On Russia's Early Introduction of QUIC SNI Censorship

Nico Heitmann
Paderborn University

Niklas Niere
Paderborn University

Felix Graf Lange
Paderborn University

Juraj Somorovsky
Paderborn University

Abstract

Governments around the world limit free access to information through Internet censorship. With the rising adoption of the QUIC protocol, these censors have been forced to evolve their systems. Russia introduced sweeping changes to its censorship after its full-scale invasion of Ukraine, including completely blocking international QUIC connections. However, after this broad filter was identified in 2022, Russian QUIC censorship received little attention: The current state of QUIC censorship by TSPU devices is largely unknown. In this paper, we provide a timeline of Russian QUIC censorship and detail its current state. We identify that Russian TSPU devices switched to SNI-dependent QUIC censorship on a large scale between May 2022 and July 2023, a fact that went largely unnoticed for three years. While the GFW was previously thought to be the first censor with broad SNI-dependent QUIC censorship, we highlight that Russian TSPU devices broadly adopted SNI-dependent QUIC censorship at least nine months before the GFW. We consider this an indicator of the TSPU devices' flexibility and of Russia's willingness to invest in strict and up-to-date censorship.

Keywords

Censorship, QUIC, SNI, Russia, TSPU

1 Introduction

Internet censorship affects more than half of all Internet users around the world [18]. Countries such as Russia [34, 45] obstruct their citizens' free access to the Internet by analyzing and selectively blocking protocols such as IP [25], DNS [20, 30], HTTP [8, 20], and TLS [10, 29, 45]. Newly developed protocols are often soon targeted by censors in an effort to maintain control [9, 23, 28]. Potentially replacing HTTP/2 over TLS, HTTP/3 over QUIC [6] is already adopted widely [19]. As such, QUIC traffic is also targeted by censors [15, 16, 44, 46].

QUIC Censorship. QUIC [21, 39], a transport protocol based on TLS 1.3 [35], provides confidentiality and authenticity—most notably to HTTP/3 traffic. Although QUIC prevents censors from decrypting and analyzing application traffic, the initial QUIC handshake messages are protected only by keys derived from public information, allowing censors to analyze their content. As the handshake contains the website's domain name in the Server Name Indication (SNI) extension [1], censors can effectively determine its destination. A censor's options for tearing down QUIC connections by injecting packets—on-path censorship—are limited because most of their control packets are encrypted; blocking QUIC connections by dropping packets—in-path censorship—is possible. As of now, QUIC SNI censorship through packet dropping has been reported for China [46] and Russia [14] and hypothesized for Ethiopia, Kazakhstan, Myanmar, and Pakistan [44]. Non-SNI QUIC censorship has been reported for Iran, India, Russia, and Uganda by Elmenhorst et al. [15, 16].

Censorship in Russia. Russia has a long history of decentralized Internet censorship [33], and discussed censorship strategies with China since 2016 [5]. In 2021, Russia centralized its Internet censorship efforts by deploying "TSPU devices" in Internet Service Providers (ISPs). Russia has severely tightened its Internet censorship since beginning its full-scale invasion of Ukraine [22], obstructing free access to information for people in Russia. In 2022, forum users reported that Russia began broad censorship of QUIC [37]. This was later confirmed by analyses by Elmenhorst [15] and Xue et al. [45]. While Elmenhorst et al. also described SNI-specific censorship for Russia's domestic traffic [16], this behavior was only anecdotally described for its international traffic [12].

Research Gap. During regular censorship tests in Russia, we observed that Russia has disabled its broad QUIC filter and instead censors QUIC traffic based on the domain in the SNI extension. Afterward, we detected anecdotal evidence of this switch in Russian-language forums. Despite anecdotal evidence, we could neither discern an existing timeline of Russia's QUIC censorship nor a description of its current QUIC censorship behavior.

Contributions. To close the aforementioned research gap, we analyzed Russia's international QUIC SNI censorship—which has previously only been discussed on Russian-language forums. We provide a detailed timeline of Russia's QUIC censorship in Section 2 and portray its current state in Section 3. Through our analyses, we make the following findings about Russia's international QUIC SNI censorship:

- It started between May 2022 and July 2023—at least 9 months before the first reports of China's GFW targeting QUIC [46].
- It was discussed in isolation but went unnoticed by the broader community.
- Its blocklist closely matches Russia's TLS censorship.
- It employs packet dropping and residual censorship.
- It exhibits domain-specific behavior.

