



Up to Spec

**TSPU & Russia's National Internet Filtering
System**

Dmitry Kuznetsov
September 2026

critical
Infrastructure
lab



Up to Spec: TSPU & Russia's National Internet Filtering System

Research Report

Published by the critical infrastructure lab, Amsterdam, September 2026.

“Up to Spec: TSPU & Russia’s National Internet Filtering System” is marked with CC0 1.0 Universal.

Set in Source Sans, Source Serif, and Source Code.

Design and visual identity by Ulrike Uhlig.

The publication pipeline is made with free software from plain text:
<https://codeberg.org/criticalinfralab/publication-pipeline>

Originally developed by Ulrike Uhlig, currently maintained by Anders Aarvik and maxigas.

critical infrastructure lab document series
CIL#017

DOI 10.5281/zenodo.22794150

This work was supported by the Open Technology Fund.

The author thanks everyone who contributed to this report through discussions, careful reading, and helpful feedback.

Table of Contents

Overview	1
1. How Control Works	2
1.1 In-path filtering	2
1.2 The compliance perimeter	3
1.3 Exceptions and approved access	5
2. What the System Changes	6
2.1 Operator autonomy	6
2.2 Market structure	7
2.3 Access to information	7
3. How the System Became Durable	8
3.1 Deployment and investment	8
3.2 Built into markets and institutions	11
3.3 Expanding functions and entrenchment	13
4. Why This Matters Beyond Russia	15
4.1 Ordinary technology, different governance	15
4.2 Cross-border effects	17
4.3 A replicable model	18
5. What Civil Society Can Do	18
5.1 Standards governance	18
5.2 Export controls and procurement accountability	19
5.3 Independent measurement and early warning	19
Notes	20

Overview

Russia has built a comprehensive centralised internet filtering system. Its core component is TSPU (Technical Means of Countering Threats), a hardware-and-software stack for deep packet inspection built by Russian vendors. Measurement research conducted by Xue et al. (2022) found the equipment sitting in-path: all traffic on a covered route passes through it before reaching its destination⁰¹. Roskomnadzor reports that all operator traffic is covered. The equipment is state property, operated remotely by GRFC (the General Radio Frequency Centre, Roskomnadzor's technical arm) from a centralised management system⁰², and Internet Service Providers (ISPs) have no access to the devices' configuration, filtering rules, or operational status⁰³.

For years, internet controls in Russia relied on delegation: ISPs implemented state requirements but retained substantial discretion over how they did so. They filtered selectively, embedded protest messages in blockpages, and organised through industry associations to challenge regulatory overreach⁰⁴. TSPU changed that relationship. The state now operates filtering equipment inside private networks, while operators carry traffic through devices they cannot inspect or control.

Federal Law No. 90-FZ ('On Amendments to the Laws on Communications and Information', May 2019), widely referred to as the 'Sovereign Internet Law', provided the legal basis for this shift. The telecom industry initially dismissed it as a rent-seeking exercise⁰⁵. The state subsequently mapped the network, specified and supplied the equipment, established centralised management, increased the cost of non-compliance, and made network requirements a formal condition of an ISP licence^{06, 07}.

The system works because in-path filtering is reinforced by licensing rules, state institutions, domestic vendors, and pressure on the platforms and payment systems through which circumvention reaches users. It does not disconnect Russia from the global internet. It administers what may pass across a network that remains interconnected.

This report is written for civil society organisations, advocates, researchers, and others seeking to understand or respond to Russia's internet controls. It explains how the system works, what it changes for operators and users, why it has become difficult to reverse, and why the model matters beyond Russia's borders.

—

1. How Control Works

1.1 In-path filtering

TSPU's core capability is traffic classification and filtering via Deep Packet Inspection. It combines network- and transport-layer controls with application-layer inspection, identifying, slowing, or blocking traffic by URL, IP address, protocol signature, or server name.

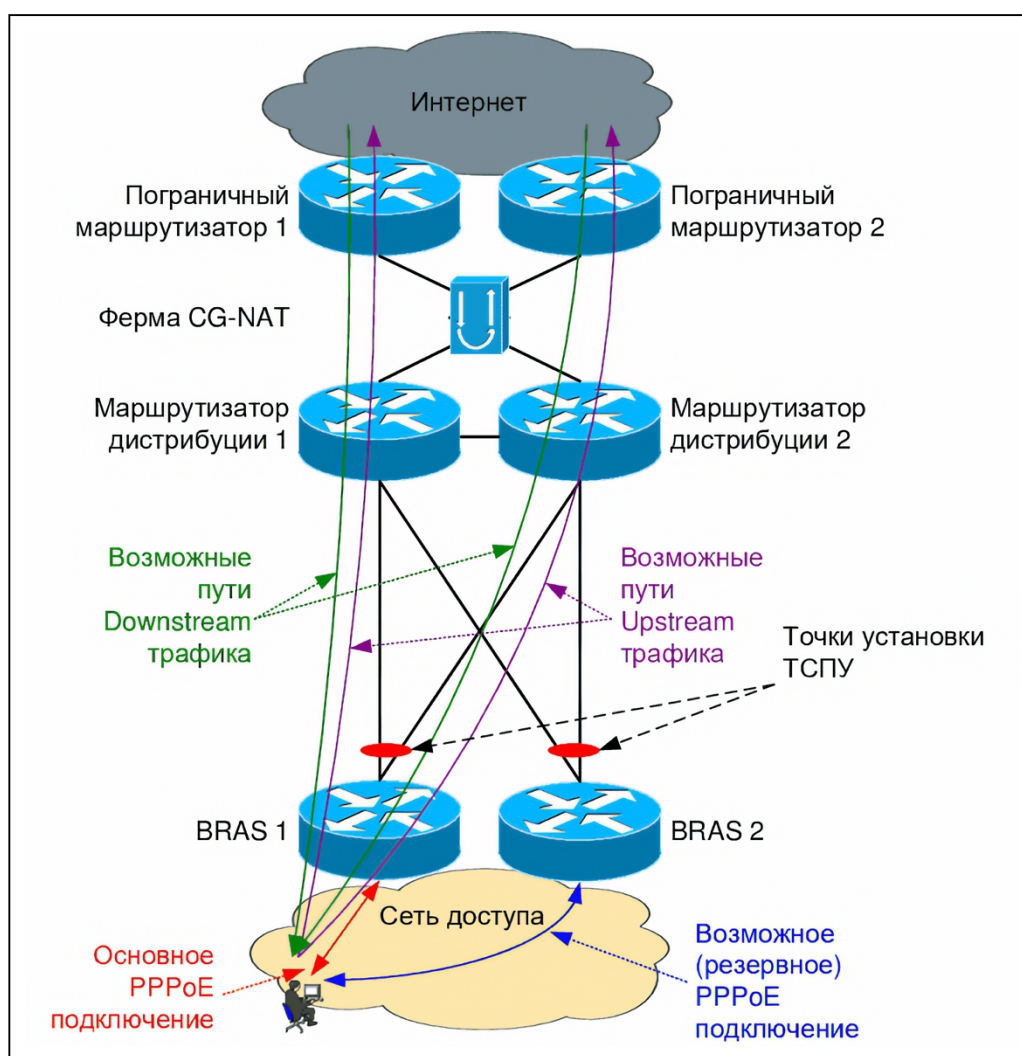


Figure 1: ISP network topology showing TSPU placement between border routers and access network. Source: Nabr, "Операторы связи фиксируют проблемы с оборудованием РКН."

Roskomnadzor blocked more than 1.2 million resources during 2025, 50% more than the year before⁰⁸. The number of VPN services targeted for blocking rose from 167 in October 2023 to 469 by February 2026^{09, 10}. VPN blocking has expan-

ded from website-level to protocol-level, targeting how circumvention tools communicate rather than only where they connect⁰⁹.

TSPU can also degrade services without blocking them outright. YouTube was throttled to near-unusable speeds from August 2024 by inspecting the plaintext Server Name Indication (SNI) label in encrypted connections. Telegram¹¹ and WhatsApp calls were blocked first, then media was throttled, then the services were progressively restricted¹².

DNS controls add another point of restriction: a user needs both a usable answer to a domain-name lookup and a working connection to the resolver supplying it. Teplit's August 2026 investigation found that access to external DNS services varied by network and transport. Failure of ordinary UDP queries from one residential connection did not mean encrypted DNS was also unavailable there¹³.

Roskomnadzor's digitalisation plan, presented in December 2025, allocated 2.27 billion roubles for machine-learning-based traffic analysis¹⁴. Machine learning is being added to the system's repertoire, but filtering technology alone does not explain its reach. Control also extends to the companies, platforms, and payment systems through which circumvention is distributed and sustained.

1.2 The compliance perimeter

When technical filtering encounters resistance, control extends to the organisations that help users find, obtain, and pay for circumvention. From March 2024, publishing information about how to use circumvention tools is illegal¹⁵. Users may need a VPN to read about VPNs. Apple removes VPN apps from the Russian App Store at Roskomnadzor's request¹⁶.

