Encrypted Client Hello (ECH) in Censorship Circumvention

Niklas Niere
Paderborn University
Paderborn, NRW, Germany
niklas.niere@upb.de

Felix Lange
Paderborn University
Paderborn, NRW, Germany
felix.lange@upb.de

Nico Heitmann
Paderborn University
Paderborn, NRW, Germany
nico.heitmann@upb.de

Juraj Somorovsky
Paderborn University
Paderborn, NRW, Germany
juraj.somorovsky@upb.de

Abstract

Censors have long censored Transport Layer Security (TLS) traffic by inspecting the domain name in the unencrypted Server Name Indication (SNI) extension. By encrypting the SNI extension, the Encrypted `ClientHello` (ECH) prevents censors from blocking TLS traffic to certain domains. Despite this promising outlook, ECH's current capability to contest TLS censorship is unclear; for instance, Russia has started censoring ECH connections successfully. This paper clarifies ECH's current role for TLS censorship. To this end, we evaluate servers' support for ECH and its analysis and subsequent blocking by censors. We determine Cloudflare as the only major provider supporting ECH. Additionally, we affirm previously known ECH censorship in Russia and uncover indirect censorship of ECH through encrypted DNS censorship in China and Iran. Our findings suggest that ECH's contribution to censorship circumvention is currently limited: we consider ECH's dependence on encrypted DNS especially challenging for ECH's capability to circumvent censorship. We stress the importance of censorship-resistant ECH to solve the long-known problem of SNI-based TLS censorship.

Keywords

censorship, circumvention, ECH, TLS

1 Introduction

Various countries censor websites or services on the Internet [32]. For instance, the Great Firewall of China (GFW) [2, 7, 9, 15, 21, 49], Iran [4, 5, 27, 33], and Russia [41, 42, 52, 53] censor a vast number of websites by analyzing and subsequently interrupting traffic of various protocols. So-called deep packet inspection (DPI) targets unencrypted protocols—e.g., DNS [15, 39] and HTTP [4, 19]—and encrypted protocols—e.g., TLS [6, 52] and QUIC [20, 52]—alike. This holistic approach to censorship allows censors to adapt to new protocols. As such, the introduction of Transport Layer Security (TLS) [1] led to the widespread encryption of HTTP [35] traffic [30]: previously censoring unencrypted HTTP traffic, censors started to target the TLS protocol and its extensions.

TLS Censorship. The TLS protocol [12, 43] encrypts application data, such as HTTP, and prevents its analysis by censors. While TLS prevents censors from extracting the content of a website, it leaks the domain name of the accessed website through the Server Name Indication (SNI) extension [13]. The SNI extension is transmitted unencrypted in the first message sent by the client to the TLS server. Similar to the SNI extension, the unencrypted ALPN extension [17] reveals the encrypted application protocol. The unencrypted transmission of the ALPN and SNI extensions allows censors to block TLS-encrypted traffic based on the accessed domain and the used protocol.

ECH. To prevent middleboxes from analyzing the domain name in the unencrypted SNI extension, the IETF is drafting the Encrypted `ClientHello` (ECH) extension [45]. In a previous version, the ECH extension—called Encrypted Server Name Indication (ESNI) at that point—encrypted only the SNI extension [44]. To encrypt other sensitive extensions, such as the ALPN extension, the ECH extension has been changed to encrypt the entire `ClientHello` message with all included extensions. The keys used in this encryption are provided to clients over so-called HTTPS DNS records. The encryption of the `ClientHello` message prevents censors from blocking TLS connections based on the accessed domain and protocol. Despite the availability of the ECH extension, censorship cannot be fully prevented. For instance, Russian TSPU devices started blocking all ECH connections to Cloudflare in November 2024 [38, 48]. Similarly, China and Russia blocked the previously drafted ESNI extension [7, 22]. Censors can also block ECH by preventing a client from collecting the server's ECH configuration from the DNS server— over unencrypted or encrypted DNS. In light of apparent ECH censorship, ECH's role in TLS censorship circumvention remains unclear.