2 Timeline of QUIC Censorship in Russia

To retrospectively identify the start of Russia's QUIC SNI blocking, we reconstruct the timeline of QUIC censorship in Russia. We collected past QUIC censorship observations, particularly from Russian-language forum posts, and contextualized our findings with QUIC traffic data from Cloudflare Radar [13]. Figure 1 depicts a consolidated timeline of Russian QUIC censorship, highlighting three major time periods. Until February 2022, QUIC traffic in Russia was not censored (**Period A**). By March 2022, Russia likely

Free and Open Communications on the Internet 2026(2), 1–6

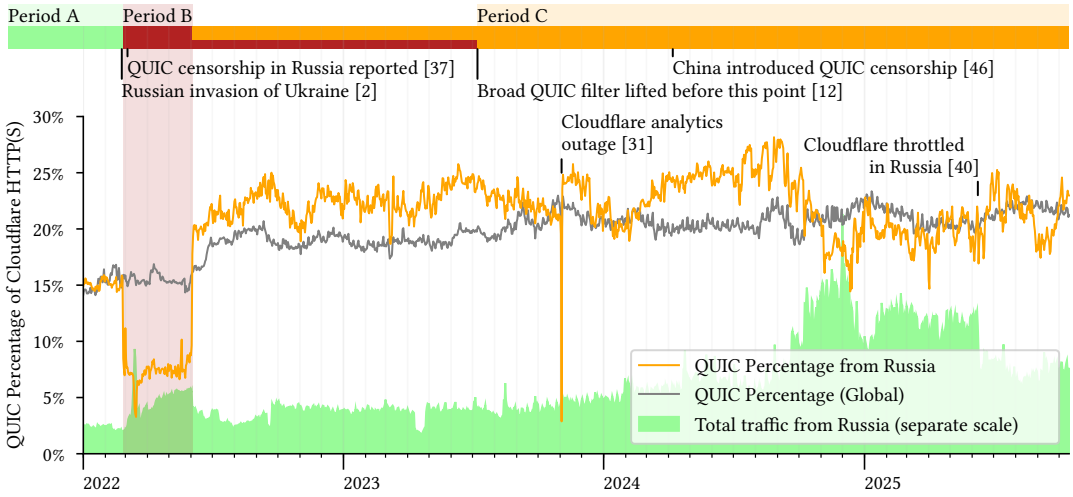

Figure 1: Timeline of QUIC censorship in Russia reconstructed from forum posts and data provided by Cloudflare. The timeline shows the total number of HTTP(s) requests from Russia to Cloudflare and QUIC usage as a percentage of requests to Cloudflare, archived from Cloudflare Radar [13]; Cloudflare does not report absolute traffic statistics. The shaded red area highlights a drop in QUIC traffic from February 26, 2022 to June 3, 2022, where broad QUIC censorship was likely present (Period B, see Section 2.2). After Russia lifted the broad QUIC filter, they used an SNI-based filter (Period C, see Section 2.3).

started dropping all international QUIC traffic (**Period B**)—this coincides with Russia's full-scale invasion of Ukraine. Between May 2022 and July 2023, Russia switched from dropping all QUIC traffic to dropping only QUIC traffic with an SNI containing a forbidden domain (**Period C**). Below, we detail each period.

2.1 No QUIC-specific Censorship (Period A)

We found no evidence of Russian QUIC censorship prior to February 2022. Since QUIC was standardized in May 2021, it has been uncensored in Russia for approximately 9 months. Simultaneously, TLS was censored in Russia through widely installed TSPU devices [45]. As browsers would infer a website's QUIC support over the `Alt-Svc` header in an earlier TLS connection [7], TLS censorship might have impacted QUIC accessibility in Russia. Similarly, potential DNS censorship might have prevented clients from determining websites' QUIC support via early deployments of `HTTPS` records [36].

2.2 Broad QUIC Blocking (Period B)

On March 4, 2022, users first reported that Russia enabled QUIC-specific censorship by dropping all international QUIC traffic [37]. This is corroborated by QUIC traffic from Russia to Cloudflare dropping 46% [13] compared to HTTP over TLS/TCP a few days earlier [38]—on February 26, 2022, two days after Russia's full-scale invasion of Ukraine.