Payment barriers have several origins. After the 2022 invasion, sanctions and the withdrawal of international payment services narrowed access to cross-border payments. Mastercard, for example, distinguished regulator-required exclusions of particular banks from its broader decision to suspend Russian operations. Domestic processing continued through Russia's own system¹⁷. Russian authorities subsequently closed additional routes: on 1 April 2026, mobile operators disabled carrier billing for Apple ID payments on instruction from the Ministry of Digital Development¹⁸. App-store removal obstructs download, while closing payment routes can prevent subscription renewal. VPN use itself is not banned.

—

For services that resist, cost becomes another filtering mechanism. Liberty VPN, which reports 250,000 users, estimates that fully countering active blocking would cost roughly \$25,000 per hour, a sum it says it has never had. Services with fewer than 50,000 users may be unable to sustain continuous server replacement¹⁶. None of the services surveyed in April 2026 reported having been fully blocked¹⁶, but continued adaptation is expensive. From June through July 2026, Amnezia was disrupted by successive blocking waves, alongside a denial-of-service attack on its payment gateway and phishing directed at its staff. A developer attributes the campaign to Roskomnadzor and says the service's traffic had been studied for roughly a year, allowing new blocking methods to be introduced as Amnezia adapted¹⁹.

Cloudflare shows how the layers combine. When it enabled Encrypted Client Hello (ECH) by default in October 2024, it encrypted the server-name field TSPU uses for selective application-layer filtering. On 7 November, GRFC's operational arm urged Russian website operators to disable ECH or migrate to domestic content-delivery networks, saying ECH was already restricted by TSPU²⁰. In February 2025, Roskomnadzor listed Cloudflare as an organiser of information dissemination under FZ-149, placing it in a category of companies required to store user data in Russia and provide the FSB with access²¹. Roskomnadzor repeated its recommendation in April²², and from June ISPs throttled Cloudflare traffic, degrading content delivery, DNS-over-HTTPS, API access, and certificate validation²³.

Tests from one Moscow vantage point in March 2025 found ECH blocking under specific conditions involving Cloudflare, alongside ways around it²⁴. ECH availability therefore needs to be assessed for the connection and network concerned.

Evgeny Martynov, IT director of the registrar RU-CENTER, put Cloudflare at roughly 44% of the CDN services used for .ru domain delegation and about 11% of .ru sites overall²⁰. Cloudflare stated that it had received no official communication from Russian authorities and had no means to restore connectivity²³. Technical blocking, pressure on Russian website operators, regulatory reclassification, and infrastructure-level throttling reinforced one another. The compliance perimeter reached a global infrastructure provider through the Russian organisations and customers that depended on it.

1.3 Exceptions and approved access

The system also administers exceptions. Traffic that would otherwise be blocked may pass when an address, protocol, or service is approved. Protocol-level blocking also disrupts the OpenVPN connections that Russian banks and commercial companies use for secure internal communications²⁵. Roskomnadzor therefore operates an exemption list through the Centre for Monitoring and Management of the Public Communications Network (CMU SSOP). The list grew from 12,000 corporate IP addresses in October 2023 to 75,000 entries by April 2025²⁶. To obtain an exemption, a company supplies its name and tax number, the protocol it uses, the source and destination addresses, and the purpose of the connection. Relief from the filter depends on declaring what a network carries and why.

During security-justified mobile shutdowns, the same logic operates at service level: ordinary access is restricted to pre-approved services²⁷. Russia recorded 655 mobile internet shutdowns in June 2025, ten times the May figure²⁸. In Belgorod Oblast, mobile internet was shut down in November 2025 while air-defence systems were operating, disrupting the civil alert system. The governor tied the decision to security concerns²⁹. In Ulyanovsk, the regional digital development minister said no end date had been set and that, absent other federal decisions, restrictions would run until the end of the war²⁷.

The access list grew from more than 50 sites in October 2025 to more than 500 entries by April 2026. The April additions included volunteer search organisations, banks, retailers, and IT firms. The Ministry of Digital Development approves entries on grounds of popularity and essential use, while security services assess them on security grounds³⁰. Those security requirements determine which banks appear on the list. In February 2026, Sberbank, T-Bank, and Gazprombank were absent because they lacked the System of Operative-Investigative Measures (SORM), Russia's lawful interception framework, while VTB and Promsvyazbank were admitted. Gazprombank was added by April, and full SORM implementation becomes mandatory for banks in 2027³⁰.

In March 2026, users in Rostov-on-Don reported that home internet had been placed under access-list restrictions, with Telegram blocked and VPNs non-functional on fixed broadband. The operator disputes the account³¹. If confirmed elsewhere, such an expansion would narrow the distinction between temporary mobile shutdowns and persistent access control. TSPU now determines what may pass, for whom, and under what declared purpose.

—

2. What the System Changes

2.1 Operator autonomy

The Russian segment of the internet remains heterogeneous and distributed, with approximately 5,000 active autonomous systems and 32 Internet Exchange Points as of 2026³². TSPU did not require a major reconfiguration of that topology. It changed the state's relationship to the operators who run it: filtering decisions moved from delegated enforcement into equipment operated from the centre, while licensing conditions and penalties raised the cost of refusal.

Pavel Vasiliev, an operator who documented the installation process³³ and a year of operations³⁴ with TSPU, describes filter-rule changes deployed without notice and no visibility into what the state equipment is doing to traffic. Yarnet, a Yaroslavl ISP, confirmed that all of its traffic passes through the device and that the operator has no local override³⁵. The devices function as black boxes inside operator networks^{33, 34, 35}, extending a pattern previously documented for SORM and blacklist filtering³⁶.

The consequences of central management can spread beyond one operator. In January 2025, a TSPU misconfiguration cascaded across ISPs, cutting traffic at Russia's largest exchange point by roughly 11% until the settings were rolled back some fifteen to twenty minutes later³⁷. Operators could neither inspect the broken rule nor exempt their customers from it.

Operators did initially contest FZ-90. A collective industry submission assembled in a week and attracted around 30 company signatories. Two of its three objections were removed from the bill, and the third was clarified³⁸. The mandate survived. By 2022, industry discussion had shifted from resistance to absorbing higher compliance costs³⁸, and by 2023 to implementing domestic replacements in a market where operators were told there was “not always a choice”³⁹.

Penalties make non-compliance commercially dangerous. Since January 2024, breaches of SORM obligations, a missing commissioning certificate, or failure to implement an interception plan have drawn turnover-based fines or a minimum fine of one million roubles. Separate penalties apply to TSPU breaches, rising to between 3 and 5 million roubles for a repeat corporate offence. An official or sole trader already sanctioned administratively can face up to three years in prison⁴⁰.

—

In March 2026, a St Petersburg magistrate fined the provider Tinko 250,000 roubles for allowing subscribers to reach YouTube around its TSPU⁴⁰. When Beeline briefly offered a “YouTube without VPN” service in January 2026, routing subscribers around the throttle, it was shut down within days⁴¹. Abramovskaya, a practising lawyer and self-described perfectionist, described the interlocking framework as an impressively constructed scheme. Attempts to reduce or escape one liability, she explained, expose operators to another. She also advised operators to limit the portion of their tariff counted as telecom revenue, reducing the base for turnover-calculated fines⁴⁰.

2.2 Market structure

Higher entry and compliance costs put particular pressure on small ISPs. From January 2024, the state duty for a new telecom licence carrying lawful-interception obligations rose roughly 130-fold, from 7,500 to 1 million roubles per service type. Renewals remained at 7,500. Human Rights Watch assesses that the increase made market entry harder for small ISPs^{10, 42}. The Association of Small Operators (AMOR) has documented exit pressure among more than 100 members, engaged GRFC on TSPU compliance, and challenged revocations it considers unjustified⁴³.

Seven leading providers now manage more than half of RuNet IP addresses, with state-owned Rostelecom alone accounting for a quarter¹⁰. Rostelecom openly advocates further consolidation. At KROS 2023, its director for regional operator relations, Yekaterina Kazakova, opened an acquisition segment from the stage: “look at your neighbour, maybe someone is ready to sell, someone to buy. And we will share our expertise with you today. How does Rostelecom see this?”⁴⁴ In 2024, she argued that the market needs large, full-cycle infrastructure providers and presented consolidation as the response to staff shortages, ageing infrastructure, traffic growth, and low revenue per subscriber⁴⁵.

2.3 Access to information

Human Rights Watch describes circumvention tools as a precondition of access to information in Russia¹⁰. Their availability is nevertheless being narrowed at several points: websites and protocols are blocked, information about circumvention is restricted, apps disappear from stores, and payment pathways close. Each measure raises the knowledge, time, and money required to reach independent information.

Access is stratified by technical knowledge, affordability, and access to usable payment methods. These resources shape which circumvention services people

–

can obtain and sustain as blocking changes. Provider interviews describe the costs of maintaining access and the difficulty of reaching users who need it¹⁶. An Amnezia developer also identifies foreign cards as an exception to payment difficulties¹⁹. Advanced protocols can preserve routes to independent information, but require continued adaptation: Amnezia reported restoring access after the June–July 2026 blocking waves through a further protocol revision¹⁹. Knowing a tool exists, obtaining a trustworthy client, paying where necessary, and keeping it configured are all part of usable access. Socket’s investigation of VPN-brand impersonation aimed at Russian-speaking users illustrates the risks at the point of choosing and obtaining a tool⁴⁶.

