The Darkest Times of Runet

A Review of Internet Censorship in Russia in 2024

Contents

From “Blacklists” to “Whitelists”: The Evolution of Internet Censorship in Russia

The Russian internet is becoming increasingly similar to the Iranian internet. We are witnessing in real time how the authorities are gradually implementing "whitelists", preparing for the transition to a sovereign internet.

Censorship of the Russian internet officially began in 2012 with the introduction of "blacklists," official registries of banned websites. Roskomnadzor, the Russian government agency responsible for communications, information technology, and the media, has published these lists for years. Although establishing such a registry was an aggressive attack on freedom of information and speech, the blocking process was based on a relatively open procedure that required censors to comply with formalities and take responsibility for their actions. In this system, public control tools were somewhat effective, and human rights defenders were able to publicize significant blockages. There were also judicial practices for challenging illegal blockages through the judicial process. People could express their opinion about the prohibitive actions of the authorities through protests.

Russia is now entering a new era characterized by the government's complete control over the domestic internet through TSPU - a system of technical measures to counter threats. This system consists of specialized software and hardware that all internet providers in the country must install on their networks. Avoiding blacklists, TSPU blocks individual internet resources, hosting providers, VPN protocols, and other technological solutions that are not controlled by the authorities and are used by individuals and organizations to securely access the global internet. The system can also slow down or completely shut down internet traffic in certain regions for reasons of national security.

Russia began actively deploying TSPU in 2020, gradually covering all telecommunications operators. In 2024, imported DPI systems were replaced with domestic ones to reduce reliance on Western technology.

TSPUs are under the complete control of Roskomnadzor. At the same time, the system operates in an extremely opaque, unpredictable, and arbitrary manner. The increasingly complex and pervasive blocking and slowing down of various resources and protocols negatively impact network connectivity, causing sudden shutdowns, disruptions, and malfunctions of a large number of resources. Moreover, along with the resources deliberately targeted by censors, completely unrelated websites are also blocked. However, this collateral damage does not encourage the authorities to reconsider their plans.

On March 20, 2025, Cloudflare experienced an unprecedented system failure. The incident affected regions from the Urals to Primorye. According to expert estimates, approximately 1.5 million IP addresses in the subnet were blocked. The outage not only disrupted VPNs, but also took down many popular websites, including TikTok, Steam, Roblox, Twitch, Epic Games, DeepSeek, Figma, Miro, SoundCloud, Aviasales, Genshin Impact, and Duolingo, as well as websites of mobile operators.

Roskomnadzor announced that officials would "conduct scheduled technical inspections of the use of foreign server infrastructure by Russian services and telecommunications operators." After some time, the problem was resolved, but experts began discussing "Iranian scenario" more insistently. The incident was very similar to testing that occurred during preparations for a total Cloudflare block, which has already happened in Iran.

In April 2025, Roskomnadzor posted a recommendation on its website urging owners of Russian virtual private networks (VPNs) to avoid using foreign encryption protocols, including those "used by applications that provide access to prohibited information." If this is not possible, they should submit the IP addresses of the VPN servers so they can be added to a special list of exceptions. One of Roskomnadzor's divisions already maintains a "whitelist" of IP addresses that use foreign encryption protocols. As of April 2025, the list contained 75,000 entries, six times more than in 2023.

Russian censors are working to make it practically impossible to use VPN technology without official permission from the authorities. Those who fail to register in time and are not included in the approved lists take a risk of being blocked.

In Iran, the concept of "whitelists" originated from the authorities' requests for information about the foreign resources used by Iranian officials and businesses. These lists formed the basis of a system in which anything not permitted is prohibited. In addition to blocking external news and entertainment websites, virtually all global social networks and messaging apps, such as Facebook, Twitter, YouTube, and Telegram, Iran strictly blocks most circumvention tools. Article 19 researchers note that, according to the November 2023 government decree "On Strategies to Increase the Share of Domestic Traffic and Counteract VPNs," the use of VPNs in Iran is only allowed by law in certain cases, while in all other cases, using VPNs is prohibited. However, the criteria for what constitutes "legally allowed cases" remains unclear. It is also noted that the authorities are attempting to introduce certain approved VPNs for accessing foreign content, which require special registration.

Throughout 2024, Russia blocked VPN protocols via TSPU, which rendered those used by mass-market commercial VPNs inoperable. OpenVPN, WireGuard, and Shadowsocks all experienced difficulties, which significantly narrowed the market of reliable and affordable tools to circumvent blocks. Additionally, regular major outages at providers, during which half of the websites on the internet became unavailable, may indicate planned TSPU tests in preparation for "whitelists."

At the same time, we are witnessing the initial implementation of "graylists" in Russia. According to these lists, not only content officially included in "blacklists" is censored, but also anything deemed suspicious or unclear. Blockings are implemented based on in-depth traffic analysis using DPI and the identification of "suspicious" IP addresses. Again, we can refer to the examples of Iran and even China. The latter has no "whitelists"; it relies only on black and graylists.

"Graylists" represent a higher level of censorship development. They indicate that the system has been functioning successfully for a long time, accumulating the technology and experience to use them effectively. It is the work of a master who has refined their craft over time.

This image reflects Russian internet censorship, which has a 12-year history.

Context of 2024: the strictest censorship restrictions in the history of Runet

In 2024, Russia experienced the highest level of digital censorship. This was not only due to the slowdown and subsequent blocking of YouTube or the numerous new blocks. A year ago, Russia essentially banned public discussion about ways to circumvent the blocks using anti-censorship solutions. Advertising, promoting, or sharing scientific, technical, and statistical information about these tools is forbidden under threat of punishment. Furthermore, authorities use a DPI system to detect and block such solutions and remove them from app stores.

It all started with the ban on popularizing circumvention tools, which came into force on March 1, 2024 (it was published on November 14, 2023). The ban applies to information about such services, including anonymizers, VPNs, Tor, browser extensions, and other tools. Those who fail to comply with the requirements face fines ranging from 800,000 to 4,000,000 rubles. Repeating offenses are punishable by fines ranging from 1/20 to 1/10 of a company's total annual revenue.

Information resources may also be blocked if they publish instructions on how to access websites blocked by Roskomnadzor or if they promote the use of such tools. At that time, the law contained an exception allowing the publication of scientific and statistical information about anti-censorship solutions. However, by the end of the year, this exception was rescinded. The ban on scientific, technical, and statistical information about VPNs took effect on November 30, 2024, and will remain in force until September 1, 2029. Legally, the only remaining option for discussing VPNs is as a means of ensuring secure remote access.

In July 2024, Russia began throttling YouTube and by the end of the year, its traffic had dropped to 20% of normal levels. The authorities described the throttling as a

necessary response to Google's "inaction" and failure to comply with Russian laws. However, Russian legislation does not specifically mention throttling as a means of censorship. Nevertheless, this method has been used before. In 2021, for instance, it was employed to restrict Twitter's operations for failing to remove banned content from the platform.

In December 2024, Roskomnadzor published a draft order proposing that operators provide the agency with data on users who visit blocked websites, including their network addresses, places of residence, device identifiers, and IP addresses. In practice, this means monitoring individuals who circumvent censorship, and tracking VPN users. However, the authorities claim these measures are for cybersecurity purposes only, not surveillance or punishment.