Russia identified, and subsequently dropped, all international QUIC traffic via QUIC's Initial packets [21]. TSPU devices analyzed all UDP flows destined to port 443 [41, 45] that originated in Russia [11]. A flow was blocked when the first packet was at least 1001 bytes long and contained the four-byte version header for QUIC version 1 (`0x00000001`) [41, 45]. The TSPU maintained state for UDP flows for 420 seconds [45] and residually censored the UDP flow: All following packets with the same IPs and ports were dropped during this time. If the first packet did not trigger censorship, the flow was not analyzed further—a phenomenon we call residual clearance. Similar to other censorship by the TSPU devices, flows that began outside of Russia were unaffected [11].

SNI-based Filtering Within Russia. While international QUIC traffic was entirely blocked in Russia, national QUIC traffic exhibited SNI-specific blocking. This was first reported anecdotally for the Russian social media site vk.com on March 4, 2022 [37]. Elmenhorst analyzed this special case in March 2022. They confirmed that the TSPU devices could decrypt QUIC Initial packets and extract the hostname located in the SNI [14, 15].

2.3 International SNI-based QUIC Censorship (Period C)

We strongly believe that since at least July 2023, Russia has disabled international QUIC traffic dropping and switched to fine-grained SNI-based QUIC censorship, as supported by forum posts and data independently provided by Cloudflare [12, 13]. To extract the SNI, TSPU devices analyzed the first packet of all UDP flows, limited to destination port 443 [12]. They decrypted the QUIC Initial packet, and, if the domain was forbidden, dropped the packet and all following packets on the UDP flow for an unknown duration. If the first packet did not trigger censorship, the rest of the connection was residually cleared.

When was the Broad Filter Lifted? User reports indicate that Russia switched from broad to SNI-specific QUIC filtering somewhere between May 2022 and July 2023 [3, 12]. Although we cannot determine exactly when the broad filter was lifted, Cloudflare's traffic reports indicate it occurred on June 3, 2022 in many areas of Russia. On that day, QUIC usage in Russia returned to pre-block levels (see

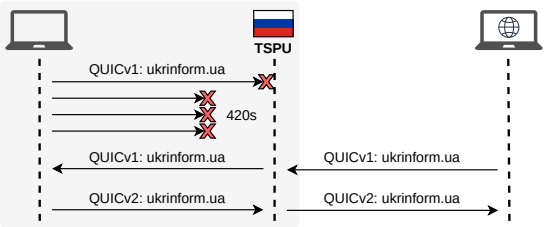

Figure 2: Russia blocks QUICv1 Initial Packets if the SNI extension in the request contains a censored domain. QUICv2 is not affected. After blocking an Initial Packet, the Russian censor drops subsequent packets on the same 4-tuple for 420 seconds. Subsequent packets reset the timer. All censorship, including residual, is unidirectional: Traffic that enters Russia is never censored.

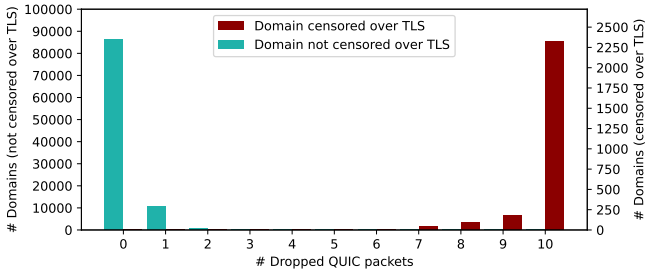

Figure 3: Number of censored QUIC connections out of 10 per domain from the Tranco Top 100k list.[2] Domains accessible via TLS are also accessible via QUIC (light blue bars). Domains blocked via TLS are also blocked via QUIC (dark red bars). The variance indicates that both the network and the Russian QUIC censorship are unreliable.

Figure 1). Despite a small drop in overall traffic from Russia, the absolute QUIC traffic increased by at least 38% on that day alone [13]. As this timing is corroborated by a forum post [4], we suspect that Russia lifted its broad QUIC filter on June 3, 2022. A third source independently reports it being lifted by July 8, 2023 [12].

SNI-based Throttling. In addition to blocking domains, the SNI in QUIC packets was used as a trigger to throttle traffic to YouTube. The throttling via QUIC had started by July 18, 2024 [43]—one week after TLS throttling [26]. The throttled bandwidth was inconsistent across Russia. On August 8, 2024, YouTube was blocked completely, via SNI-based blocking in TLS [24]. It is unclear whether QUIC was affected initially, but at least one Internet provider also blocked YouTube via QUIC by April 18, 2025 [27].