During approved-access restrictions, ordinary connectivity is organised around an administratively selected list. Circumvention may remain possible where a service can use reachable infrastructure, but its availability depends on the network and the resources required to sustain it. In April 2026, Amnezia described services specialising in allow-list circumvention and the higher costs they could face when replacing IP addresses¹⁶. This is evidence of continuing adaptation, rather than a guarantee of access in every affected region. Banking, transport, communications, and civil alerts consequently become more dependent on administrative inclusion, even where some routes beyond the list remain.

The restrictions accumulate across several actors: TSPU filters traffic, GRFC manages infrastructure and exemptions, security services set access conditions, and app stores and payment processors enforce commercial pressure. No single intervention explains the result. Together they make independent information progressively harder to find, obtain, and sustain.

3. How the System Became Durable

3.1 Deployment and investment

TSPU expanded from 558 communications nodes in 2021 to 860 in 2022, with 1,360 planned for 2023⁴⁷. In October 2023, the Centre for Monitoring and Management of the Public Communications Network reported more than 1,100 nodes, full traffic coverage, and more than 100 Tbit/s carried⁴⁷. By October 2025, Roskomnadzor reported 1,406 nodes carrying 132.3 Tbit/s⁴⁸.

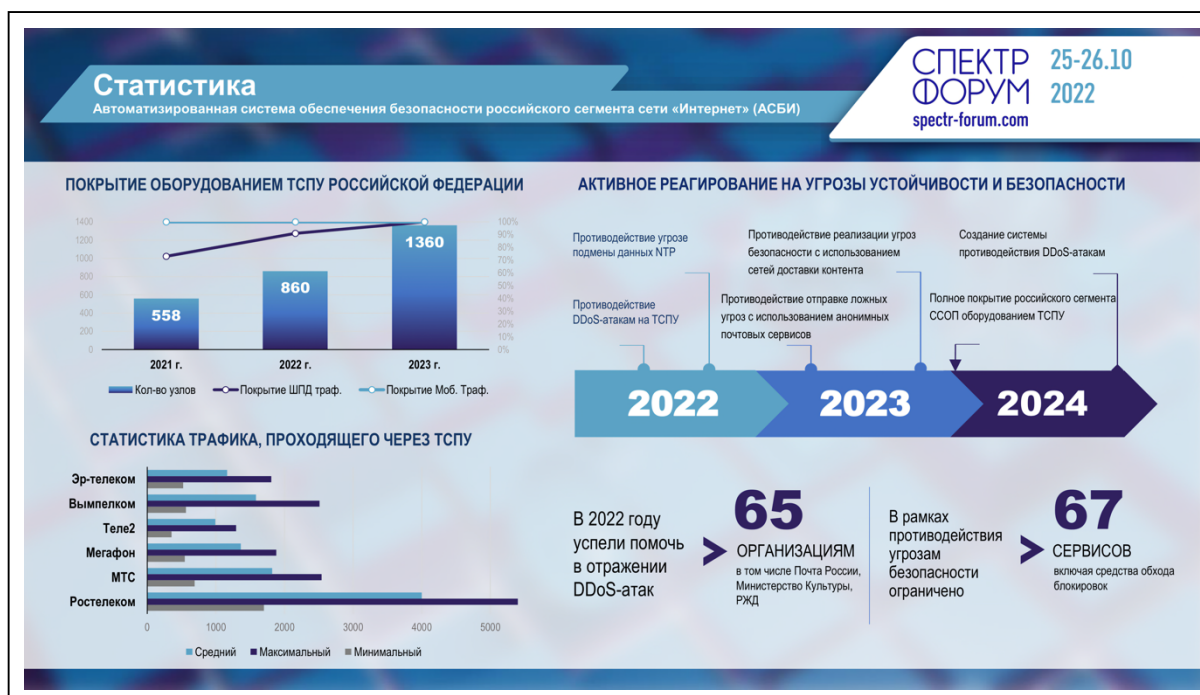


Figure 2: TSPU node expansion: 558 -> 860 -> 1,360. Source: Khutortsev, Spektr Forum, October 2022 (2023 value as then planned).

Independent measurement provides a lower bound rather than a competing device count. Xue et al. identified approximately 6,871 in-path TSPU “links” across 650 autonomous systems in 2022. Their method inferred network paths from traceroute clustering and could not see TSPU behind Network Address Translation, so the authors treat the result as a substantial underestimate of deployed equipment⁰¹.

GRFC’s monthly operational reports document the same expansion in monitored traffic across every federal district⁴⁸. Data extracted from the reports (May 2023 – January 2025) show total monitored traffic rising from 77.7 to 120.4 Tbit/s, an increase of some 55%, with broadband consistently accounting for roughly 80% of the total and mobile for 20%⁴⁸. District-level data show year-on-year growth ranging from 95% in the North Caucasus to 18% in the Far East⁴⁸. The variation shows uneven growth in monitored traffic rather than gaps in the districts represented.

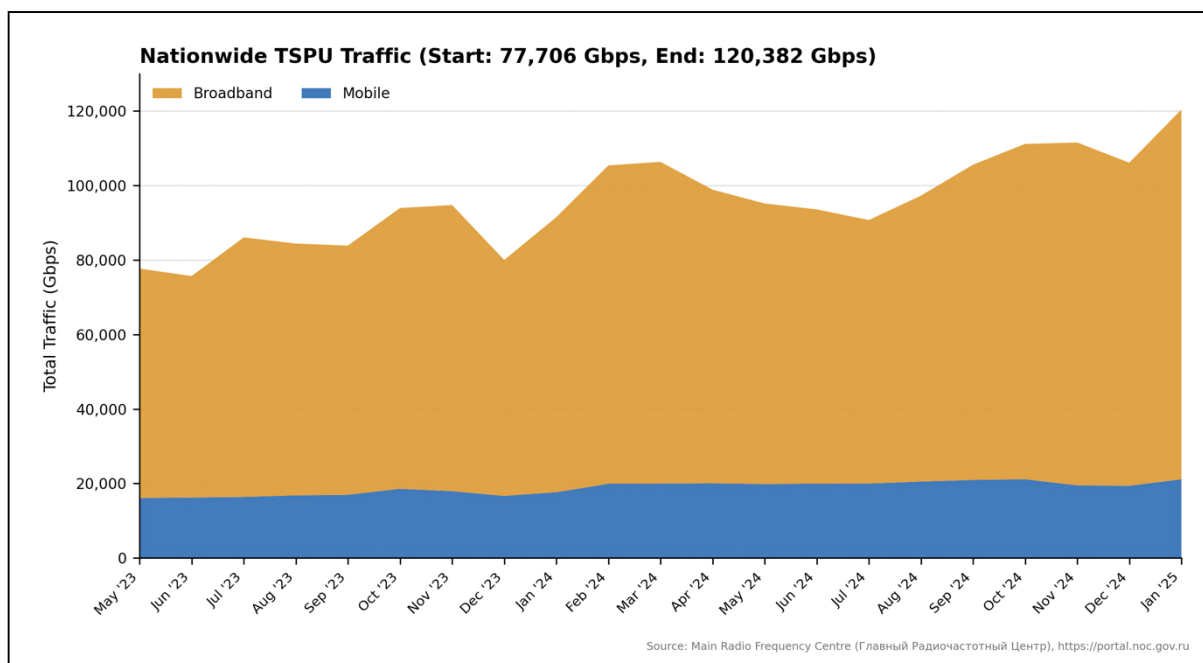


Figure 3: Total TSPU-monitored traffic (broadband and mobile), May 2023 – January 2025. Source: GRFC monthly operational reports.