The development of this story took place in the spring of 2025. Order No. 5 of Roskomnadzor which was registered with the Ministry of Justice on March 31, 2025, once again stirred public opinion. According to experts, the agency is gaining new powers and capabilities to monitor user traffic. The order outlines the agency's interactions with telecommunications operators, who are now required to collect and transmit data to Roskomnadzor that enables identification of connected devices on the internet, including IP addresses, MAC addresses, IMEI numbers, serial numbers, and geolocation data down to the municipal level.

For several years now, Russia has been using TSPU - Technical Measures of Countering Threats - for censorship purposes. TSPU components are integrated into telecommunications operators' networks, enabling them to block websites and specific internet pages, slow down services, and restrict access to VPN protocols that are subject to blocking. In September 2024, it was revealed that 60 billion rubles would be allocated over the next five years to modernize the TSPU system. These funds will be used to combat VPNs and other tools that circumvent censorship more effectively, purchase new equipment and software, and develop new blocking methods.

In addition to unregistered blockings carried out through the TSPU, "classic" blockings are still being implemented in Russia. According to Roskomsvoboda, a group that monitors the Register of Prohibited Websites, 419,140 websites were blocked in Russia in 2024, 62,000 of which were blocked without specifying the government agency that initiated the block. This number is twice as high as in 2023, when experts identified 197,000 blocked websites.

According to OONI, Russia uses various methods for website blocking, including DNS tampering and TLS man-in-the-middle blocking. These blocks are implemented in a decentralized manner. Providers in some regions may use multiple methods simultaneously, making circumvention more difficult.

According to a study by OONI, Russian internet providers use the following methods to block websites:

- DNS tampering, in some cases redirecting to block pages
- HTTP man-in-the-middle, displaying blocking pages
- TLS man-in-the-middle blockings
- RST packet injection after ClientHello during the TLS handshake
- Session termination after ClientHello during the TLS handshake
- Connection closure after ClientHello during the TLS handshake

In Russia, the websites of independent media outlets, non-governmental organizations (NGOs), and global social networks such as X (formerly Twitter), Facebook, and Instagram remain inaccessible. In 2024, the list expanded to include the messaging apps Signal, Discord, Session, SimpleX Chat and Viber, as well as dozens of new Russian and foreign media and an extensive list of VPN services and other tools for circumventing censorship.

Russian authorities have announced plans to increase the effectiveness of VPN blocking to 96% by 2030.

Blocking for Information About Circumventing Censorship

In April 2024, one month after the ban on popularizing circumvention tools took effect, Roskomnadzor reported blocking 700 materials on bypassing blocks, as well as 150 VPN services. This figure only increased over the course of the year. By February 2025, one year after the VPN ban took effect, Roskomnadzor reported that it had blocked over 6,300 web pages with information on bypassing blocks. Fines during this period amounted to 19 million rubles.

Over the past year, the websites of Amnezia VPN, Lantern, Outline, ProtonVPN, Red Shield, ExpressVPN, VPN Generator, the Censor Tracker browser extension, and the VPNpay marketplace were blocked.

Censorship also affected research projects long before the official ban on disseminating scientific and technical information about VPNs and ways to circumvent blocks came into force. In August 2024, the DPIdetector project, which monitored VPN protocol blocks, was blocked. Then, in September, the OONI Explorer project, which provided open data on internet censorship around the world, was blocked as well.

Experts note that the number of censored resources may be significantly higher. Pages and websites that removed information about VPNs and other ways to bypass blocks after receiving notifications from Roskomnadzor are not included in the registry of banned sites. These sites may also have geoblocked specific links, rendering them inaccessible to users in Russia. Nevertheless, censorship still occurred in these cases.

Removal of anti-censorship apps from the App Store

In 2024, Roskomnadzor began turning to Big Tech corporations for help censoring the Russian internet.

Opera, Google, and Mozilla were requested to remove plugins that could be used to bypass blocks from their app stores. Opera complied with this request by removing the Censor Tracker plugin in July. Mozilla was asked to remove PlanetVPN, FastProxy, Runet Censorship Bypass, and others. However, the company only temporarily imposed geoblocking on the extensions to assess its own risks. Mozilla later returned the extensions to its store and subsequently was fined 3.5 million rubles by a Russian court for not complying with Russian law.

Google has not yet been reported to have removed VPN services from Google Play at the request of Russian authorities. However, in March 2025, journalists discovered a database containing registered removal requests. Later, experts from the GreatFire project, which studies internet censorship, estimated that between March 12 and April 1, 2025, Russia, represented by Roskomnadzor, sent 214 requests to Google Play targeting 212 VPN applications. The requests also included the removal of more than 80,000 URLs from Google search. However, the corporation did not comply with the censors' requests.

In contrast, Apple was noted for its close cooperation with Russian officials in 2024. In July, it was revealed that at least four VPN applications — Proton VPN, Red Shield VPN, NordVPN, and Le VPN — had been removed from the Russian App Store. Later, experts estimated that approximately one hundred VPN apps had been removed. Roskomnadzor reported blocking 197 VPN services, likely referring to VPN websites.

One of the most illustrative removals occurred with the Amnezia VPN app. At midnight, the team received a notification from Apple with a request from Roskomnadzor to remove the circumvention tool. Three hours later, the app was already unavailable in the Russian App Store. Apple complies with Russian government agencies' censorship requirements within hours, without delay and without the possibility of challenging the decision. The corporation does not

respond to calls for transparency and respect for human rights from human rights defenders and activists.

At the request of Roskomnadzor, Apple also removed independent media apps that were censored in Russia. In October and November of 2024, the RFL/RL app, which featured content from Radio Liberty's Russian service, the Siberia.Realities and Sever.Realities apps, the Kyrgyz Service Radio Liberty app, and the Current Time app disappeared from the Russian App Store. Apple also hid several podcasts, including *The Insider*, *Echo of Moscow*, and *What Was That?* from the BBC Russian Service.

Apple Corporation cooperates with Roskomnadzor to restrict Russians' access to applications unfavorable to the Russian authorities. At the same time, Apple participates in anti-Russian sanctions. For example, the RuTube app was permanently removed from the AppStore, despite requests for its restoration.

Blocking of VPN protocols

Roskomnadzor actively uses DPI (Deep Packet Inspection) equipment to analyze traffic and block VPN protocols. DPI enables the analysis of data packet contents transmitted over the network and the filtering of internet traffic at a deep level. This equipment is installed at internet service providers and is part of the TSPU.

The first cases of VPN blocks occurred in 2021. In 2023, large-scale testing of VPN protocols began via TSPU. The WireGuard protocol was the first to be addressed: its unavailability was observed among Beeline and MTS providers in Moscow and several other regions. Users also complained about the unavailability of OpenVPN and IKEv2, though the IP addresses of VPN servers were not blocked. Researchers from the University of Arizona and the University of Michigan released a study in 2024, which found that blocking OpenVPN poses virtually no difficulty for internet providers, and detecting a connection takes about 8 seconds with up to 85% accuracy.

In 2024, the blocking of VPNs became more intense. Throughout the year, mobile operators restricted the operation of at least the ShadowSocks and WireGuard protocols. From April to May of that year, attempts were observed to block proxy protocols such as VMess and Shadowsocks (and consequently, Outline, which uses them).

In the VMess and Shadowsocks protocols, the transmitted data is encrypted. At least one blocking pattern for all unidentified protocols on censoring equipment looks like this:

1. The client sends three packets, each containing 411 or more random bytes.
2. The server sends an arbitrary number of bytes more frequently than the client sends packets.

When these conditions are met, the connection is blocked. It is also assumed that blocking is based on packet size or the ratio of sent to received size.