3 Current QUIC Censorship in Russia

To evaluate Russia's current QUIC censorship, we sent QUIC Initial packets from vantage points in three Russian cities (see Appendix A) to a vantage point under our control in Germany. We ran our measurements in March and April 2026, and found identical behavior across our three Russian vantage points. We provide pcap files that show our key results on GitHub.[1]

SNI Censorship. Our measurements show that Russia censors QUIC connections based on their target domain: Instead of blocking all QUIC connections, Russia's censor now decrypts the QUIC Initial packets, locates the SNI extension in the embedded TLS handshake, and blocks the connection if the domain should be censored (see Figure 2). To this end, it drops packets with unwanted domains in the SNI extension. Therefore, Russia's QUIC censorship must operate in-path. This is similar to Russian TLS censorship, which drops `ClientHello` messages with unwanted domains [34].

Censorship Details. We determined that Russian QUIC censorship employs residual censorship on the 4-tuple (src IP, src port, dst IP, dst port) for 420 seconds—sending additional messages resets the timer. It operates unidirectionally, only targeting traffic leaving the country. Interestingly, it targets only QUICv1; the standardized update QUICv2 is not censored, facilitating potential circumvention at all our vantage points (see Table 2).

Affected Ports. Russia's broad QUIC censorship (see Section 2.2) and initial SNI-based censorship (see Section 2.3) only affected port 443 [12, 41, 45]. Russia's current QUIC censorship is not limited to port 443; we detected QUIC censorship on random ports, up to port 65535. We found all destination ports to be affected at two of our vantage points (Saint Petersburg and Novosibirsk). In Moscow, 22% of the system ports (1–1023) were not targeted by censorship. Notably, the ports relevant to QUIC are targeted at all locations: 443 (HTTP/3) and 853 (DNS over QUIC).

Blocked Domains. We compared Russian TLS and QUIC censorship of domains on the Tranco Top 100k list.[2] We sent TLS `ClientHello` messages and QUIC Initial Packets containing the tested domain in the SNI extension from our Russian vantage points[3] to our vantage point in Germany. To reduce false positives and false negatives, we tested each domain 10 times and randomized the execution order. We determined that Russia censored TLS through packet dropping for 2,644 domains.[4] Figure 3 shows that these domains are also blocked over QUIC. Similarly, domains that are not blocked over TLS are also not blocked over QUIC. Our results are highly consistent with blocklists for TLS and QUIC being equal.

Location of Censorship Devices. We manually validated the location of the QUIC censorship devices by gradually increasing the TTL of our packets and measuring ICMP responses [32]. From our vantage point in Moscow, all QUIC censorship occurred between the third and fourth hop, which lay in Moscow and outside of Russia, respectively. At all vantage points, the TLS and QUIC censorship we measured were located at the same hop. We strongly suspect the censorship devices to be Russian TSPU devices described by Xue et al. [45].

Comparison to China's QUIC Censorship. SNI-based QUIC censorship has previously been described for the GFW by Zohaib et

[1] https://github.com/UPB-SysSec/RussiaQuicResults

[2] Tranco list L7684, March 12, 2026, available at https://tranco-list.eu/list/L7684.

[3] Due to RAM limitations, we were unable to run this experiment on our vantage point in Novosibirsk.

[4] This corresponds to the type "SNI-Based (IV)" described by Xue et al. [45].

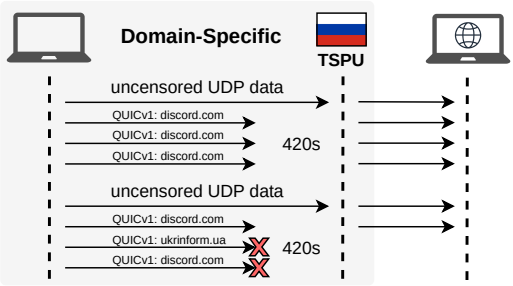

Figure 4: For selected domains, Russian QUIC censorship does not trigger if uncensored data was sent over the same 4-tuple. After 420 seconds, the residual clearance ends. Notably, censorship of unaffected domains still triggers residual censorship that overwrites the residual clearance.

al. [46]. Both—the Russian censor and the GFW—censor QUIC by dropping packets. A key difference is that the Russian censor drops the initial packets and immediately enforces residual censorship, while the GFW allows the initial packet to pass and only enforces residual censorship after a short delay. This mirrors the different designs of the Russian TSPU devices [45] and the GFW, which perform packet inspection in-path and on-path, respectively. Further similarities are that both do not limit their censorship to port 443, do not censor QUICv2, and only censor outgoing traffic—the GFW disabled bidirectional QUIC censorship in September 2024. Appendix B details QUIC parsing differences between Russia and China, and shows that some circumventions that worked in China [46] are not successful in Russia (payload no. 8).