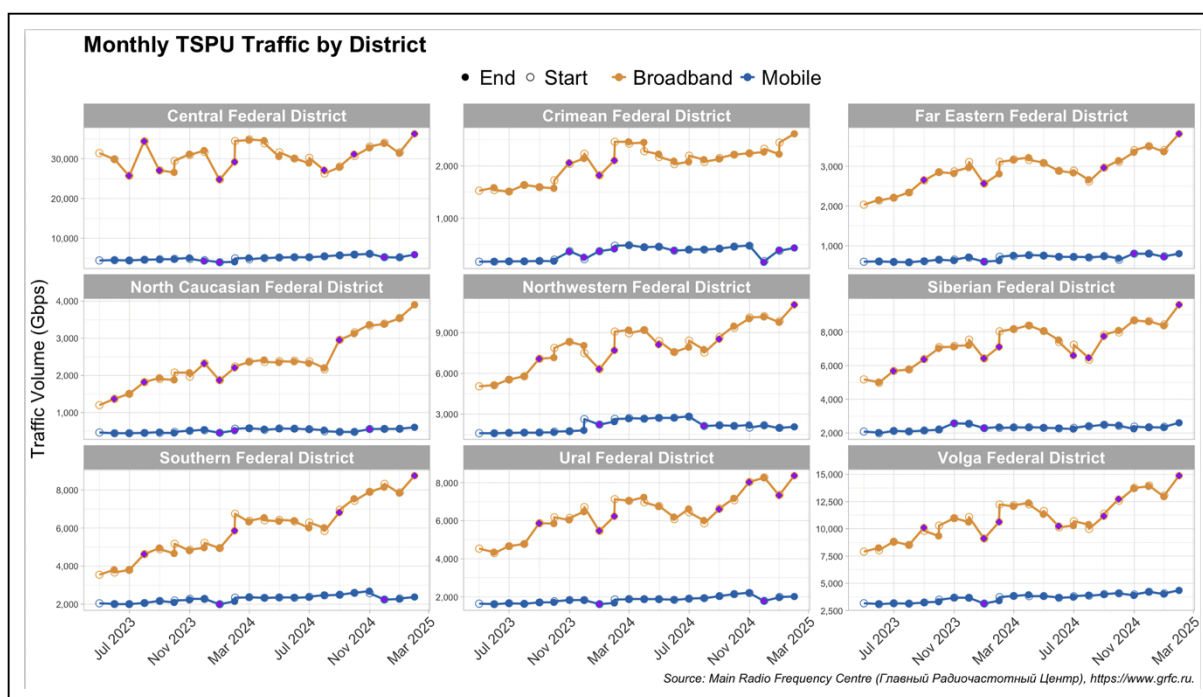


Figure 4: TSPU-monitored traffic by federal district, September 2023 to January 2025. Source: GRFC monthly operational reports.

The public record documents commitments exceeding 100 billion roubles. More than 30 billion roubles was earmarked for 2019–2021, of which 20.8 billion was planned for TSPU. How much was spent has not been reported. A draft federal budget published in September 2021, five months before the invasion, projected a further 31 billion for 2022–2024⁴⁹. TSPU modernisation then received 58.97 billion roubles for 2025–2030, the bulk of a Cybersecurity Infrastructure

federal project initially totalling 68.77 billion⁵⁰. The project total rose by 14.9 billion to 83.7 billion in March 2026, most of it earmarked for capacity and renewal, although no revised TSPU-specific figure was published⁵¹.

An industry estimate reported in 2021 put support, warranty servicing, and operation at 10–15% of initial infrastructure costs. This was not a published annual maintenance budget for TSPU. The source does not specify a time basis sufficient to calculate one⁴⁹.

The Ministry of Digital Development's targets are a capacity increase to 954 Tbit/s by 2030 and the processing of all traffic on the Russian segment of the internet through the national filtering architecture by 2026⁵¹. Successive allocations have given TSPU its own procurement cycles, maintenance contracts, and institutional constituencies.

3.2 Built into markets and institutions

TSPU is not a magic box. The state built it from technologies and firms already active in Russia's commercial network-management market. RDP.RU and VAS Experts were competitive before TSPU was mandated: together they claimed roughly 80% of the Russian network address translation market by 2023³⁹, and VAS Experts counted more than 600 operator clients by 2018⁵². For the TSPU project, GRFC described specifying equipment requirements and guaranteeing manufacturers minimum orders⁵³.

Its account describes a staged localisation: Russian-developed DPI software initially ran on foreign hardware, and a domestic platform replaced it from 2022. In 2024, GRFC said it had ended foreign equipment purchases for its sites, although some replacement products were still being tested. This claim concerned equipment procurement. Imported components remained, with a domestic communications processor then targeted for 2027⁵³. In January 2026, EcoRouter's Nikolai Guzakov still identified high-performance processors and specialised chips as sources of import dependence across Russia's telecommunications industry⁵⁴. These accounts show how domestic supply and support could develop while reliance on foreign components continued. They do not establish that the installed TSPU fleet had become wholly domestic.



Figure 5: “How we survived 2022: 5 stages of import substitution” - Denial, Anger, Bargaining, Depression, Acceptance. Source: Artyom Mikhailov (RDP.RU), KROS 2023.

Each legal instrument added since 2019 has raised the cost of reversal. FZ-90 established the mandate and state provision of equipment. Order No. 228 set technical requirements, while Government Decrees No. 126 and 127 governed transfer, operation, return, and centralised management⁶⁶. Federal Law No. 497-FZ introduced the one million rouble duty for licences carrying interception obligations. Federal Law No. 473-FZ made network compliance an independent licensing condition and basis for revocation⁴². Federal Law No. 33-FZ shielded compliant operators from contractual liability when service failures followed an FSB demand⁵⁵. The framework now spans primary law, government decree, technical orders, taxation, licensing, and operator liability.



Figure 6: TSPU hardware: labelled server rack, EcoSGE DPI manual, and installation at ISP premises. Sources (left to right): CNews, 10 July 2024; RDP.RU; ISP practitioner documentation.

GRFC's role has expanded from frequency monitoring to TSPU operation and industry liaison. Domestic vendors are now organised around specialised TSPU production, while AMOR represents compliance-burdened ISPs in formal dialogue with the state. These arrangements make the system harder to unwind.

Operationally, every licensed ISP must maintain TSPU compliance as a precondition of operation and report infrastructure changes to GRFC within 7 working days, with 90 calendar days' advance notice for reconstruction or liquidation affecting TSPU locations⁵⁶. The reporting infrastructure, training, and inter-organisational workflows are now embedded in standard ISP operations. A service market has grown up around the filings: licensing consultancies submit Order No. 51 returns on operators' behalf as routine work, alongside the other CMU SSOP reports, from 65,000 roubles for a single node, uplink and TSPU⁵⁶. Reversing the system would require dismantling not only the equipment but the procedural ecosystem built around it.

3.3 Expanding functions and entrenchment

TSPU has become harder to reverse as its functions have expanded beyond content filtering. Annual exercises in centralised network management have been conducted since 2019. In 2024, Roskomnadzor described the planned exercise as testing internet operation under different conditions and said ordinary users would not be affected. Users in Dagestan, Chechnya, and Ingushetia nevertheless reported that foreign websites and messengers were unreachable, most VPNs failed, and some local services were disrupted^{10, 57}.

Legal coverage now extends to satellite connectivity. From July 2026, traffic from 5G handsets used in satellite mode must pass through TSPU, while domestic gateway stations must meet SORM requirements⁵⁸. A satellite-industry source considers near-term enforcement against foreign providers such as Starlink unlikely and interprets the rule instead as preparation for Russian operators building or leasing satellite networks⁵⁸. Government Decree No. 1667 replaced the centralised management rules from March 2026 and runs to March 2032⁵⁹. Since August 2024, the Prosecutor General or a deputy has also been able to require Roskomnadzor to act on the public network through TSPU⁶⁰.

The filtering infrastructure now supports a wider data-collection system. Roskomnadzor Order No. 51 requires ISPs to report subscriber IP addresses, the municipality where they are used, and the identifiers of the TSPU through which the traffic passes, including upstream equipment⁶¹, ⁶². Roskomnadzor estimated the industry's annual compliance cost at 389 million roubles across 1,981 operators. MTS objected that the data is protected as communication secrecy and that it could not price compliance at all⁶³.

9. Формат передаваемой информации, предусмотренной подпунктом «г» пункта 2 настоящего Порядка, должен соответствовать следующим требованиям:

а) поле данных выделяется следующими символами «{ }» (фигурные скобки и запятая);

б) информация предоставляется при помощи программного приложения и имеет вид «{ID}, {TTL}, {xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xx}, {xxx.xxx.xxx.xxx}, {Operation}, {Timestamp}, {x...x}», где:

ID – уникальный идентификатор пользовательского оборудования (оконечного оборудования);

TTL – срок использования протоколов в формате IPv4 и IPv6 (количество знаков определяется оператором связи в зависимости от срока использования протоколов в формате IPv4 и IPv6, измеряемого в минутах и состоящего из положительных целых чисел);

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xx – выделенный сетевой адрес в соответствии с протоколом в формате IPv6;

xxx.xxx.xxx.xxx/xx – выделенный сетевой адрес в соответствии с протоколом в формате IPv4;

Operation – операция, положительное целое число, где:

0 – окончание использования протоколов в формате IPv4 и IPv6;

1 – начало использования протоколов в формате IPv4 и IPv6;

2 – продление использования протоколов в формате IPv4 и IPv6;

Timestamp – время создания записи оператором связи (количество миллисекунд, прошедших с полуночи 1 января 1970 года), целое число.

x...x – целые положительные числа, обозначающие уникальные номера технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети «Интернет» и сети связи общего пользования, на которые осуществляется пропуск трафика пользователя услугами связи.

Figure 7: The reporting format proposed in Roskomnadzor's December 2024 draft: user-equipment identifier, TTL, IPv6 and IPv4 addresses, operation code, timestamp and TSPU serial numbers. The final Order No. 51 does not include the user-equipment identifier. Source: RKN.⁶²

Separate anti-fraud amendments require ISPs to provide subscriber identity data to the FSB and Ministry of Internal Affairs within 24 hours of a request, without notifying subscribers⁶⁴. One regime maps where users are on the network. The other identifies who they are. RDP.RU's EcoFilter product line also advertises the ability to export HTTP GET requests, which can expose the unencrypted pages a subscriber visits. Which functions are enabled on deployed TSPU equipment is not public⁶⁵.