There were reports of malfunctions in Outline, as well as issues with SSTP and Cloak if the "default" SNI for obfuscation was set to googletagmanager.com or yahoo.com. The Cloak issues could have been caused by some fingerprints not being updated on time.

Specific cases of SSH protocol blocking on TSPU were documented in November 2024:

- The provider blocks SSH access to servers if detectable TSPU VPN protocols (such as Shadowsocks and OpenVPN) were previously observed on them.

- The block is applied only when authentication is attempted via an SSH key. Changing the keys or their type does not resolve the issue. Password-based authentication remains available and stable.
- At the TSPU level, DPI fully blocks packets after a particular packet in the connection, resulting in timeouts and disconnections. There has been no observed interference with the traffic itself (such as injecting "fake" packets).
- SSH connection through VPN remains successful because DPI does not see the SSH protocol inside the encrypted tunnel.
- Blocking is based on traffic analysis and "suspicious" IP addresses, which is confirmed by the absence of issues with servers without VPN protocols.

Along with VPN protocols, Roskomnadzor targeted Snowflake, which is used in Tor to obfuscate connections to bypass censorship. The blocking was likely implemented by restricting direct access to bridges or by using distinctive DTLS fingerprint characteristics in Snowflake. In November 2024, a sharp decline in Snowflake users was registered in Russia, although at that time testing did not reveal the use of DTLS fingerprinting, which had previously been employed for blocking.

VPN protocol blocking measurements

VPN protocol blockages can be detected, in particular, using the internet censorship research tool, DPIdetector. DPIdetector enables real-time tracking of VPN protocol blockages and records their duration, specifying particular regions and operators. The tool analyzes the availability of VPN protocols, such as Cloak, OpenVPN,

OpenVPN+TLScrypt, WireGuard, Amnezia WireGuard, and Shadowsocks, in different regions of Russia where user nodes are present during testing. Currently, the project has over 100 node holders with various telecom operators in more than 30 Russian regions. The analysis considers different mobile and home internet operators, as well as traffic analysis within and outside of Russia. Automatic checks are carried out every 10 minutes.

> To become a 'node' and participate in monitoring, the device must have special software installed, which users (volunteers) download from GitHub, configure, and maintain continuous internet access for uninterrupted operation. Technical requirements include a device with a Linux operating system (OS), the latest version of Docker, and the "buildx" and "compose" (v2) plugins, or a device running Windows with WSL installed.

According to the data charts from DPIdetector, the WireGuard protocol was blocked by mobile operators in Russia from mid-August to the end of November 2024. At the end of December 2024, WireGuard began experiencing blockages again on mobile internet. WireGuard was not blocked everywhere on home internet, but local connection issues may have persisted in some regions.

Shadowsocks was unavailable on mobile internet from October 15, 2024, to the end of December 2024. The protocol remained blocked on mobile internet until the end of 2024 but worked fine on home internet.

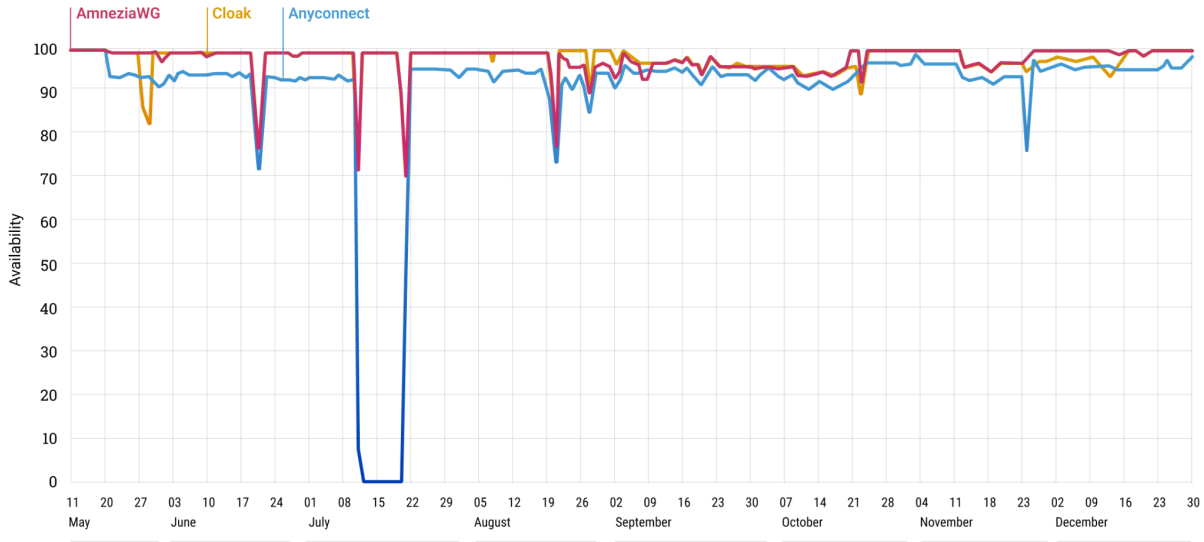
WireGuard protocol was blocked on fixed-line internet providers from August 21 to the end of November 2024, while Shadowsocks was blocked from November 23 to early December 2024.

Additionally, other protocols were blocked throughout the year.
- in May and June, OpenVPN was blocked on mobile devices;

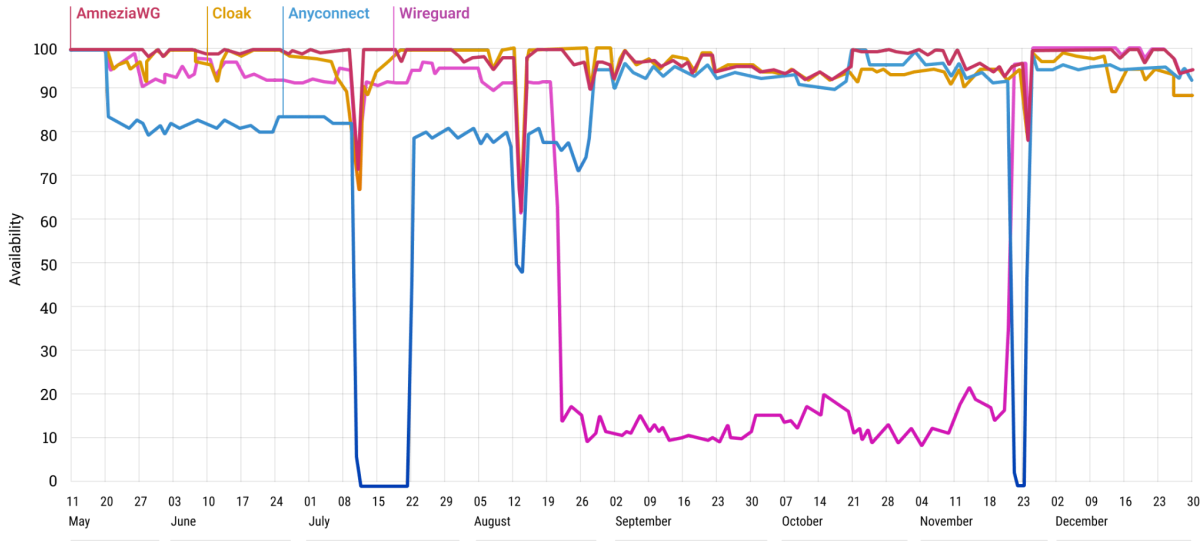
- from May to August, attempts to block Cisco AnyConnect were recorded in several regions on both home and mobile internet;
- some regions experienced brief blocks of the Cloak and OpenVPN protocols on home internet.