Research Gap. An important step to prevent censorship of the TLS protocol is the encryption of the `ClientHello` message—and most importantly the SNI extension [8]. While the ECH extension provides this encryption, its practical aid for censorship circumvention is currently uncertain. Previous studies focused on the censorship of the ESNI extension in 2020 [7] and 2022 [22], and TLS servers' support for the ESNI and ECH extensions in 2023 [47, 54]. Since then, several noteworthy changes occurred: the RFC draft has been updated—updating the ESNI extension to the ECH extension, Cloudflare has announced support for the ECH extension [23], and Russian TSPU devices have started censoring ECH connections to Cloudflare [38, 48]. In the wake of these changes, we consider an

Free and Open Communications on the Internet 2025(2), 64–73

updated view on ECH support by TLS servers and censors' behavior on the ECH extension necessary. From this updated view, we expect to be able to determine ECH's current role in censorship circumvention. In 2022, Hoang et al. [22] linked hostname encryption in TLS via ESNI and hostname encryption in DNS via encrypted DNS: to effectively circumvent censorship, the censored hostname would have to be encrypted in both places. In this paper, we confirm this link by showing effective ECH censorship through DNS censorship.

Methodology. To determine ECH's current role for censorship circumvention, we seek the answers to the following research questions.

RQ1: What is the current support for ECH by TLS servers?

RQ2: How do censors prevent the usage of the ECH extension?

To answer these research questions, we evaluate TLS servers' support of the ECH extension by evaluating TLS servers from the Tranco Top 1M list [28]. Over 4 months, we determine the advertisement of ECH on DNS servers by servers on the daily Tranco Top 1M list. We further determine the acceptance of various ECH handshakes by servers of the Tranco Top 1M list generated on 16th February 2025.[1] To determine censorship of the ECH extension, we send ECH handshakes through censors in China, Iran, and Russia, and evaluate ECH's interplay with DNS censorship. Finally, we discuss ECH's current role in censorship circumvention.

Findings. Our evaluations reveal that ECH's benefit for censorship circumvention is limited: TLS server support of ECH is restricted to Cloudflare, and almost a third of Cloudflare's servers do not advertise their support for it—preventing browsers from handshaking ECH with the server. Concurrently, ECH is censored in Russia, Iran, and China. Russian TSPU devices censor the ECH extension in connections to Cloudflare, proving fast adaptation capabilities of the Russian censor. China and Iran prevent ECH usage by censoring unencrypted and encrypted DNS, showing that, instead of solving the problem of SNI censorship, ECH shifts censorship efforts to encrypted DNS and the ECH extension—similar to how TLS shifted censorship of HTTP to the SNI extension. Nevertheless, we could circumvent the censorship encountered in all three countries. Motivated by our findings, we consider censorship circumvention techniques for ECH censorship, SNI censorship, and DNS censorship highly important for the future.

Contributions. In this paper, we contribute the following:

- We present a longitudinal analysis of ECH configuration advertisement on DNS servers.
- We determine TLS server's acceptance of various ECH handshakes.
- We provide novel findings about ECH censorship in Russia and describe ECH censorship through the censorship of encrypted DNS in China and Iran.

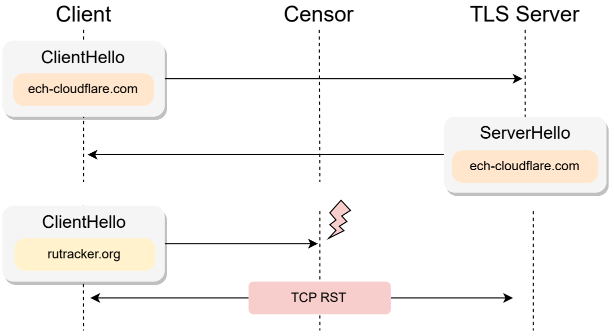

Figure 1: Two ClientHello messages sent to a TLS server. The SNI of the second ClientHello message triggers interruption by the censor. Censors can utilize the SNI extension to prevent TLS connections to specific domains.

2 Background

2.1 Encrypted Client Hello (ECH)

The TLS protocol provides confidentiality and authenticity to otherwise unencrypted protocols, such as HTTP, preventing censors from analyzing their content. Before encrypting application data, TLS performs a key agreement in an unencrypted handshake. In the first—unencrypted—message of the TLS handshake, the client includes the server's domain name in the so-called SNI extension. Censors can extract the server's domain name from the SNI extension and block connections to undesired websites. Figure 1 visualizes this process.