Expansion into network security creates structural lock-in because removing TSPU would also mean losing security functions. The National Anti-DDoS System (NSPA), operational since March 2024, uses 88 TSPU devices handling cross-border traffic—the 'transborder' segment—as its first echelon of attack filtering⁶⁶. In 2025, Roskomnadzor recorded more than 21,000 DDoS incidents, more than double the previous year⁶⁷. The 465 million rouble Security Scanner, contracted to GRFC in 2023, identified 26,000 critical vulnerabilities across more than 300 Russian companies while still in test operation. Roskomnadzor says services exposing unremediated vulnerabilities can be blocked at TSPU level⁶⁸.

By 2024, GRFC was offering these functions to operators. At KROS, a representative described an interface that would let DDoS providers and large infrastructure owners apply seven countermeasures to declared IP ranges in the cross-border segment⁶⁹. Operators once resisting the black box were now invited to use it. Federal Law No. 33-FZ also releases operators from contractual liability when service failures follow an FSB shutdown demand⁵⁵. TSPU is becoming shared infrastructure for administration, surveillance, security, and censorship.

4. Why This Matters Beyond Russia

Russia's significance lies in how ordinary commercial capabilities are owned, coordinated, and governed. The technology is widely available, filtering effects cross borders, and the institutional model is replicable.

4.1 Ordinary technology, different governance

DPI is embedded in global telecommunications standards, vendor products, and network architectures. The International Telecommunication Union's standardisation body (ITU-T) has specified requirements for DPI in next-generation networks (Y.2770, 2012), performance models and metrics (Y.2773, 2017)⁷⁰, and an architecture extending into software-defined networking, virtualisation,

and 5G (Y.2775, 2019)⁷¹. These recommendations describe particular applications of DPI as network functions. Whether inspection is used for congestion management or population-scale censorship is a governance choice.

9	DPI functional architecture for service function chaining and DPI as a service	15
9.1	Overview of service function chaining.....	15
9.2	Introduction of DPI as a service	16
9.3	DPI functional architecture for DPaaS in service function chaining	16
9.4	DPI functional architecture for extended DPI as a service.....	17
10	DPI functional architecture in network virtualization environment	18
10.1	Overview of network virtualization.....	18
10.2	DPI functional architecture for network virtualization	19

6.8 Inspection of encrypted traffic There is a common view that DPI signatures can be applied only to unencrypted traffic. Nevertheless, DPI signatures could be applicable to encrypted traffic depending on: • the level of encryption (see clause 6.8.1) • local availability of the decryption key (see clause 6.8.2) • inspection conditions based on encrypted information (see clause 6.8.3). 6.8.1 Extent of encryption Any 'packet' as protocol data unit (PDU) consists of protocol control information (PCI) and service data units (SDU) at various protocol layers. When encryption is applied on the inspected communication path, then encryption may be applied:	International Telecommunication Union ITU-T TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU Y.2775 (08/2019) SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES Next Generation Networks – Security Functional architecture of deep packet inspection for future networks Recommendation ITU-T Y.2775 
---	---

Figure 8: ITU-T Recommendation Y.2775 (2019): table of contents, cover page, and section on encrypted traffic inspection. DPI was formalised as a standard network function years before FZ-90. Source: ITU-T.

DPI is sold globally for traffic management, network optimisation, and “quality-of-service” differentiation by Cisco, Nokia, Ericsson, Allot, Sandvine, and others. VAS Experts’ commercial overview describes 800+ installations across Russia and the CIS as of 2019, with export markets in Lebanon, Cyprus, Turkey, and Moldova⁷². RDP.RU’s EcoFilter product sheet advertises the same product line that constitutes TSPU hardware, sold as standard network equipment⁶⁵.

Bendrath and Mueller documented this convergence a decade before TSPU: the same DPI equipment serves traffic management, copyright enforcement, lawful interception, and content filtering across jurisdictions^{73, 74}. Comparable inspection capabilities appear in communications and interception systems in the United Kingdom, United States, India, and elsewhere. Russia’s distinctive feature is the state’s centralised control over where DPI is deployed, how it is commanded, and what legal constraints apply.

Lawful-interception requirements are also embedded in 3GPP 5G standards⁷⁵. In Russia, however, the state owns and centrally operates filtering hardware inside private networks, makes compliance a licensing condition, and uses the system for population-scale content filtering rather than targeted interception.

Government decree, not the operator, determines when traffic may bypass the equipment. The FSB separately verifies lawful-interception compliance.

The Russian segment remains connected to the global network. At the 2024 KROS international roundtable, operators reported that international traffic was growing, not declining⁷⁶. As one participant put it: “We can only reorient eastward when at least 50% of people know Chinese... The internet lives by language zones”⁷⁶. TSPU exercises control across a network that remains interoperable.

4.2 Cross-border effects

Measurement research (Ortwein et al. 2023) scanned IP address spaces of 18 countries surrounding Russia and documented Russian-origin DPI filtering affecting users in at least 8 countries, traced to at least 6 Russian autonomous systems⁷⁷. Two of those systems were running commercial DPI bought from VAS Experts rather than state-owned TSPU: the filtering crosses the border either way, but the equipment behind it is not always the state’s⁷⁷. For ISPs in neighbouring states whose upstream paths cross Russian backbone infrastructure, an inline filtering device need not appear as a separate hop in standard route diagnostics⁷⁷. Any country whose internet traffic transits a state with deployed DPI filtering is potentially subject to collateral censorship, regardless of its own domestic policies.



Figure 9: Fibre routes from Russia through the Urals to Kazakhstan, Kyrgyzstan, Tajikistan, and Afghanistan. Traffic transiting these routes crosses Russian networks subject to TSPU and to operator-purchased commercial DPI, exposing neighbouring states to Russian filtering rules. Source: Habr, “Пытаюсь представить жизнь при суверенном интернете в России.”

4.3 A replicable model

The cross-border effects are a consequence of network topology. The transferability of the model is institutional. Unlike China's Great Firewall, TSPU did not require a purpose-built network. It shows that centralised filtering can be constructed at national scale on a heterogeneous network through sustained political commitment and staged regulation. Many countries' networks look more like Russia's than China's.

Several Commonwealth of Independent States (CIS) members operate similar filtering capabilities, shaped by domestic demand as well as Russian vendor presence. At the 2023 Multiservice Forum, a VAS Experts representative described regulators, including in Uzbekistan, asking to "block links inside HTTPS"⁷⁸. Chinese vendors such as Geedge Networks sell similar systems in Kazakhstan, Ethiopia, Pakistan, and Myanmar⁷⁹. Russian vendors report active markets across the CIS, Middle East, India, Africa, Southeast Asia, and Latin America⁸⁰, ⁷⁶. These examples show multiple pathways: domestic demand, commercial substitution, and cross-border vendor sales.

The replicability risk lies in this institutional model. TSPU demonstrates a sequence: map a heterogeneous network, install centrally controlled inspection, make compliance a condition of operation, and sustain the system through vendors and public institutions. The technology is already embedded in networks worldwide. What the model adds is political and administrative coordination.

5. What Civil Society Can Do

The system was assembled through coordination across state agencies, domestic industry, and regulatory instruments reaching global platforms. Civil society responses must match that breadth through sustained engagement with standards governance, export-control policy, compliance documentation, and measurement infrastructure.

5.1 Standards governance

DPI is normalised in ITU standards as a core network capability⁸¹. Treating population-scale filtering as ordinary network management makes it easier for states to adopt. Lawful interception requirements are already embedded in 5G standards⁷⁵. ITU-T Study Group 13 handles the DPI recommendations (Y.2770 and successors) that normalise the technology TSPU is built on. The 3rd Generation Partnership Project's security group (3GPP SA3) defines the lawful-inter-

ception architecture for 5G networks. The ITU-T recommendations build on protocols defined by the Internet Engineering Task Force (IETF), so protocol-design decisions there affect what DPI can inspect. The IETF's TLS working group developed Encrypted Client Hello (ECH), standardised as RFC 9849 in March 2026, which encrypts information TSPU uses for selective filtering^{20, 82}. Civil society can engage directly in the IETF⁸³, but influencing ITU-T and 3GPP generally requires institutional membership or partnerships with organisations already inside those processes^{84, 85}. Across these forums, civil-society engagement should address how standardised network functions provide capacity for population-scale control and what governance safeguards that capacity requires.

5.2 Export controls and procurement accountability

Export controls targeting named companies miss the structural risk. When Sandvine withdrew from more than 50 markets in 2024, one Middle Eastern operator replaced its platform with functionally compatible VAS Experts equipment⁸⁶. Commercial compatibility allows one supplier to take another's place. Effective controls therefore require transparency in DPI procurement, human rights impact assessments for interception-equipment exports, and accountability mechanisms that survive vendor substitution.