These blockages were not long-lasting and occurred sporadically across different operators.

In all cases, the connection restrictions only apply to foreign traffic and only in situations where the user attempts to connect to a VPN with servers outside of Russia.



Home internet traffic. Source [DPIdetector]



Mobile internet traffic. Source [DPIdetector]

Active Probing

In February 2024, a global failure occurred on the Russian internet, likely due to Active Probing testing. According to experts' observations, Active Probing technology had been operating in Russia for approximately one month at the time of the failure. The large-scale internet outage may have resulted from an attempt to launch the technology automatically across the entire Russian internet.

Active Probing is a method where the system itself sends requests to suspicious IP addresses or domains to check whether a banned circumvention tool, such as VPN, Tor, or proxy, is being used.

Experts recorded an activity from an IP address in the AS61280 group, belonging to the state institution "The General Radio Frequency Centre" (GRFC). A scan of port 443 was conducted on many servers (which could have been empty or had a VPN installed on them).

Using the example of the VPN service Windscribe, expert ValdikSS described how such scanning and subsequent blockages work.

This happens as follows:

When accessing via HTTPS with the SNI (api|checkip|assets).windscribe.com and other domains of the Windscribe service on port 443, or by sending a TCP SYN to one of the known IP addresses of Windscribe VPN servers and ports 443, 587, 21, 22, 80, 123, 143, 3306, 8080, 54783, 1194 (for example, 149.88.108.1),

or by UDP to the OpenVPN or WireGuard VPN protocol on these same ports, a 5-minute block occurs:

The SNI by the regexp (api|checkip|assets).[0-9a-f]{40}.com, but only if the zone name contains at least 5 digits and 4 letters.
For example,
https://api.abcdef0123456789abcdef012345678900000000.com would be blocked, but
https://api.abc00001234567892222220123456789000000000.com would not.

It is possible that this method with triggers is also used to identify new VPN servers: if a user accesses (api|checkip|assets).windscribe.com or a regexp domain after it has been blocked, and then within 5 minutes connects via OpenVPN or WireGuard to some unknown IP address, it is most likely a Windscribe server. However, if this happens, it is likely not in automatic mode.

В 2024 году российские цензоры заметно нарастили использование Active Probing для поиска и блокировки VPN-сервисов. В течение года регистрировались проблемы с сервисом Outline, а именно с его админкой, которую можно найти и заблокировать.
In 2024, Russian censors significantly increased their use of Active Probing to identify and block VPN services. Throughout the year, there were reports of issues with the Outline service, particularly with its admin panel, which can be located and blocked.

STP, SoftEther, and OpenConnect are highly susceptible to blocking without updates/patches due to their response characteristics to requests with payload:

- SoftEtherVPN, in response to a GET request with the path /vpnsvc/connect.cgi, content type application/octet-stream, and

payload 'VPNCONNECT', will return a 200 code and a predictable binary blob describing what it is.

- In the case of MS SSTP, censors, wanting to find out what the user is doing, will simply make a request to its server with the URL /sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/ using the HTTP method SSTP_DUPLEX_POST, as described in the protocol standard, and the server will confirm in the response that it is indeed an MS SSTP VPN.
- AnyConnect/OpenConnect, when accessed via / or /auth, will respond with a very characteristic XML. This cannot be corrected—these features are defined in the protocols, and VPN clients operate based on this logic.

Source: https://habr.com/ru/articles/710980/

Clearly, in the near future, almost all protocols will be detectable by Active Probing. The most popular protocols have already been discovered and blocked. This is driving the demand for alternatives, such as XRay and other tools that can disguise themselves as web traffic and offer protection against Active Probing.

Encrypted Client Hello (ECH) blocking

In September 2023, Cloudflare began using the Encrypted Client Hello (ECH) protocol for all websites using their servers. This technology hides all information during a secure TLS connection (i.e., HTTPS, not HTTP), including metadata. ECH encrypts the ClientHello message as part of the TLS handshake. The goal of this protocol is to improve users' privacy; otherwise, the host name of the visited website would be revealed to the network provider.

An ECH side effect is that it complicates the work of DPI by encrypting and masking the Server Name Identification (SNI) field during the TLS handshake. Consequently, websites hosted on Cloudflare that were previously inaccessible due to DPI blockages became accessible within the country, no longer requiring special censorship circumvention technologies.

In November 2024, it was reported that Roskomnadzor had begun blocking access to Cloudflare's ECH in Russia. As a result, hundreds of thousands of websites across the country, including that of the Yakutsk State Agricultural Academy, became inaccessible.

Cloudflare's use of ECH was called a "violation of Russian legislation," and censors recommended that Russian website owners discontinue using ECH and switch to domestic CDN services that "ensure the reliable and secure operation of resources and protection against cyberattacks."

> Blocking was implemented if the SNI = cloudflare-ech.com was installed in the ClientHello packet and an ECH extension was present.
>
> Blocking did not occur with just SNI = cloudflare-ech.com without the ECH extension, nor with the ECH grease without SNI = cloudflare-ech.com.
>
> The filter is applied to HTTP2 (TCP) and HTTP3 (QUIC) connections.
>
> The TSPU “freezes” the connection immediately after receiving the ClientHello, rather than breaking it at the TCP level or in some other more suitable way. As a result, the browser only realizes that the connection is broken after about a minute.
>
> Source: ntc.party/t/блокировка-encrypted-clienthello-ech-на-cloudflare/12837

Therefore, the use of ECH is not an effective method for circumventing censorship in Russia. Additionally, Roskomnadzor's regular statements about the need to

switch to domestic hosting providers and collect IP addresses may indicate preparations for new blockages.

DNS issues

Throughout 2024, expert communities discussed DNS issues affecting popular services such as Cloudflare, Google, AdGuard, ControlD, and others. These issues occurred at different times and lasted for varying periods.

Problems were most often observed with Cloudflare because their DNS was used in WARP, a free VPN. Due to DNS blocking, it was difficult to use WARP to bypass blocks. However, it received a second chance when instructions appeared on how to "revive" it using the AmneziaWG protocol (obfuscation using AWG).

Back in 2020, it was revealed that Roskomnadzor had blocked the three DNS servers of the DigitalOcean cloud service: ns1, ns2, and ns3. However, the block was unstable, and the services were periodically accessible.

The Domain Name System (DNS) is a hierarchical system of domain names that converts familiar addresses, such as google.com, into numerical IP addresses used for routing traffic in networks. In Russia, DNS tampering, such as altering responses or blocking requests, is used to censor the internet and restrict access to information.

In 2019, the adoption of the law on the "sovereignization" of the Russian segment of the internet brought about the proposal of a Russian Domain Name System (DNS) as an alternative to the global DNS supported by the Internet Corporation for Assigned Names and Numbers (ICANN). National Domain Name System (NDNS) began operating the in 2021. The same year, Roskomnadzor required providers and owners of autonomous systems to connect to the NDNS, imposing the first fines for noncompliance.

In 2024, the NDNS was actively used to redirect DNS requests and implement blockages at the network level. In September 2024, Roskomnadzor blocked access to the OONI Explorer platform, which provides data on internet censorship.