Domain-specific Behavior. In our evaluations, some domains exhibited different blocking behavior. For instance, QUIC connections containing discord.com were subject to residual clearance: They were not censored over QUIC when preceded by non-censored data. Figure 4 depicts this behavior. We stress that in our evaluations, only a few domains were affected by this behavior. Some of these domains also triggered distinct behavior in previous work [42, 45]. Another example of domain-specific behavior is port-specific blocking: In our evaluations, some domains were only blocked on port 443. We refer to Appendix C for a list of domain-specific behaviors. All domains that triggered domain-specific behavior were blocked at the same network hop as other QUIC traffic. We speculate that complex configuration options or multiple TSPU devices with differing configurations are the cause of domain-specific QUIC behavior.

4 Discussion and Future Work

Public Knowledge, but Not Discussed. The initial broad QUIC filter in Russia was well-known [14, 15, 38, 45], but the switch to SNI-based censorship was only discussed on Russian-language forums [37]. The broad filter was well-understood by the time it was lifted, so there may have been little reason for international researchers to continue analyzing Russia's QUIC censorship. At the same time, the SNI-based filter received little attention, possibly because it initially only applied to domestic traffic. Notably, as of 2025, widespread SNI-based censorship in Russia was unknown in scientific literature [46].

Russia Censored QUIC SNI Before China. China's international QUIC SNI censor has been reported as the first of its kind [46]. In this work, we note that Russia's QUIC SNI censorship was very likely deployed at least 9 months prior, and even earlier domestically. This aligns with previous findings about Russia adapting to new protocols before China [28]. Other earlier QUIC SNI censors might exist: In 2025, a leak of internal documents of the company Geedge revealed code for QUIC-specific censorship [44]. Geedge has customers in Ethiopia, Kazakhstan, Myanmar, and Pakistan [44]. This implies that more censors—especially those using Geedge's software—already have or may gain support to censor QUIC.

Identifying Circumvention Techniques. The rising number of QUIC censors highlights the need for QUIC censorship circumvention. Like in the GFW's QUIC censorship [46], parsing QUIC Initial packets and ClientHello opens avenues for circumvention (see Appendix B). For example, Zohaib et al. [46] identified fragmenting the `ClientHello` as a successful circumvention for the GFW. Successful modifications in Russia—like using QUICv2—show that their QUIC parser is also incomplete. We advocate for future work to evaluate QUIC censors for circumvention techniques.

TSPU Uniformity. Russia's TSPU infrastructure is highly uniform [45], implying that measurements from our three vantage points likely generalize beyond the vantage points' network providers. Nevertheless, there may be exceptions, as for the initial broad QUIC filter, which did not apply to all traffic from Russia (see Figure 1).

Ethical Considerations. Our scans aim to minimize the risks imposed on Russian individuals. To this end, we rented vantage points in Russia and sent traffic only between servers under our control. We took care to minimize the number of vantage points rented in Russia, and complied with all applicable sanctions [17]. Although our findings might be used by Russia to modify the TSPU, we strongly believe the direct benefit to their people and the censorship circumvention community outweighs this risk.

5 Conclusions

In this paper, we reconstruct a timeline of Russian QUIC censorship and detail its current state. We identify that Russia switched from a broad block of all international QUIC traffic to SNI-dependent QUIC censorship between May 2022 and July 2023. This SNI-dependent QUIC censorship persists to this day and is characterized by packet drops, long residual censorship, and domain-specific behavior. We stress that Russia's SNI-dependent QUIC censorship went largely unnoticed for three years. Russia also started censoring QUIC via the SNI at least nine months before China's GFW—the first academically discussed SNI-dependent QUIC censor. We advocate for an analysis of potentially unnoticed QUIC censorship in other countries and emphasize the need for usable circumvention techniques.