Encrypting the SNI. To prevent a third party from extracting a server's domain name from the SNI extension, the IETF is currently standardizing the encryption of the SNI extension [46]. As TLS 1.2 and previous versions leak the server's domain name over the certificate—offsetting the benefits of ECH—ECH is only specified for TLS 1.3. In previous drafts of the standard [44], the ESNI extension was intended to encrypt only the SNI extension. In the draft's current version—as depicted in Figure 2—the ECH extension encrypts the entire ClientHello extension. The keys used in the encryption are provided in the server's ECH configuration. The client has to query the ECH configuration from a DNS resolver before handshaking ECH, making ECH censorship directly dependent on the censorship of DNS.

ECH Structure. When using ECH to connect to a censored website, the client encrypts the entire ClientHello message, including the censored domain name, using the keys provided in the server's ECH configuration. To maintain middlebox compliance, the client includes the encrypted ClientHello message as an extension inside another unencrypted ClientHello message (cf. Figure 2). The server has two options when receiving such a nested ClientHello message: The server can decrypt the encrypted—inner—ClientHello and handshake for the censored domain, or the server can reject the inner ClientHello and handshake with the unencrypted—outer—ClientHello. For a censor, whether the server handshakes the inner or outer ClientHello message is indistinguishable.

[1] Tranco Top 1M list, https://tranco-list.eu/list/3N4WL, 16.02.2025

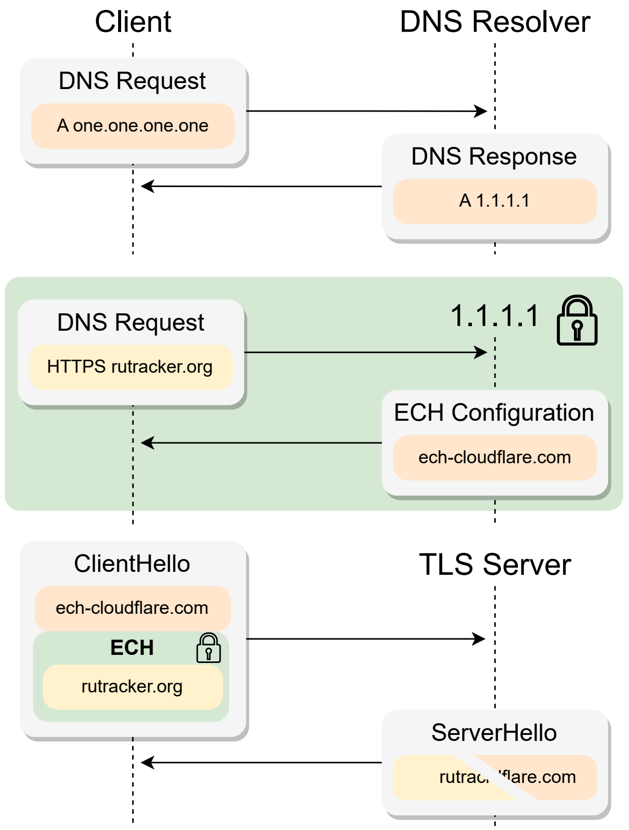

Figure 2: A ECH handshake with preceding encrypted ECH configuration query to a DNS resolver and the domain resolution of the encrypted DNS resolver over unencrypted DNS. The domain ech-cloudflare.com advertised in the server's ECH configuration is included unencrypted in the client's `ClientHello` message and readable by a censor. The domain rutracker.org is encrypted and unreadable to a censor. Both domains can be handshaked by the server.

Outer SNI. To handshake with the outer `ClientHello`, the server has to select a domain name to authenticate with a certificate. The server provides this domain name to the client via its ECH configuration. The standard further requires that clients SHOULD include that hostname in a SNI extension in the unencrypted outer SNI (cf. cloudflare-ech.com in Figure 2). While this eases the handshaking process for clients and servers, it also allows censors to analyze the domain name in the outer `ClientHello`: A censor can crawl ECH configurations for their advertised domain names and block all traffic to a specific provider by blocking their advertised domain names for the SNI extension in the outer `ClientHello`.