> In some Russian networks, DNS requests to explorer.ooni.org returned Roskomnadzor's censorship service messages. For example, the IP address 188.186.154.88 returned the message, "Access to the information resource is restricted under Federal Law No. 149-FZ of 27.07.2006 'On Information, Information Technologies, and Information Protection.'" In other cases, DNS requests returned an error indicating that the domain does not exist. These methods confirm the use of DNS response manipulation to block access to resources.

Similarly, according to OONI research, access to at least 279 news media domains, both independent and foreign, was restricted in Russia as of September 2024. In these cases, DNS-based blocking occurs in a decentralized manner, returning the address 188.186.146.208 as part of the DNS resolution.

In December 2024, Roskomnadzor conducted training drills on the isolation of the Russian internet segment from the global network. During this time, three regions — Chechnya, Dagestan, and Ingushetia — were disconnected from the global internet. The Russian NDNS maintained the operation of internal resources during the isolation.

In 2024, Russian authorities significantly strengthened measures to block encrypted DNS protocols such as DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT), labeling them as a threat to state censorship. These protocols encrypt DNS queries, making them harder to intercept and alter. The authorities used DPI systems for blocking, and these systems are capable of analyzing network traffic in real time to detect characteristic signs of DoH and DoT, such as specific ports, headers, and traffic patterns.

Censorship against hosting providers

As early as May 2022, users in Russia began reporting issues when trying to access the Cloudflare and DigitalOcean networks through certain ports. They were unable to establish a TCP connection through port 443, and all packets were dropped. However, connections through other ports worked fine. This phenomenon was observed in many cable and mobile networks, including those owned by Beeline, Rostelecom, and Dom.Ru. TCP port 443 is used by the HTTPS protocol, indicating that the attack may have targeted it specifically.

In April 2024, the issue of blocking hosting providers arose again when Roskomnadzor blocked the websites of those who had not complied with the requirements of the "landing" law.

Three months later, users in Russia reported that HTTP/HTTPS traffic on ports 80 and 443 was being blocked when they attempted to connect to the IP addresses of Linode, OVH, Fastly, DigitalOcean, and Scaleway. As a result, some websites, including Nmap and Reddit, were temporarily inaccessible.

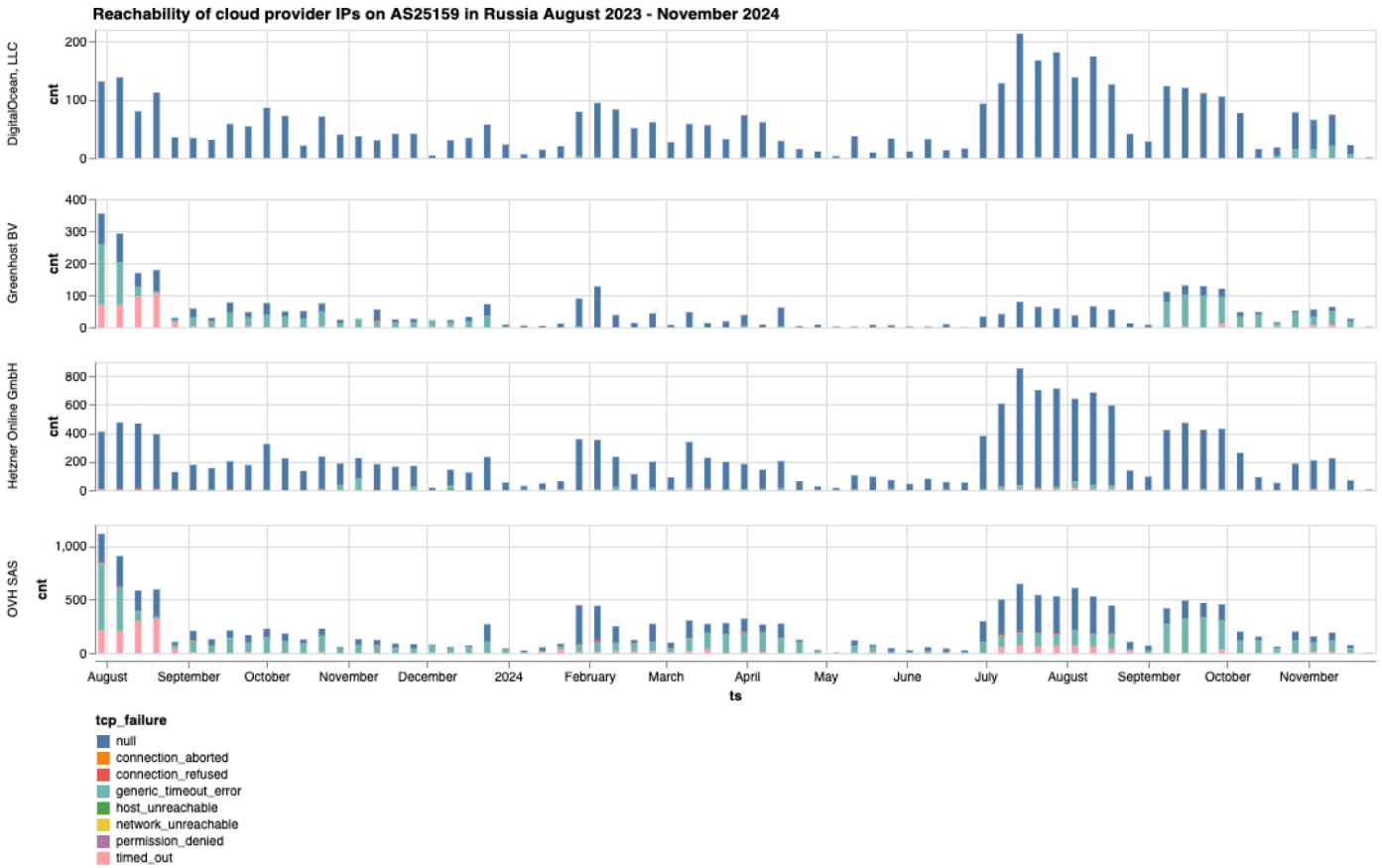
> These are the blocked ranges (it is possible that the list is not complete):
> 51.68.188.0/22
> 51.38.124.0/22
> 50.116.0.0/18
> 151.101.0.0/16
> 206.189.65.0/24
> 51.15.0.0/17

In November, reports of issues with websites hosted on platforms such as Greenhost, Cloudflare, Hetzner, OVH, and Aeza first emerged. These problems affected resources such as 2ip, the Notepad++ website, Arch Linux, FileZilla, and

others. Roskomnadzor was most likely attempting to combat VPN services that use IP subnets from these hosting providers.

> When attempting to open the HTTP version of the website, TCP Retransmissions or packet retransmissions were returned, which indicates artificial interference with the traffic. This results in an "eternal loading" page or a "timeout" error.

These user reports are confirmed by OONI data, which show a spike in timeout errors when testing IP addresses of cloud providers on the AS25159 network (PAO Megafon) in Russia between September 2024 and October 2024.



Availability of IP addresses of cloud providers on AS25159 in Russia from August 2023 to November 2024. Source: ooni.org

Roskomnadzor later officially admitted that it may restrict access to foreign hosting services. The government agency claims that companies such as GoDaddy, Kamatera, Network Solutions, Ionos, HostGator, DigitalOcean, Amazon Web Services, and Hetzner Online GmbH pose risks to the resources of Russian organizations. As in other cases, the agency cites violations of the law, specifically the failure of hosting providers to include themselves in the registry.

Throughout 2024, subnets belonging to hosting providers have been blocked because, according to censors, they could potentially be used to deploy VPNs. At the same time, the authorities consider the associated losses from blocking many unrelated websites that are simply hosted nearby to be insignificant.