Acknowledgments

We want to thank the reviewers for their insightful comments and constructive feedback. We also thank all individuals who provided evidence for Russian QUIC censorship in forums and other discussion spaces. Niklas Niere was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 555828767.

References

[1] D. Eastlake 3rd. 2011. *Transport Layer Security (TLS) Extensions: Extension Definitions*. RFC 6066. IETF. http://tools.ietf.org/rfc/rfc6066.txt

[2] Al Jazeera. 2022. Russian forces launch full-scale invasion of Ukraine. https://www.aljazeera.com/news/2022/2/24/putin-orders-military-operations-in-eastern-ukraine-as-un-meets

[3] anonymous28. 2022. Forum Post: "Система может расшифровать QUIC_V1 и декодировать SNI.". https://ntc.party/t/1823/32

[4] anonymous57. 2022. Forum Post: "Локалхост в надежных руках. [...]". https://ntc.party/t/1823/69

[5] Daniil Belovodyev, Andrei Soshnikov, Reid Standish, and Systema. 2023. Leaked Files Show China And Russia Sharing Tactics On Internet Control, Censorship. *Radio Free Europe/Radio Liberty* (April 2023). https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html

[6] M. Bishop. 2022. *HTTP/3*. RFC 9114. IETF. http://tools.ietf.org/rfc/rfc9114.txt

[7] Mike Bishop. 2022. *HTTP/3*. Request for Comments RFC 9114. Internet Engineering Task Force. https://doi.org/10.17487/RFC9114

[8] Kevin Bock, George Hughey, Xiao Qiang, and Dave Levin. 2019. Geneva: Evolving Censorship Evasion Strategies. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association for Computing Machinery, New York, NY, USA, 2199–2214. https://doi.org/10.1145/3319535.3363189

[9] Kevin Bock, iyouport, Anonymous, Louis-Henri Merino, David Fifield, Amir Houmansadr, and Dave Levin. 2020. Exposing and Circumventing China's Censorship of ESNI. https://gfw.report/blog/gfw_esni_blocking/en/

[10] Kevin Bock, Gabriel Naval, Kyle Reese, and Dave Levin. 2021. Even Censors Have a Backup: Examining China's Double HTTPS Censorship Middleboxes. In *Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet (FOCI '21)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3473604.3474559

[11] bolvan. 2022. Forum Post: "Подтверждаю. Добавлю к этому, что к входящим пакетам фильтрация не применяется и используется stateful фильтр. [. . .]". https://ntc.party/t/1823/11

[12] bolvan. 2023. Forum Post: "Текущая ситуация по QUIC примерно такая. [. . .]". https://ntc.party/t/1823/74

[13] Cloudflare. 2025. Cloudflare Radar. https://radar.cloudflare.com/

[14] Kathrin Elmenhorst. 2022. Broad blocking of HTTP/3 traffic in Russia (AS31213, AS12389). https://github.com/kelmenhorst/quic-censorship/issues/4

[15] Kathrin Elmenhorst. 2022. A Quick Look at QUIC Censorship. https://www.opentech.fund/news/a-quick-look-at-quic-censorship/

[16] Kathrin Elmenhorst, Bertram Schütz, Nils Aschenbruck, and Simone Basso. 2021. Web censorship measurements of HTTP/3 over QUIC. In *Proceedings of the 21st ACM Internet Measurement Conference (IMC '21)*. Association for Computing Machinery, New York, NY, USA, 276–282. https://doi.org/10.1145/3487552.3487836

[17] European Commission. 2026. EU Sanctions Map. https://sanctionsmap.eu/

[18] Freedom House. 2024. Freedom on the Net 2024. https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online

[19] Huston Geoff. 2025. A QUIC Progress Report | blabs. https://labs.apnic.net/index.php/2025/06/16/a-quic-progress-report/

[20] Michael Harrity, Kevin Bock, Frederick Sell, and Dave Levin. 2022. GET /out: Automated Discovery of Application-Layer Censorship Evasion Strategies. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 465–483. https://www.usenix.org/conference/usenixsecurity22/presentation/harrity

[21] J. Iyengar and M. Thomson. 2021. *QUIC: A UDP-Based Multiplexed and Secure Transport*. RFC 9000. IETF. http://tools.ietf.org/rfc/rfc9000.txt

[22] Anastasiia Kruope. 2025. Disrupted, Throttled, and Blocked. https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation

[23] Ruixuan Li, Baojun Liu, Chaoyi Lu, Haixin Duan, and Jun Shao. 2024. A Worldwide View on the Reachability of Encrypted DNS Services. In *Proceedings of the ACM Web Conference 2024*. ACM, Singapore Singapore, 1193–1202. https://doi.org/10.1145/3589334.3645539

[24] loskiq. 2024. Forum Post: "видимо, начали блочить домен www.youtube.com по SNI [. . .]". https://ntc.party/t/8055/145

[25] Alexander Master and Christina Garman. 2023. A Worldwide View of Nation-state Internet Censorship. *Free and Open Communications on the Internet* (2023). https://petsymposium.org/foci/2023/foci-2023-0008.php

[26] Meduza. 2024. В России, как заявил источник «Медузы», начали замедлять YouTube. «Ростелеком» утверждает, что возникли проблемы в работе оборудования Google. https://meduza.io/feature/2024/07/12/v-rossii-kak-zayavil-istochnik-meduzy-nachali-zamedlyat-youtube-rostelekom-utverzhdaet-chto-voznikli-problemy-v-rabote-oborudovaniya-google

[27] Molchun. 2025. Forum Post: "В то время как на йоте полный блок ВСЕХ ресурсов. [. . .]". https://ntc.party/t/8055/337

[28] Niklas Niere, Felix Lange, Nico Heitmann, and Juraj Somorovsky. 2025. Encrypted Client Hello (ECH) in Censorship Circumvention. *Free and Open Communications on the Internet* (2025). https://www.petsymposium.org/foci/2025/foci-2025-0016.php

[29] Niklas Niere, Felix Lange, Robert Merget, and Juraj Somorovsky. 2025. Transport Layer Obscurity: Circumventing SNI Censorship on the TLS-Layer. In *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, San Francisco, CA, USA, 1344–1362. https://doi.org/10.1109/SP61157.2025.00151

[30] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global Measurement of DNS Manipulation. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, Canada, 307–323. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/pearce

[31] Matthew Prince. 2023. Post mortem on the Cloudflare Control Plane and Analytics Outage. https://blog.cloudflare.com/post-mortem-on-cloudflare-control-plane-and-analytics-outage/

[32] Ram Sundara Raman, Mona Wang, Jakub Dalek, Jonathan Mayer, and Roya Ensafi. 2022. Network measurement methods for locating and examining censorship devices. In *Proceedings of the 18th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '22)*. Association for Computing Machinery, New York, NY, USA, 18–34. https://doi.org/10.1145/3555050.3569133

[33] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. 2020. Decentralized Control: A Case Study of Russia. In *Proceedings 2020 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2020.23098

[34] Reethika Ramesh, Ram Sundara Raman, Apurva Virkud, Alexandra Dirksen, Armin Huremagic, David Fifield, Dirk Rodenburg, Rod Hynes, Doug Madory, and Roya Ensafi. 2023. Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, USA, 2581–2598. https://www.usenix.org/conference/usenixsecurity23/presentation/ramesh-network-responses

[35] E. Rescorla. 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. IETF. http://tools.ietf.org/rfc/rfc8446.txt

[36] Benjamin M. Schwartz, Mike Bishop, and Erik Nygren. 2023. *Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)*. Request for Comments RFC 9460. Internet Engineering Task Force. https://doi.org/10.17487/RFC9460

[37] serfreeman1337. 2022. Forum Post: "Не устанавливается соединение по QUIC для зарубежных сайтов. [. . .]". https://ntc.party/t/1823/1

[38] Max Stucchi and Robin Wilton. 2022. QUIC vs TLS on Russian Networks. https://pulse.internetsociety.org/blog/internet-perspectives-ukraine-and-russia#QUIC

[39] M. Thomson and S. Turner. 2021. *Using TLS to Secure QUIC*. RFC 9001. IETF. http://tools.ietf.org/rfc/rfc9001.txt

[40] Michael Tremante and Alissa Starzak. 2025. Russian Internet users are unable to access the open Internet. https://blog.cloudflare.com/russian-internet-users-are-unable-to-access-the-open-internet/

[41] ValdikSS. 2022. Forum Post: "Фильтр работает только для пакетов с UDP-нагрузкой больше 1001 байтов (включительно). [. . .]". https://ntc.party/t/1823/10