GREASE ECH. As discussed above, ECH is realized through an extension in another unencrypted `ClientHello`. A censor that wants to force unencrypted SNI usage could just block all TLS connections that contain an ECH extension. Countering this effect, the standard [46] specifies that clients SHOULD send so-called Generate Random Extensions And Sustain Extensibility (GREASE) ECH extensions containing random data to servers that do not support and ignore ECH. By sending ECH extensions in every `ClientHello` message, clients dissuade censors from blocking the ECH extension, as this would entail widespread overblocking of TLS connections by the censor. Firefox and Chrome implement GREASE ECH and send ECH extensions with every `ClientHello` message. Thus, a censor that blocks all `ClientHello` messages with an ECH extension would block all traffic from Firefox and Chrome.

Summary. Facing ECH, censors are left with three options: The censor can block the clients' initial DNS connection—preventing it from querying the encryption keys for ECH, the censor can block the presence of ECH altogether, and the censor can block specific ECH connections based on the SNI value in the outer `ClientHello`. In this paper, we explore all three types of ECH censorship.

2.2 ECH Browser Support

Despite not being fully standardized, the ECH extension is fully supported by Chrome [18] and Firefox [16]; Safari intends to support it in the future [3]. Below, we describe ECH support in Firefox and Chrome and detail censors' possibilities to block their ECH connections.

To determine a server's support of ECH, Chrome and Firefox query their ECH configuration from the configured DNS resolver. If an unencrypted DNS resolver is configured, censors can preemptively block ECH for Firefox and Chrome by blocking the initial DNS query containing the server's domain in cleartext. If an encrypted DNS resolver is configured, censors can block access to the encrypted DNS resolver (cf. Section 6) or analyze the outer SNI in the ECH handshake. Blocking every `ClientHello` message with an ECH extension is infeasible for censors, as Chrome and Firefox send a GREASE ECH extension in every `ClientHello` message they send. Interestingly, Chrome does not handshake ECH if a proxy server is configured; Firefox only handshakes ECH over a proxy if the proxy uses SOCKSv5 proxy [10]. This prevents ECH from circumventing TLS censorship if IP censorship has to be circumvented concurrently. We positively summarize that ECH and GREASE ECH are enabled by default in Chrome and Firefox, but point out that ECH's interaction with DNS and proxies nevertheless enables censors to block it.

2.3 DNS

Censorship of DNS directly impacts the usability of ECH: To handshake ECH, a client must query the server's ECH configuration from a potentially censored DNS server first. To evade DNS censorship—and enable ECH—a client can choose one of four encrypted DNS protocols: DNS over HTTPS (DoH), DNS over TLS (DoT), DNS over HTTP/3 (DoH3), and DNS over QUIC (DoQ). DoT and DoQ are detectable by censors through their unique port number 853. DoH and DoH3 share port 443 with usual TLS and QUIC servers. When configuring encrypted DNS, Firefox and Chrome first resolve the domain of the encrypted DNS resolver over unencrypted DNS and only then handshakes DoH with the encrypted DNS resolver. By default, Firefox offers two default providers: Cloudflare (mozilla.cloudflare-dns.com) and NextDNS (firefox.dns.nextdns.io).

3 Methodology

To determine ECH's capability to aid in censorship circumvention, we proceeded in three steps. First, we evaluated TLS servers' capability to handshake ECH. Second, we measured TLS servers' daily advertisement of ECH configuration on DNS servers over four months. Third, we determined different types of ECH censorship in China, Russia, and Iran.

3.1 ECH Support

To determine servers' capabilities to handshake ECH, we attempted various ECH handshakes with the TLS servers from the Tranco Top 1M list generated on 16th February 2025.[2] For each server, we ran a variety of tests from a server in the DFN.[3] As a ground truth, we determined whether the server supports TLS 1.3—ECH is only defined for TLS 1.3. To determine a server's implementation support of ECH, we sent two `ClientHello` messages to the server. One `ClientHello` contains an unparseable ECH extension. The other `ClientHello` contains an unknown extension (`0x01FF`) with the same unparseable extension content. If the server answers differently to the messages—for instance, sending an alert in only one case—the server attempts to parse the ECH extension, and we consider the server to have code support for the ECH extension. As servers that support ECH might ignore broken ECH extensions, our methodology yields a lower bound for the number of servers exhibiting code support. For each server, we queried the server's ECH configuration and attempted to handshake ECH with the server's ECH configuration and the latest ECH configuration by Cloudflare. At last, we determined whether the server allows ECH handshakes with incorrect, empty, and missing outer SNI values. These altered ECH handshakes are particularly interesting for censorship circumvention.