This closely resembles the "iranization" of Russian censorship, where almost all IP address ranges of major hosting providers are blocked. It's a path toward "whitelists" of approved websites where everything else is blocked, prohibited and doesn't work except for a few sites permitted by the censors.

Problems with website mirrors on CDN

In February 2024, Fastly, a well-known CDN server, disabled the ability to use Domain Fronting on its service. This put the functionality of many circumvention tools that relied on this method, such as meek and VLESS and others, at risk. The two largest CDN providers, Google and Amazon, banned Domain Fronting in 2018 to prevent hacker attacks.

Domain Fronting tools are used not only by hackers, but also by developers of VPN services and designers of mirrors for blocked websites. It is a method of masking a resource's real address by manipulating requests in the Content Delivery Network (CDN).

Blocked websites create their own copies, or mirrors, which they hide using Domain Fronting within the extensive server space of content delivery network (CDN) providers. This allows them to avoid being blocked using the Collateral

Freedom strategy. Interfering with CDN operations leads to the collapse of an important means of circumventing censorship.

Independent Russian media outlets that are subject to censorship and forced to maintain a complex system of mirrors and anti-censorship tools to allow readers to access their content, told researchers that blocking of CDN and hosting providers has affected their work. These blocks reduce content download speed, increasing infrastructure costs and making it more vulnerable to cyberattacks. This is particularly concerning for independent outlets operating under political pressure.

In addition to Domain Fronting, Russian media also use URL shorteners to hide mirrors. While these tools are still functioning (including Bitly, vk.cc, and others), they can be blocked.

Provider outages during testing of the sovereign Runet

In mid-October 2024, users of the Skynet internet provider reported being unable to access various websites, including Wikipedia and bank websites. Skynet announced that it was not imposing any restrictions on internet resources.

Users discussed the hypothesis that the failure was related to the application of new settings to the TSPU equipment. This could have occurred during the testing of "whitelists," a model for internal internet operations in which all websites are blocked except those on the approved list. Such connectivity failures happen quite frequently, often due to human error, poorly executed updates, or hardware imperfections.

On November 1, a similar mass failure was observed with at least four other providers — MGTS, MTS, Rostelecom, and Dom.ru.

In December, training drills on "sovereignization of the Russian internet" were conducted, which was particularly noticeable to residents of Dagestan. On

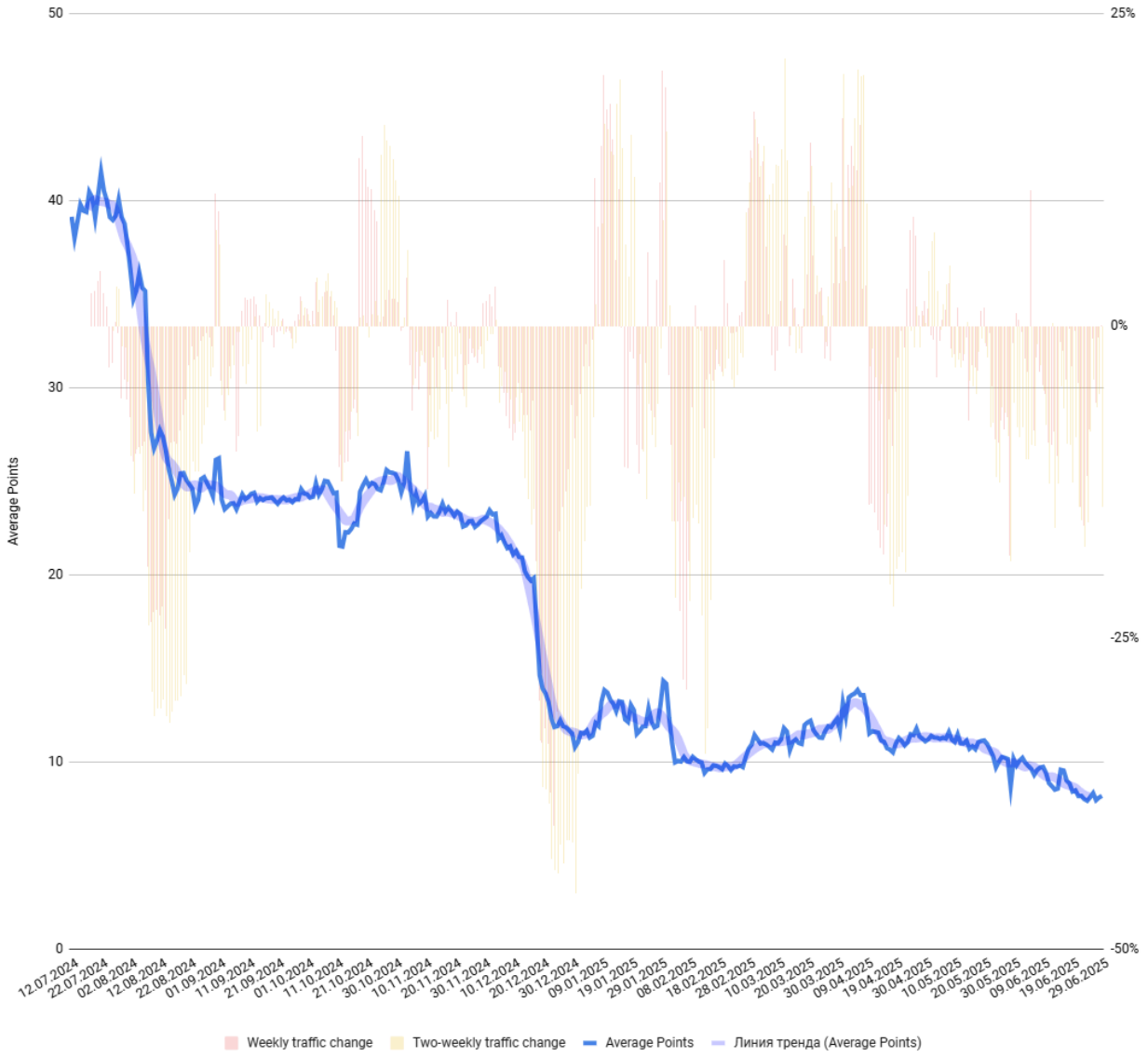
December 6-7, 2024, most foreign resources (GitHub, GPT, WhatsApp, Telegram, etc.) there were inaccessible, and attempts to connect to foreign VPNs resulted in errors.

Throttling of YouTube and VPN protocols

In 2024, Russia experienced a slowdown in services and tools. The most resonant and indicative example is the throttling of YouTube, which began in July of that year.

Initially, the authorities explained the issues with the video service as degradation of Google's equipment, which the corporation had not properly maintained or updated since 2022. However, on July 25, 2024, officials announced that YouTube was intentionally being slowed down in Russia. Roskomnadzor later outlined the reasons for taking action against the video service, citing numerous violations of Russian legislation and "disrespect towards our country and citizens."

Starting August 1, YouTube's speed dropped sharply for all providers across the country, slowing it down completely. While the YouTube website and apps loaded without issue, videos either didn't play at all or took a long time to load.
During the first two weeks of the blockage, YouTube traffic in Russia decreased by over 20%.



Average daily traffic on YouTube, Russia. Source ЗаТелеком

At this point, Russia experienced a surge in user interest in censorship circumvention tools and widespread VPN installation. Telecom operators reported a 5-10% increase in overall traffic volume. In the networks of regional operators, the increase reached 20%. This resulted in additional expenses for regional operators, who had to purchase more traffic from backbone operators.

