorship system that operates closer to the user, adapts rapidly to new circumvention methods, and increasingly combines network-level controls with pressure on infrastructure and distribution channels.

While it remains technically possible to mitigate restrictions on messaging applications in Russia, **the associated costs and operational complexity are substantial.** The evidence suggests that any serious centralized circumvention effort must function as an **ongoing program supported by dedicated engineering resources, rapid iteration, and strong telemetry**.

A more realistic long-term approach is **hybrid**: combining internal transport agility and monitoring with a broader grassroots and ecosystem strategy. Russia's censorship system is specifically designed to **detect and shut down uniform, centralized circumvention methods once they become visible at scale**.

Email: fbk@fbk.info