3.2 ECH Configuration Advertisement

TLS servers that want to handshake ECH have to provide an ECH configuration containing key material. To gain an overview of ECH across the TLS landscape, we measured TLS servers' advertisement of ECH configurations. An ECH configuration is advertised in the server's HTTPS DNS record. Using ZDNS [26] and a local Unbound resolver—similar to Zirngibl et al. [54]—we queried servers' HTTPS records between November 2024 and April 2025. Each day, we queried the HTTPS records of all TLS servers from the latest Tranco Top 1M list [28]. From each HTTPS record, we extracted potential ECH configurations and their contents, such as the advertised key, the advertised unencrypted domain name, the cipher suite, and the key exchange mechanism.

3.3 ECH Censorship

To determine whether and how ECH aids in censorship circumvention, we evaluated how ECH is censored in China, Iran, and Russia. While ECH prevents censorship of the unencrypted SNI extension, it can be targeted by censors—either through direct blocking or censorship of DNS (cf. Section 2.1). To holistically analyze ECH usability, we evaluated direct censorship of ECH and censorship of encrypted DNS from vantage points in China, Russia, and Iran—see Appendix A for their specifications.

ECH Extension. We determined direct blocking of the ECH extension by sending TLS and QUIC handshakes containing a ECH extension and all outer SNI values advertised in ECH configurations (cf. Section 3.2) from the vantage points in China, Iran, and Russia to three locations: a controlled vantage point in Germany, a TLS server behind Cloudflare's official IP ranges, and a TLS server operated by Cloudflare that is not located behind their official IP ranges.[4] On our controlled vantage point, we set up a TLS server—nginx[5] with OpenSSL 3.0.15[6]—and a QUIC server—aioquic v1.2.0[7] answering our queries. We determined ECH censorship to all three destinations by measuring differences to usual TLS and QUIC handshakes—we provide pcap files of censorship events in a GitHub repository. [8] To gain deeper insights into the censorship mechanisms in each country, we further modified the `ClientHello` handshakes we executed: for instance, we omitted the ECH extension, we omitted the outer SNI value, and split the `ClientHello` message across multiple TCP segments (TCP segmentation) [6] and TLS records (TLS record fragmentation) [36].

Encrypted DNS. We evaluated the impact of encrypted DNS censorship on ECH by measuring the censorship of the DNS resolvers configured in Firefox. While this exemplary analysis is not a complete analysis of encrypted DNS censorship—we discuss this in Section 6.1—it suffices to highlight the connection between the censorship of ECH and encrypted DNS. Firefox provides two default providers: Cloudflare—located at mozilla.cloudflare-dns.com—and NextDNS—located at firefox.dns.nextdns.io. We measure censorship of both providers in China, Iran, and Russia. To this end, we evaluate whether direct connections to the providers are blocked based on the IP and port, and whether their hostnames are blocked in an unencrypted DNS query, in TLS and QUIC handshakes, and in the HTTP Host header.

4 Evaluation Results

In this section, we detail our findings acquired with the methodology described in Section 3 and correlate TLS servers' and censors' handling of the ECH extensions.

4.1 ECH Support

We analyzed servers' capability to handshake ECH from the Tranco Top 1M list in February 2025.

Figure 3 depicts servers' capability of handshaking the ECH extension. We determined a lower bound of 328,541 TLS 1.3 servers that parse the ECH extension—that is 51.28% of all TLS 1.3 servers from the Tranco Top 1M list. Of those, 278,040 servers—43% of TLS 1.3 servers—handshaked with Cloudflare's ECH configuration, six servers handshaked with another, non-Cloudflare ECH configuration, and 50,494 did not handshake with any ECH configuration.