5.3 Independent measurement and early warning

Independent measurement (OONI, Censored Planet, and specialised tools) is the primary accountability mechanism for internet filtering worldwide⁸⁷. Russia's ban on circumvention information (March 2024) specifically targets the knowledge infrastructure that enables informed measurement and resistance¹⁵. The information ban makes documentation harder from inside Russia. External measurement networks become correspondingly more important.

Other governments can replicate the regulatory sequence even when they use different products. Tracking regulatory steps may therefore provide earlier warning than tracking vendor sales. Indicators include network-topology disclosure requirements, mandatory encrypted-traffic inspection, filtering as a licensing condition, and approved-access architectures. Russia's access list draws banking, payments, and other essential services into the same compliance regime as communications. Where approved-service lists replace open-by-default networks, this logic can spread beyond communications into other sectors. Filtering objectives have repeatedly prevailed when they conflicted with commercial interests. Economic costs should not be expected to limit the system.

—

Notes

- 01** Xue, D., et al. (2022). 'TSPU: Russia's decentralized censorship system'. Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22). <https://dl.acm.org/doi/10.1145/3517745.3561461> (archived)
- 02** Government Decree No. 127, 'On Approval of Rules for Centralised Management of the Public Communications Network' (in Russian), 12 February 2020. <http://publication.pravo.gov.ru/Document/View/0001202002170013> (archived)
- 03** GRFC and DCOA (Data Centre for Data Processing and Automation), contract no. 000 000 000 9619 P01 0002/№ 3, 24 March 2020 (in Russian). Procurement documentation; no public URL.
- 04** Ermoshina, K. and Musiani, F. (2017). 'Migrating servers, elusive users: Reconfigurations of the Russian internet in the post-Snowden era'. *Media and Communication*, 5(1), 42–53. <https://doi.org/10.17645/mac.v5i1.816> (archived) On selective and simulated compliance: Ermoshina, K., Loveluck, B. and Musiani, F. (2022), 'A market of black boxes', *Journal of Information Technology & Politics*, 19(1), 18–33, at p. 27. See also Ermoshina and Musiani (2021), 'Networked craftiness: how internet service providers resist "by infrastructure" in Russia', *Quaderni* 103, 53–70.
- 05** KROS 2019 roundtable, 'The Splendour and Misery of the Sovereign Runet' (in Russian). Video, https://www.youtube.com/watch?v=3GcDoQ4wq_Y (archived)
- 06** Federal Law No. 126-FZ art. 65.1(3), which provides the equipment free of charge, and Government Decree No. 126, 'On Approval of Rules for the Installation, Operation and Modernisation of Technical Means of Countering Threats' (in Russian), 12 February 2020, which supplies transfer, return and the reporting deadlines. https://portal.noc.gov.ru/documents/49/Постановление_Правительства_РФ_от_12_02_2020_N_126_p2W1A4X.docx (archived)
- 07** Shakhmetova, O., 'Overview of Legislative Changes' (in Russian), MUSE 2023. Video, <https://www.youtube.com/watch?v=cZQob6Yw3vo> (archived)
- 08** Cableman.ru, 'Roskomnadzor blocked 50% more resources in 2025' (in Russian), 24 October 2025. <https://www.cableman.ru/content/kolichestvo-zablokirovannykh-roskomnadzorom-resursov-vyroslo-na-50-v-2025-godu> (archived)
- 09** Cableman.ru, 'Roskomnadzor has restricted access to 469 VPN services' (in Russian), 26 February 2026. <https://www.cableman.ru/content/roskomnadzor-ogranichil-dostup-k-469-vpn-servisam> (archived) For the October 2023 count, cumulative since 2021: Interfax (in Russian), 25 October 2023. <https://www.interfax.ru/russia/927461> (archived) On protocol-level blocking: Roskomsvoboda, 'VPN in Russia: from blocking services to blocking protocols', October 2023. <https://roskomsvoboda.org/ru/analysis/vpn-russia-2023-eng/> (archived)
- 10** Human Rights Watch, 'Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia', 30 July 2025, 70pp. <https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation> (archived) VPN figures p. 21; licences and ISP counts pp. 26–27; exercises p. 37; shut-downs p. 51.
- 11** ComNews, 'Roskomnadzor to begin restricting Telegram' (in Russian), 10 February 2026. <https://www.comnews.ru/content/243744/2026-02-10/2026-w07/1009/roskomnadzor-nachnet-ogranichenie-raboty-telegram> (archived)
- 12** Habr, 'Senator Sheikin: restrictions on Telegram are being introduced step by step, hence the trouble loading video' (in Russian), 21 January 2026. <https://habr.com/ru/news/987526/> (archived)

- 13** Teplitsa of Social Technologies, 'What is happening with DNS in Russia? We may have found signs of censorship. Analysis no. 26' (in Russian), 7 August 2026, updated 31 August 2026. <https://te-st.org/2026/08/07/dnsdnsdns/> (archived)
- 14** ComNews, 'Algorithmic exercises: RKN to filter traffic using machine learning' (in Russian), 19 January 2026. <https://www.comnews.ru/content/243319/2026-01-19/2026-w04/1009/algoritmicheskie-uprazhneniya-rkn-budet-filtrovat-trafik-pomoschyu-mashinnogo-obucheniya> (archived)
- 15** Habr (Xeovo corporate blog), 'The ban on articles about Tor and VPN takes effect' (in Russian), March 2024. <https://habr.com/ru/companies/xevo/articles/797463/> (archived)
- 16** Meduza, 'Can all VPNs really be blocked? Meduza asked the biggest VPN services how they hold out against Roskomnadzor' (in Russian), 3 April 2026. <https://meduza.io/feature/2026/04/03/mozhno-li-deystvitelno-zablokirovat-vse-vpn> (archived)
- 17** Mastercard, 'Mastercard statement on suspension of Russian operations', 5 March 2022, clarification added 6 March 2022. <https://www.mastercard.com/news/press/2022/march/mastercard-statement-on-suspension-of-russian-operations> (archived)
- 18** Habr, 'Russian operators disable Apple ID top-ups from mobile phones' (in Russian), 1 April 2026. <https://habr.com/ru/news/1017762/> (archived)
- 19** Meduza, "Theoretically they can block any service entirely": an interview with a developer of Amnezia VPN' (in Russian), 3 August 2026. <https://meduza.io/feature/2026/08/03/teoreticheski-oni-mogut-zablokirovat-lyuboy-servis-tselikom> (archived) See also Amnezia, 'How VPNs are blocked in Russia and what to do if Amnezia VPN won't connect' (in Russian), 16 July 2026. <https://amnezia.org/ru/blog/amnezia-vpn-no-connection-what-to-do> (archived)
- 20** RBC (in Russian), 7 November 2024. https://www.rbc.ru/technology_and_media/07/11/2024/672cc8079a7947318949ba7d (archived) Relayed verbatim by Habr (denis-19), 8 November 2024. The recommendation was issued by ЦМЭ ЦСОП on 7 November 2024 and published at portal.noc.gov.ru. The 44% and 11% are a market estimate by Evgeny Martynov, IT director of RU-CENTER.
- 21** Habr, 'RKN advises Russian site owners to drop Cloudflare's TLS ECH extension' (in Russian), 2 April 2025. <https://habr.com/ru/news/896920/> (archived) On the ORI registration: Habr, 'Roskomnadzor forcibly enters Cloudflare in the register of organisers of dissemination of information' (in Russian), 20 February 2025. <https://habr.com/ru/news/884710/> (archived)
- 22** Habr, 'RKN advises Russian site owners to drop Cloudflare's TLS ECH extension' (in Russian), 2 April 2025. <https://habr.com/ru/news/896920/> (archived)
- 23** Habr, 'Cloudflare explains how traffic to its networks is restricted in Russia' (in Russian), 27 June 2025. <https://habr.com/ru/news/922532/> (archived)
- 24** Niere, N., Lange, F., Heitmann, N., and Somorovsky, J. (2025). 'Encrypted Client Hello (ECH) in Censorship Circumvention'. Free and Open Communications on the Internet, 2025(2), 64–73, especially §5 and Appendix A. <https://petsymposium.org/foci/2025/foci-2025-0016.pdf> (archived)
- 25** Roskomsvoboda, 'VPN in Russia: from blocking services to blocking protocols' (in English), October 2023. <https://roskomsvoboda.org/ru/analysis/vpn-russia-2023-eng/> (archived)
- 26** Habr, '75,000 entries added to the "white list" of IP addresses using foreign encryption protocols' (in Russian), 17 April 2025. <https://habr.com/ru/news/901584/> (archived) The 12,000 is RKN head Andrei Lipov's figure of October 2023, the 75,000 RKN's own, of 16 April 2025.
- 27** ComNews, 'A forced measure: what is happening with mobile-internet shutdowns' (in Russian), 12 November 2025. <https://www.comnews.ru/content/242284/2025-11-12/2025-w46/1009/vynuzhdennaya-mera-cto-proiskhodit-otklyucheniem-mobilnogo-interneta> (archived)
- 28** Belkova, E. and Rozhkov, R., 'Russia to get a list of services available during mobile-internet blocks' (in Russian), Forbes Russia, 7 August 2025. <https://www.forbes.ru/tekhnologii/>