In addition to YouTube, the speed of VPN protocols such as OpenVPN, WireGuard, AmneziaWG, and Cloak slowed down in 2024. Some users reported issues with less popular protocols, such as SoftEther and OpenVPN XOR. Speed slowed down when connecting via port 443, but returned to normal on any other port. This issue was observed on home internet but was resolved by switching to mobile networks.

The throttling occurred on various VPS providers, meaning it was not dependent on location or the hosting provider. Most often, the slowdown was temporary and lasted for about half an hour or a couple of hours. Changing obfuscation settings, such as those in AmneziaWG or Cloak, helped resolve the issue.

The era of throttling services began in Russia in 2021 when authorities started using this technology on Twitter. The social network was slowed down because, according to the authorities, it failed to remove content containing prohibited information. Thus, the throttling sanctions were intended to encourage Twitter to cooperate.

> At that time, experts conducted thorough research into the new censorship technology. They found that throttling is initiated by Twitter domains in the TLS SNI extension and it limits both upstream and downstream traffic to a range of 130–150 kbps, dropping packets that exceed this speed. They also found that the throttling devices are apparently located close to end users and that throttling is consistent across different internet providers, suggesting centralized coordination.

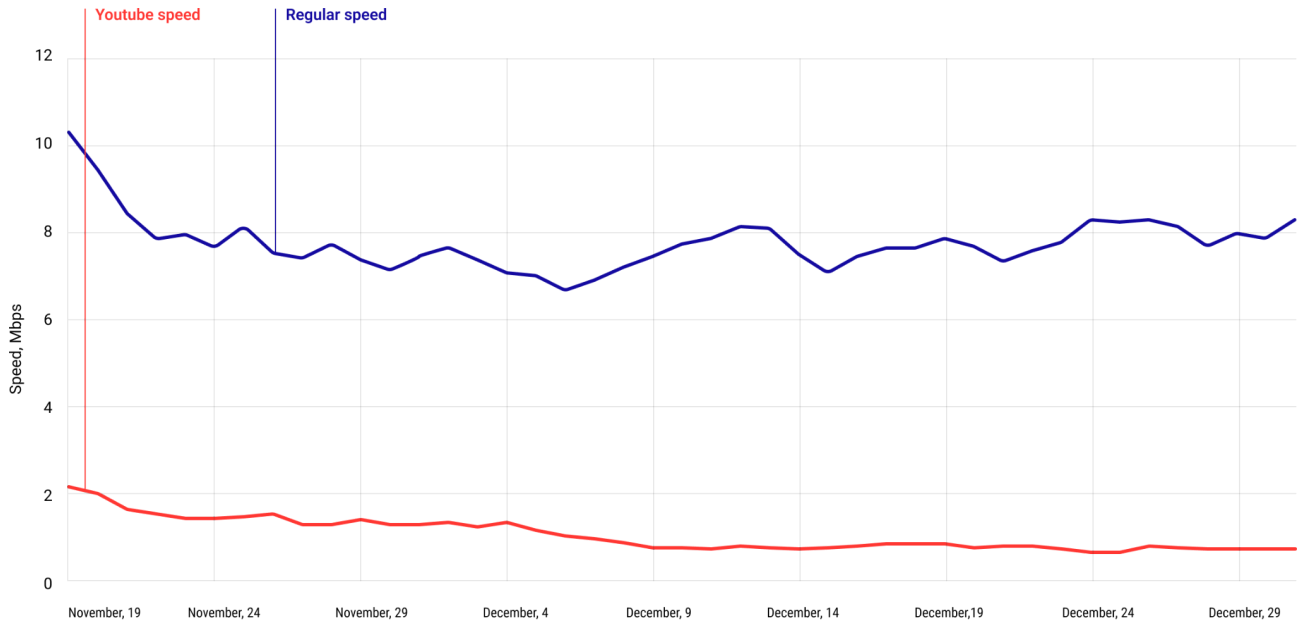
Russia's adoption of throttling technology was a consequence of shifting away from a transparent censorship model in favor of a centralized one, which gives censors more power to impose unilateral restrictions. The previous system relied on blocking IP addresses, a list of which is published by Roskomnadzor. Full-scale implementation of TSPU has made censorship more sophisticated. TSPU enables authorities to use throttling, fingerprinting, SNI blocking, protocol blocking, and other technologies.

Measuring YouTube slowdown

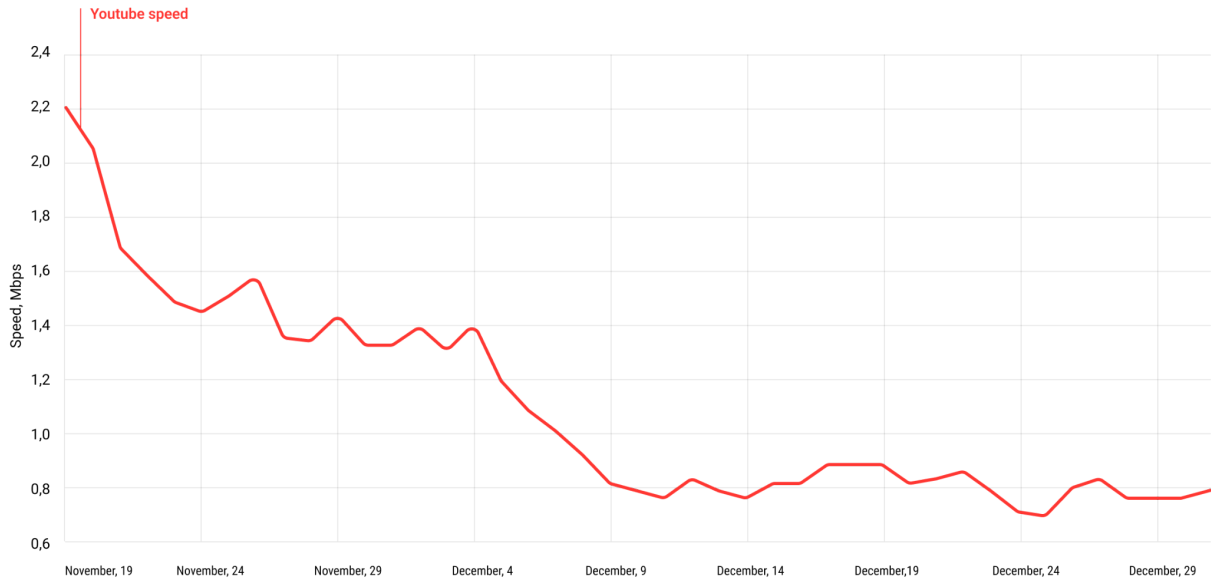
Since November 2024, DPIdetector has been measuring YouTube throttling. This data is based on the difference between regular internet speed and YouTube loading speed.

To test the speed, the first 400 kilobytes of the test file are downloaded from the server. Then, the download time is measured to determine how many megabits per second are being received. The download is performed twice: once in "normal" mode and again with the server name replaced by a YouTube server name. The blue graph shows the measurements in "normal" mode and the red graph shows the measurements with the name replaced by YouTube.

As the graph shows, the already low download speed on YouTube continued to decline after November 19, 2024, reaching a minimum of 0.8 Mbps by the end of the year.



Source DPIdetector



Source DPIdetector

Anti-censorship tools in Russia

The number of functioning tools for circumventing censorship in Russia is gradually decreasing. What was available to users at the beginning of the year may not work by the end, and effective tools often require more sophisticated settings, making them less suitable for inexperienced users.