[2] Tranco Top 1M list, https://tranco-list.eu/list/3N4WL, 16.02.2025

[3] German National Research and Education Network, https://www.dfn.de/

[4] IP Ranges | Cloudflare, https://www.cloudflare.com/ips/, Accessed: 10.04.2025

[5] nginx, https://nginx.org/, Accessed: 10.04.2025

[6] OpenSSL Library, https://openssl-library.org/, Accessed: 10.04.2025

[7] aiortc, aioquic, https://github.com/aiortc/aioquic, Accessed: 10.04.2025

[8] GitHub repository containing pcap files, https://github.com/UPB-SysSec/EchCensorshipResults, Created: 04.06.2025

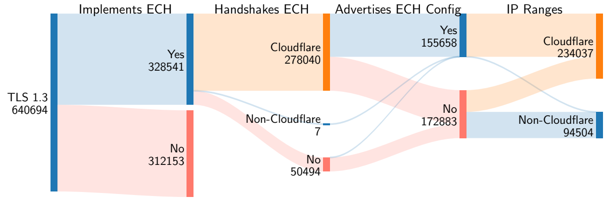

Figure 3: TLS servers' handling of the ECH extension. Support of the ECH extension is driven by Cloudflare, with many servers not advertising their existing support for the ECH extension.

Interestingly, 37,26% of servers that handshaked with the Cloudflare ECH configuration did not advertise it on a DNS resolver. Almost all TLS servers that advertised Cloudflare's ECH configuration also lie in their advertised IP ranges: We suspect a limited advertisement of ECH configurations by providers that manage their own DNS entries. Overall, we measured almost no support for ECH besides Cloudflare servers and detected that 44% of Cloudflare servers do not advertise their ECH configuration despite being able to handshake with it. We suspect that the high number of Cloudflare servers that do not advertise their ECH configuration stems from servers that do not rely on Cloudflare to handle their DNS entries. These servers must re-configure their DNS entries to advertise their ECH configuration; servers that have their DNS entries handled by Cloudflare advertise their ECH configurations automatically.

4.2 ECH Configuration Advertisement

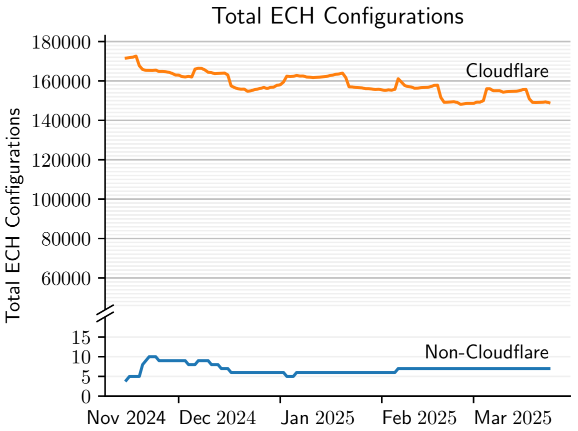

Figure 4: The number of ECH configurations advertised by the Tranco Top 1M servers. Cloudflare issues the vast majority of all ECH Configurations.

We collected the ECH configurations advertised by servers from the Tranco Top 1M list every day from November 2024 until April 2025.

Figure 4 depicts the number of collected ECH configurations over time. Our results show that ECH configurations are almost exclusively advertised by Cloudflare servers—we detail Cloudflare's ECH configuration in the paragraph below—with at most 10 non-Cloudflare servers advertising an ECH configuration on the same day. As Cloudflare is the only large service provider that openly advertises ECH configurations, the overall number of advertised ECH configurations stays below 180,000 each day: this places ECH advertisement for servers on the Tranco list below 18%. Since November 2024, the number of ECH configurations has dropped from almost 180,000 to around 150,000—either through domains leaving Cloudflare's managed IP address space [11] or server owners disabling it themselves [40]. This diminishing advertisement of ECH configurations by TLS servers hinders the usability of ECH as a censorship circumvention technique. Despite Caddy, a popular web server, adopting ECH in April, [9] we could not detect an increase in advertised ECH configurations during follow-up scans.

Non-Cloudflare Configurations. While the vast majority of ECH configurations are advertised by Cloudflare, some non-Cloudflare servers advertise their own ECH configuration. Using `whois` queries, we traced all non-Cloudflare servers that advertised an ECH configuration to the same server operator. Their ECH configurations advertise the same cipher suite and key exchange mechanism as Cloudflare's ECH configurations. They are sparsely updated and often contain an outer SNI not owned by the operator such as google.com and `pornhub.com`. As the server owner can not handshake with these outer SNI values—hampering a usable ECH setup—and these outer SNI values are often subject to censorship, we are unsure about the server owners' objectives behind their ECH deployment.