543521-v-rossii-poavitsa-spisok-servisov-dostupnyh-v-period-blokirovki-mobil-nogo-internet (archived)

- 29** Cableman.ru, 'Mobile internet temporarily shut off in Belgorod Oblast to secure air-defence operations' (in Russian), 28 November 2025, reporting Kommersant. <https://www.cableman.ru/content/v-belgorodskoi-oblasti-vremenno-otklyuchili-mobilnyi-internet-dlya-obespecheniya> (archived)
- 30** Cableman.ru, 'The Ministry of Digital Development expands the list of sites available during internet shutdowns' (in Russian), 17 November 2025. <https://www.cableman.ru/content/mintsi-fry-rasshirilo-spisok-saitov-dostupnykh-pri-otklyucheniakh-interneta> (archived) October 2025 baseline: Cableman.ru, 17 October 2025. The 500-entry total and the April tranche: Cableman.ru, relaying Kommersant, 24 April 2026, <https://www.cableman.ru/content/perechen-dostupnykh-onlain-servisov-v-belom-spiske-rasshiren-do-500-pozitsii> (archived) and RBC, 23 April 2026. The FSB veto over bank apps without SORM: Anti-Malware.ru, 4 February 2026, <https://www.anti-malware.ru/news/2026-02-04-111332/48928> (archived) The requirement set and the 2027 deadline: Frank Media, 26 February 2026, relaying Izvestia. <https://frankmedia.ru/263929>
- 31** Meduza, "'Durov's Code': Rostov-on-Don is testing a 'white list' on home internet" (in Russian), 31 March 2026. <https://meduza.io/news/2026/03/31/kod-durova-v-rostove-na-donu-testiruyut-belyy-spisok-na-domashnem-internete> (archived)
- 32** Internet Society Pulse, 'Country Report: Russia', 2026 data. <https://pulse.internetsociety.org/en/reports/RU/> (archived)
- 33** Vasiliev, P., 'Installing TSPU' (in Russian), pavel.su blog, 12 December 2022. <https://pavel.su/internet/setting-up-tspu/> (archived)
- 34** Vasiliev, P., 'TSPU: A Year in Operation' (in Russian), pavel.su blog, 18 August 2023, section 'Can I remove my own TSPU?'. <https://pavel.su/internet/tspu-1-year/> (archived)
- 35** Habr, 'Yaroslavl provider Yarnet reveals how RKN's TSPU behaves during an outage on the operator's network' (in Russian), 17 November 2023. <https://habr.com/ru/news/774734/> (archived)
- 36** Ermoshina, K., Loveluck, B. and Musiani, F. (2022). 'A market of black boxes: The political economy of Internet surveillance and censorship in Russia'. *Journal of Information Technology & Politics*, 19(1), 18–33. <https://doi.org/10.1080/19331681.2021.1905972> (archived) Their black boxes are SORM and blacklist filtering, not TSPU.
- 37** Vedomosti, 'Major outage hits Runet services' (in Russian), 14 January 2025, for the duration and Roskomnadzor's restoration time of 18:08 Moscow time. <https://www.vedomosti.ru/technology/articles/2025/01/14/1086185-runeta-masshtabnii-sboi> (archived) The ~11% is read from MSK-IX's published traffic graph, <https://www.msk-ix.ru/traffic/> (archived), as reproduced by Habr the same day, <https://habr.com/ru/news/873606/> (archived) and <https://habr.com/ru/news/873630/> (archived).
- 38** The 10–25% is from the KROS 2022 roundtable 'SORM through the Manufacturers' Eyes' (in Russian), and is given for SORM equipment and components. On crisis management: Galushko, D., 'Rules for Surviving an Age of Change' (in Russian), KROS 2022. Video, <https://www.youtube.com/watch?v=HVzhVR9DoS0> (archived)
- 39** Mikhailov, A., 'RDP: Yesterday, Today and Tomorrow' (in Russian), KROS 2023. Video, <https://www.youtube.com/watch?v=5qveqUP9Daw> (archived)
- 40** Abramovskaya, T., 'Risk Analysis and Forms of Liability under the Regulations: SORM and TSPU' (in Russian), MUSE 2023. Video, <https://www.youtube.com/watch?v=QyYnbkrXnKQ> (archived) The TSPU scale and the criminal provision are Roskomnadzor's own, 'Operators' refusal to use TSPU is a threat to citizens' (in Russian), 20 July 2022, <https://43.rkn.gov.ru/news/news-329104.htm> (archived), citing art. 13.42.1 of the Code of Administrative Offences. The Tinko case: Cableman.ru, 25 March 2026. <https://www.cableman.ru/content/provaidera-iz-sankt-peterburga-oshtrafovali-za-obkhod-blokirovki-youtube> (archived)

- 41** ComNews, ‘Beeline adds the option of watching YouTube without a VPN for its subscribers’ (in Russian), 21 January 2026. <https://www.comnews.ru/content/243370/2026-01-21/2026-w04/1009/bilayn-dobavil-vozmozhnost-smotret-youtube-bez-vpn-dlya-svoikh-abonentov> (archived)
- 42** Two instruments. Federal Law No. 497-FZ, 28 September 2023, effective 1 January 2024, is the tax-code amendment setting the 1,000,000-rouble duty on the *grant* of a licence. Renewals remain 7,500. <http://publication.pravo.gov.ru/Document/View/0001202309280013> (archived) The licensing condition and the revocation grounds come from Federal Law No. 473-FZ, 4 August 2023, in force 1 December 2024.
- 43** Association of Small Operators (AMOR), founded 15 August 2023; the cited page has since been withdrawn and is archived at <https://web.archive.org/web/20240421184107/https://a-mor.ru/articles/god-gryadushhij/> On TSPU specifically: D-Russia, ‘On the schemes for passing traffic through TSPU – GRFC’ (in Russian), 16 February 2024. <https://d-russia.ru/o-shemah-propuska-trafika-cherez-tspu-grhc.html> (archived)
- 44** Kazakova, E., ‘Telecom Trends: Infrastructure, Service Development, M&A’ (in Russian), KROS 2023. Video, <https://www.youtube.com/watch?v=LumiErgXV0s> (archived)
- 45** Kazakova, E., ‘What if We Leave Everything as It Is? Market Trends in the Industry’s Realities’ (in Russian), KROS 2024. Video, https://www.youtube.com/watch?v=_MPNflvcyRk (archived)
- 46** Pandya, K., ‘737 Chrome VPN Extensions Linked to Brand Impersonation and Browser Traffic Re-direction’, Socket, 11 August 2026. <https://socket.dev/blog/chrome-vpn-extension-impersonation> (archived)
- 47** For the 2022 node counts: GRFC portal, ‘Address by ЦМЭ ССОП director Sergei Khutortsev to the Spektr-2022 forum’ (in Russian), 26 October 2022. <https://portal.noc.gov.ru/ru/news/2022/10/26/vystuplenie-direktora-cmu-ssop-sergeya-hutorceva-na-forume-spektr2022/> (archived) For the 2023 figures: ЦМЭ ССОП portal, ‘Spektr-2023: information security and tools for fighting cyberthreats’ (in Russian), 25 October 2023.
- 48** GRFC monthly reports, April 2023 – January 2025, plus annual reports for 2023 and 2024 (in Russian); the monthly traffic series is extracted from these for May 2023 – January 2025. Individual issues at <https://portal.noc.gov.ru/documents/> (archived)
- 49** Habr, ‘Sovereign Runet spending for 2022–2024 estimated at 31 billion roubles’ (in Russian), 23 September 2021. <https://habr.com/ru/news/579620/> (archived)
- 50** Gavrilyuk, A., ‘RKN casts a new net: 59 billion roubles to overhaul the site-blocking system’ (in Russian), Forbes Russia, 10 September 2024. <https://www.forbes.ru/tekhnologii/520876-rkn-pletet-novye-seti-sluzba-obnovit-sistemu-blokirovki-sajtov-za-59-mlrd-rublej> (archived)
- 51** Habr, ‘Ministry of Digital Development plans to raise TSPU capacity to 954 Tbit/s by 2030’ (in Russian), 25 March 2026. <https://habr.com/ru/news/1014590/> (archived)
- 52** Moldavanov, D., ‘Building the Network of Your Dreams on SKAT Core: BRAS + DPI + NAT + BGP’ (in Russian), KROS 2018. Video, <https://www.youtube.com/watch?v=dySZBEVe2oE> (archived)
- 53** Tyomny, S. (GRFC), interviewed in ‘Roskomnadzor reports full import substitution of TSPU equipment’ (in Russian), Rossiyskaya Gazeta, 3 June 2024. <https://rg.ru/2024/05/31/v-roskomnadzore-rasskazali-o-polnom-importozameshchenii-oborudovaniia-tspu.html> (archived)
- 54** Guzakov, N. (EcoRouter), ‘Russian telecom equipment has reached critical parts of the infrastructure’ (in Russian), TAdviser, 22 January 2026. https://www.tadviser.ru/index.php/Статья:Николай_Гузаков,_EcoRouter:_Российское_телеком-оборудование_вышло_на_критические_участки_инфраструктуры (archived)
- 55** Federal Law No. 33-FZ, ‘On Amendments to Articles 46 and 68 of the Federal Law On Communications’ (in Russian), 20 February 2026. <http://publication.pravo.gov.ru/document/0001202602200054> (archived) Operators must suspend services upon FSB demand. Art. 68 cl. 6.1 removes operator liability for service disruptions caused by compliance with FSB requirements.