Following the massive blocking of VPN protocols, it has become much more difficult to find a stable VPN service. The removal of apps from the App Store has made things more difficult for users, who now have to perform special manipulations to change their region in order to install an app. Another challenge is paying for a VPN, as only a few providers successfully work with Russian cards.

At the same time, especially after YouTube was blocked, the sale of one-day VPNs flourished. Often, these are little-known Telegram bots selling Outline keys. Unknown individuals have also set up VPN services based on free, self-hosted solutions, such as Amnezia VPN or Outline, and sell access keys that stop working after a short time. When users are left with a non-functioning service they paid for,

often more than once, it undermines their trust in VPN technologies. They often stop looking for working alternatives and ways to access the free internet. This serves the Russian authorities' goal of keeping everyone within the sovereign Russian internet.

Still, we can point out a few services that did well in Russia in 2024, despite all the attempts to block and slow them down.

GoodbyeDPI, Zapret, ByeDPI

The free, open-source tool created by censorship researcher ValdikSS has effectively and reliably helped bypass blockages in Russia for a long time without the use of a server. After YouTube was blocked, the developers released a guide to help users configure the app and their computers to unblock the video service. However, GoodbyeDPI sometimes experiences connection issues, potentially because TSPU systems have learned to detect and block it.

Zapret is a similar tool, although it is more complex to set up. A popular solution for Windows was based on it, enabling users to unblock YouTube and Discord with just a couple clicks. Another solution, ByeDPI, was implemented as a plugin for NekoBox and has an Android version created by a different developer.

XRay, Cloak, OpenVPN XOR и другие рабочие решения

To bypass censorship, advanced users use XRay-Core, which includes VLESS , enabling them to mask their connection as HTTPS traffic. VLESS has enough "add-ons" that make it more resistant to blocking. For instance, it can be hidden behind a CDN or routed through gRPC or WebSocket. Additionally, the developers recently released XHTTP, which is based on SplitHTTP. XHTTP splits the connection into parts so that, when streaming video, the tunnel does not remain static. Instead, the connection is fragmented and reassembled as a series of random requests, creating the appearance of active web browsing from the outside.

In addition to XRay, Cloak, OpenVPN XOR are still functional, and with sufficient technical knowledge, NaiveProxy or PingTunnel can be configured.

Tor

In addition to VPN and proxy protocols, Tor is used to bypass censorship. The new WebTunnel transport performs particularly well. WebTunnel resembles HTTPS, which makes it harder to detect and block. In contrast, obfs4 is considered outdated and less resistant to modern blockages.

Other obfuscation methods in Tor can be blocked in Russia to some extent. For example, obfs4 bridges in Tor were blocked on 4G mobile networks and beyond. Issues were observed with bridges at least with Tele2, Beeline, and Yota.

The meek transport in Tor is inconsistent and its speed isn't ideal. Another issue with meek that should be mentioned is the withdrawal of services from providing their infrastructure for Domain Fronting, which significantly limits the configuration and usage options for meek, as it relies on this obfuscation method.

Amnezia

Amnezia VPN operates using its own protocol, AmneziaWG. This protocol is a fork of WireGuard-Go with added features for bypassing blockages and reducing the likelihood of detection. Amnezia VPN also works with other obfuscation protocols, such as OpenVPN over Cloak and XRay Reality. These features make the service highly resistant to blockages because its traffic doesn't resemble typical VPN traffic. Therefore, it cannot be easily detected and blocked by Russian censors, who have implemented large-scale VPN protocol blockages.

The team's first development was a self-hosted product that users praised for its high level of reliability and privacy. In 2022, Amnezia VPN launched a special version of Amnezia Free for Russia that allows users to access censored independent media sites, human rights organizations, social networks, and messaging apps. After YouTube was blocked in Russia, the company deployed a classic commercial solution on a block-resistant protocol, enabling users to watch streaming video without having to configure the service themselves.

VPNGenerator

VPN Generator is a service based on the collective use of VPNs. This free, reliable solution involves users forming a "brigade," for which a separate mini-VPN is created. Each mini-VPN has a unique network address, and this makes them difficult to detect and block. Operating on the Outline platform, VPN Generator allows users to unblock YouTube, Discord, and other high-traffic streaming services.

Currently, there is a commercial solution called GenVPN that distributes access keys via a Telegram bot. It is used by large Russian-language media outlets and bloggers to create solutions.

Paper VPN and other anti-censorship solutions from the media

In 2024, anti-censorship solutions developed by independent Russian media outlets to maintain their audience were actively developed. The most notable example is Paper VPN from the Bumaga media outlet. Although the VPN was launched in 2022 when the Bumaga website was blocked in Russia, it was actively promoted and grew its user base in 2024.

The independent TV channel and online media outlet Dozhd (TV Rain), which is labeled as an "undesirable organization" in Russia, developed a browser extension called Поток (Stream) after videos on YouTube began to load slowly. It allows users to "speed up" video loading and watch videos in high quality. This free tool is being promoted to Dozhd's readers and viewers.

In 2025, media outlets, human rights teams, and popular YouTube bloggers, such as the "undesirable" media outlet The Insider, the human rights project Kovcheg, and blogger Dima Tsitser, have developed their own VPN tools.

Future Scenarios

The observations described above aim to capture the stages of censorship development. By analyzing these stages, experts, researchers, and developers of anti-censorship tools — as well as ordinary internet users in Russia — can predict future events and plan accordingly.

Our outlook for the near future is as follows.

1. We will probably observe statistical blocking methods in 2025. The statistical blocking method involves monitoring a specific user, group of users, or server. The traffic will be analyzed to determine access to various services. If a lot of traffic is detected going to a specific address, it will be checked for the presence of a VPN or proxy, which may result in future blocking or monitoring.
2. Russia's Internet is moving towards the introduction of "whitelists" of authorized websites and addresses, as well as a "professional Internet," where all external resources are blocked by default, but can be accessed when necessary. For instance, qualified developers who need to use a foreign service, such as GitHub, must submit a request to the relevant authority to unblock it.
3. We can expect attempts to develop and implement legislative measures for the administrative or criminal prosecution of citizens, not only for distributing but also for using VPNs and other tools to circumvent censorship, a concept known as "consumer responsibility." Enforcement may include fines or prison sentences for those who violate the laws (as has already occurred in China, for example).
4. Russia will continue to adopt China's censorship model alongside import substitution, blocking large international services while promoting domestic alternatives. The authorities are not only banning certain services, they are also offering alternatives. We have already seen an unprecedented amount of state investment in VK and Rutube aimed at improving their services before blocking YouTube in 2024. After the block, some YouTube users simply switched to Russian services lacking the motivation to figure out how to bypass restrictions and find a functional VPN. Over time, domestic services

will become more convenient and attractive to users, despite the censorship and surveillance that are built into these services by default.

5. Split tunneling will be one of the best solutions for fighting blockages. It makes it more difficult for DPI equipment to analyze VPN traffic from users because it only passes traffic to blocked resources or geo-blocked resources, instead of all traffic from the device.

6. The main criterion for choosing an effective censorship circumvention tool in Russia will be its ability to disguise itself, for example by masking or becoming unrecognizable. This will make it more difficult for DPI equipment to detect and block its pattern, as happened with Shadowsocks, which, with default settings and no obfuscation, can be easily detected and blocked by DPI systems or standard VPN protocols such as OpenVPN and WireGuard.