[42] ValdikSS. 2024. Forum Post: "Замедляют по SNI *.googlevideo.com — домена, с которого раздаётся видео YouTube,". https://ntc.party/t/8055/2

[43] ValdikSS. 2024. Forum Post: "Начали замедлять и QUIC (HTTP/3) тоже. [. . .]". https://ntc.party/t/8055/79

[44] wkrp. 2025. Leak of Geedge Networks internal documents (100,000+ from Jira, Confluence, GitLab) · Issue #519 · net4people/bbs. https://github.com/net4people/bbs/issues/519

[45] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi. 2022. TSPU: Russia's decentralized censorship system. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22)*. Association for Computing Machinery, New York, NY, USA, 179–194. https://doi.org/10.1145/3517745.3561461

[46] Ali Zohaib, Qiang Zao, Jackson Sippe, Abdulrahman Alaraj, Amir Houmansadr, Zakir Durumeric, and Eric Wustrow. 2025. Exposing and Circumventing SNI-based QUIC Censorship of the Great Firewall of China. In *34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, Seattle, WA, USA, 783–802. https://www.usenix.org/conference/usenixsecurity25/presentation/zohaib

A Vantage Points

Table 1: Location of the vantage points used in our evaluations. We rented vantage points in Russia's three largest cities, and rented one in Germany as our scan target.

Abbr.	Location	AS Number
MOW	Moscow	50867
SPE	Saint Petersburg	214822
NVS	Novosibirsk	214822
–	Berlin, Germany	8560

B QUIC Parsing Tests

We reproduced the parsing tests by Zohaib et al. [46] in Russia, using `ukrinform.ua` as the censored domain. Table 2 shows that the blocking behavior matches across all our vantage points for all payloads and differs between Russia and China [46].

For consistency among the payloads, we made minor modifications. We included padding to 1200 bytes and a complete ClientHello in all payloads. In payload 7, we included an innocuous SNI instead of removing the SNI altogether. Zohaib et al.'s description of payload 5 diverges from the payload given in their artifacts; we include both variants.

Table 2: Results from adapting Zohaib et al.'s parsing payloads [46] for our scans from Russia. The blocking behavior was consistent across all our Russian vantage points and differs from the censorship observed in China.

No.	Description	Blocked? MOW	SPE	NVS	[46]
1	Regular Initial with censored SNI	●	●	●	●
2	Remove last byte	●	●	●	○
3	Version bytes `00000002`, invalid MAC	○	○	○	○
4	SCID & DCID empty (length 0)	○	○	○	●
5	DCID set to length 255	○	○	○	○
–	SCID set to length 255	○	○	○	–
6	Crypto frame len. 0, data unchanged	○	○	○	●
7	ALPN with censored hostname	○	○	○	○
8	PING & PADDING before/after Crypto	●	●	●	○
9	ECH, outer SNI `cloudflare-ech.com`	○	○	○	○
10	QUIC version 2	○	○	○	○

MOW: Moscow SPE: Saint Petersburg NVS: Novosibirsk
○ not blocked ● blocked

C Domain-specific Behavior

Table 3: Domain-specific blocking behavior. We detected 22 domains that triggered censorship only on port 443, and 31 patterns that passed the TSPU if the flow was cleared by an uncensored first packet.

Domain	443 Only	Residual Clearance
default	○	○
discord.com	●	●
discordapp.com	●	●
napps-1.com	●	●
napps-2.com	●	●
nordaccount.com	●	●
nordlayer.com	●	●
nordpass.com	●	●
fralcks.com	●	●
gillsonse.com	●	●
horizono.xyz	●	●
janetvill.com	●	●
maleyu.org	●	●
oakdenet.com	●	●
seagrav.com	●	●
valentiae.com	●	●
viewlak.com	●	●
wirevpn.app	●	●
icpsuawn1zy5amys.com	●	●
njtzzrvg0lwj3bsn.info	●	●
p99nxpivfscyverz.me	●	●
x9fnzrtl4x8pynsf.com	●	●
zwyr157wwiu6eior.com	●	●
*.googlevideo.com	○	●
news.google.com	○	●
play.google.com	○	●
totallyacdn.com	○	●
whiskergalaxy.com	○	●
deepstateplatypus.com	○	●
hubstack.net	○	●
mariberimajinasi.store	○	●
xhentai.tv	○	●

○ absent ● present (different than default behavior)