Cloudflare ECH Configuration. Cloudflare configurations were homogeneous during our evaluation period. For all its servers, Cloudflare advertises the same ECH configuration, which it updates once per hour. With each configuration change, Cloudflare updates the identification number of the configuration and—more importantly—its public key. Other fields in the configuration, such as the used cipher suite (`AES_GCM_128_HKDF_SHA256`) and key exchange mechanism (`DHKEM_X25519_SHA256`), remain unchanged. The outer SNI advertised in Cloudflare's ECH configuration also remains steady: The hostname `cloudflare-ech.com` has been consistently advertised during our whole evaluation. This makes benign ECH connections to Cloudflare trivially distinguishable from GREASE ECH connections to their servers and allows censors to block every ECH connection to Cloudflare by censoring the domain `cloudflare-ech.com` in the SNI extension.

SNI Requirement. Cloudflare's static outer SNI cloudflare-ech.com makes ECH to their servers trivially blockable by censors. Omitting or invalidating the outer SNI from the ECH handshake would prevent censors from analyzing it. To determine the effectiveness of this censorship circumvention technique, we analyzed TLS severs' acceptance of ECH handshakes with invalid outer SNI values. We found that Cloudflare servers require cloudflare-ech.com in the outer SNI and do not accept ECH handshakes with omitted or invalidated outer SNI values. On the contrary, all non-Cloudflare deployments accepted missing and invalidated outer SNIs. Requiring a correct outer SNI value in all ECH handshakes allows censors to block ECH handshakes based on the hostname in the outer SNI.

[9] Caddy, Release v2.10.0, https://github.com/caddyserver/caddy/releases/tag/v2.10.0,

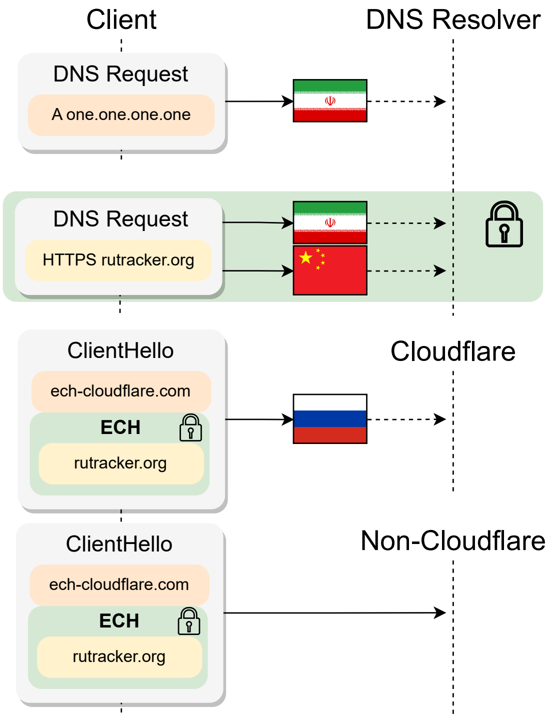

Figure 5: ECH censorship in Iran, China, and Russia. Iran prevents DNS resolution of encrypted DNS servers. China and Iran censor access to encrypted DNS servers through IP blackholing and DPI. Russia blocks ECH handshakes to Cloudflare servers. ECH connections to non-Cloudflare servers are not blocked in either country.

5 ECH Censorship

In March 2025, we analyzed censors in Iran, Russia, and China for their censorship of ECH. Figure 5 depicts the censorship behavior in the three countries. Below, we detail the censorship behavior in each country. We provide pcap files measuring detected censorship in a GitHub repository.[10]

Russia. Russian TSPU devices directly block ECH by dropping the `ClientHello` message containing the ECH extension (cf. Figure 5. To trigger the blocking, the `ClientHello` message has to contain the ECH extension and the hostname cloudflare-ech.com in the SNI extension—other hostnames do not trigger the ECH-specific blocking. The blocking affects both TLS and QUIC traffic. These properties of Russian ECH censorship were described previously [48]. In addition to these previously known properties, we detected that the blocking only occurs in connections to Cloudflare's IP ranges. Notably, TSPU devices do not block ECH connections to servers supporting ECH through Cloudflare but are outside Cloudflare's IP ranges. We confirmed this behavior by sending ECH `ClientHello` messages to 1'500 additional servers located at distinct IP addresses; only messages to IP addresses in Cloudflare's advertised IP ranges were censored. As Russia only censors ECH to Cloudflare's advertised IP ranges, Russian ECH censorship can be circumvented by using an IP proxy located outside Russia and Cloudflare's IP ranges.