- 56** Telecomika, ‘Submission of Information under Roskomnadzor Order No. 51’ (in Russian), service page of a Moscow licensing and regulatory consultancy, consulted 10 August 2026. https://www.telecomika.ru/prikaz_51_roskomnadzora_o_sredstvakh_svyazi (archived)
- 57** Habr, ‘Exercises to “switch off the international internet” expected in Russia in December 2024’ (in Russian, updated), 14 November 2024. <https://habr.com/ru/news/858608/> (archived)
- 58** Order of the Ministry of Digital Development No. 219, 16 March 2026, in force 6 July 2026, amending the Requirements approved by Order No. 1080 of 13 December 2023. Draft and industry assessment reported by Krechetova, A., Forbes Russia (in Russian), 11 August 2025. <https://www.forbes.ru/tekhnologii/543650-minicifry-obazet-sputnikovyh-operatorov-oborudovat-nazemnye-stancii-sorm-i-tpsu> (archived)
- 59** Government Decree No. 1667 of 27 October 2025, ‘On Approval of the Rules for Centralised Management of the Public Communications Network’ (in Russian), published 6 November 2025, in force 1 March 2026 to 1 March 2032, repealing Decree No. 127 of 12 February 2020. <http://publication.pravo.gov.ru/document/0001202511060014> (archived)
- 60** Federal Law No. 216-FZ, 8 August 2024, art. 2(3), inserting art. 65.2 into Federal Law No. 126-FZ; in force on official publication. <http://www.kremlin.ru/acts/bank/50951> (archived)
- 61** Habr, ‘A procedure is set for operators to supply RKN with data identifying user equipment’ (in Russian), 2 April 2025. <https://habr.com/ru/news/896832/> (archived)
- 62** Roskomnadzor Order No. 51 of 28 February 2025, made under Federal Law No. 126-FZ art. 46, cl. 5.2-1 (inserted by Federal Law No. 216-FZ of 8 August 2024); registered with the Ministry of Justice 31 March 2025, reg. no. 81700, in force 12 April 2025. Draft consultation record (in Russian): <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=153276> (archived) Official publication (in Russian): <https://rg.ru/documents/2025/04/02/roskomnadzor-prikaz51-site-dok.html> (archived) Approved procedure, paras 1–7: https://www.consultant.ru/document/cons_doc_LAW_502246/3d5e08a9395f55c7d31c51fbd8265c1dde64cb86/ (archived)
- 63** Habr, ‘MTS warns of communication-secrecy risks in RKN’s plan to collect user-equipment IP addresses’ (in Russian), 19 February 2025, reporting RBC. <https://habr.com/ru/news/883806/> (archived)
- 64** Gavriluk, A., ‘Handing over the data: what subscriber information operators will give police directly’ (in Russian), Forbes Russia, 6 May 2025. <https://www.forbes.ru/tekhnologii/536706-dannye-na-sdachu-kakuu-informaciu-ob-abonentah-operatorov-peredadut-policii-napravim> (archived)
- 65** RDP.RU, ‘EcoFILTER: Functional URL-Filtering’, product sheet (in English), 2 pp., undated; file creation date 30 May 2017. GET-request extraction, p. 2. Company document.
- 66** Cableman.ru, ‘Roskomnadzor plans to scale up the National Anti-DDoS System to defend against internal threats’ (in Russian), 28 October 2025, relaying Kommersant (kommersant.ru/doc/8159639). <https://www.cableman.ru/content/roskomnadzor-planiruet-masshtabirovat-natsionalnuyu-sistemu-protivodeistviya-ddos-atakam> (archived) The 88 transborder devices are Oleg Diyansky, head of GRFC’s cyberthreat-protection centre, at the Spektr-2025 forum.
- 67** Cableman.ru, ‘Roskomnadzor: DDoS attacks more than doubled in 2025’ (in Russian), 19 January 2026, relaying Kommersant. <https://www.cableman.ru/content/roskomnadzor-v-2025-godu-chislo-ddos-atak-velichilos-bolee-chem-vdvoe> (archived)
- 68** Habr, ‘RKN’s “Security Scanner” found 26,000 critical vulnerabilities in the networks of 300 Russian companies in 2024’ (in Russian), 25 October 2024, reporting Khutortsev at the Spektr-2024 forum the previous day. <https://habr.com/ru/news/853330/> (archived)
- 69** Smirnov, V. (GRFC), ‘Developing Measures to Counter Threats to Communications-Network Security’ (in Russian), KROS 2024. Video, <https://www.youtube.com/playlist?list=PLKzXMzX502jEC-SBeePir4NsegcDnb6Bow> (archived)

- 70** ITU-T, Recommendation Y.2773, 'Performance models and metrics for deep packet inspection', February 2017. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2773-201702-!!!PDF-E&type=items (archived)
- 71** ITU-T, Recommendation Y.2775, 'Functional architecture of deep packet inspection for future networks', August 2019. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2775-201908-!!!PDF-E&type=items (archived)
- 72** VAS Experts, 'DPI BRAS CG-NAT Overview' (in Russian), company deck, 2019. On market consolidation: VAS Experts blog (in Russian), 9 April 2020. <https://vasexperts.ru/blog/telekom/po-gloshheniya-na-rossijskom-rynke-dpi-reshenij/> (archived)
- 73** Bendrath, R. and Mueller, M. (2011). 'The end of the net as we know it? Deep packet inspection and internet governance'. *New Media & Society*, 13(7), 1142–1160. <https://doi.org/10.1177/1461444811398031> (archived)
- 74** Bendrath, R. (2009). 'Global technology trends and national regulation: Explaining variation in the governance of deep packet inspection'. Paper presented at the International Studies Association annual convention. https://ralf-bendrath.eu/ISA09_Paper_Ralf%20Bendrath_DPI.pdf (archived)
- 75** Becker, C., ten Oever, N. and Nanni, R. (2024). 'Interrogating the standardisation of surveillance in 5G amid US–China competition'. *Information, Communication & Society*. <https://doi.org/10.1080/1369118x.2024.2302991> (archived)
- 76** KROS 2024 roundtable, 'International Problems and Opportunities for Russian Telecoms Today' (in Russian). Video, <https://www.youtube.com/watch?v=WghTLMrw0j4> (archived)
- 77** Ortwein, A., Bock, K. and Levin, D. (2023). 'Towards a Comprehensive Understanding of Russian Transit Censorship'. *Free and Open Communications on the Internet (FOCI 2023)*. <https://www.petsymposium.org/foci/2023/foci-2023-0012.php> (archived)
- 78** Sapunov, I., 'The SKAT Universal Service Gateway: Import Substitution in Practice' (in Russian), MUSE 2023. Video, <https://www.youtube.com/watch?v=orEtg9jFePs> (archived)
- 79** InterSecLab, 'The Internet Coup' (2025). Investigation of the Geedge Networks document leak. <https://interseclab.org/research/the-internet-coup/> (archived)
- 80** Tereshchenko, A. and Moldavanov, D., 'Global Experience: Growth Points for Broadband Operators' (in Russian), KROS 2024. Video, <https://www.youtube.com/watch?v=NFakwisUYoQ> (archived)
- 81** ITU-T, Recommendation Y.2770, 'Requirements for deep packet inspection in next generation networks', November 2012. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2770-201211-!!!PDF-E&type=items (archived)
- 82** IETF, RFC 9849, 'TLS Encrypted Client Hello', March 2026. <https://www.rfc-editor.org/rfc/rfc9849.html> (archived)
- 83** IETF, 'Introduction to the IETF', undated, consulted 22 September 2026. <https://www.ietf.org/about/introduction/> (archived)
- 84** ITU, 'Participation', undated, consulted 22 September 2026. <https://www.itu.int/hub/membership/become-a-member/participation/> (archived)
- 85** 3GPP, 'Membership', undated, consulted 22 September 2026. <https://www.3gpp.org/about-us/membership> (archived)
- 86** VAS Experts, 'Migration from Sandvine to the VAS Experts Solution: Real Migration Case', 2 July 2025. <https://vasexperts.com/blog/functionality/migration-from-sandvine-to-the-vas-experts-solution-real-migration-case/> (archived)
- 87** Sundara Raman, R., et al. (2022). 'Network measurement methods for locating and examining censorship devices'. *Proceedings of the 18th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '22)*. <https://doi.org/10.1145/3555050.3569133> (archived)