Table 1: Censorship of the default Encrypted DNS servers configured in Firefox (●: Censored). China and Iran censor encrypted DNS with DPI, and China also blocks all traffic to IPs of DNS resolvers (IP Blackholing).

	Cloudflare[1]			NextDNS[2]		
	CN	IR	RU	CN	IR	RU
DNS	–	●	–	–	●	–
TLS SNI	●	●	–	–	●	–
QUIC SNI	●	–	–	–	–	–
HTTP Host Header	–	●	–	–	●	–
IP Blackholing	–	–	–	●[†]	–	–

[†] China censors one of two resolved NextDNS IPs on port 443 TCP
[1] mozilla.cloudflare-dns.com
[2] firefox.dns.nextdns.io

Contrasting previous research [52], TCP segmentation alone did not circumvent the blocking, and TLS record fragmentation alone was also insufficient. We consider these newly found reassembly capabilities by TSPU devices worrying for future censorship circumvention efforts. On the positive side, we also found that combining TCP segmentation and TLS record fragmentation circumvents Russian ECH censorship. We did not encounter censorship of encrypted or unencrypted DNS (cf. Table 1): thus, circumventing direct ECH censorship with an IP proxy or other circumvention techniques such as packet fragmentation suffices to circumvent Russian ECH blocking.

China. We did not encounter censorship of `ClientHello` messages that contain an ECH extension by the GFW. However, ECH is effectively censored in China through the censorship of unencrypted and encrypted DNS (cf. Figure 5). As depicted in Table 1, the GFW blocks Cloudflare's encrypted DNS server configured in Firefox through SNI-based blocking in TLS and QUIC. TLS and QUIC blocking by the GFW led to residual censorship of up to 360 and 180 seconds, respectively. The TLS blocking we encountered is equivalent to the three injectors GFW detected by Niere et al. [37] and Wu et al. [50]. Despite operating from a vantage point in Henan, we did not trigger the recently discovered Henan Firewall [50] as all of our connections had TCP options enabled. The QUIC blocking we measured is equivalent to the behavior recently detected by Heitmann et al. [20]. Firefox's other default encrypted DNS server, NextDNS, is blocked through IP blackholing. Interestingly, the hostname of the NextDNS resolver itself resolved to two different IP addresses on our VPS in China. Only one IP address was affected by IP blackholing on our VPS. Using the other IP address for the NextDNS server makes encrypted DNS—and thereby ECH—usable in China.

Iran. During our evaluations, we found no direct censorship of the ECH extension in Iran. Like the GFW, the Iranian censor

[10] GitHub repository containing pcap files, https://github.com/UPB-SysSec/EchCensorshipResults, Created: 04.06.2025

effectively blocks ECH by censoring unencrypted and encrypted DNS (cf. Figure 5). The Iranian censor blocks the hostnames of both Firefox's default encrypted DNS servers: Cloudflare and NextDNS. Their hostnames are blocked over DNS through block page IP injection, over TLS by TCP RST injection, and over HTTP through block page injection. As Iran's censor is not capable of QUIC analysis, encrypted DNS over QUIC can be used to access HTTPS records in Iran and subsequently use ECH.

Summary. Our findings indicate that ECH is not usable by default in China, Iran, and Russia: Russian TSPU devices censor `ClientHello` messages containing an ECH extension; China and Iran effectively prevent ECH usage by censoring encrypted DNS. We found that the censorship in all three countries can be circumvented: In Russia, IP proxies and packet fragmentation circumvent the blocking. In China and Iran, uncensored encrypted DNS resolvers can be used. Still, default deployments in browsers such as Firefox are prohibited in all three countries.

6 Discussion

Circumventing ECH Censorship. We could circumvent all direct and indirect ECH censorship we encountered during our analyses. In Russia, an IP proxy at a non-Cloudflare IP outside of Russia circumvents ECH censorship as TSPU devices only censor ECH traffic to Cloudflare IPs. Similarly, Russian ECH blocking can be circumvented by combining TCP segmentation and TLS record fragmentation. TSPU devices also rely on the outer SNI of `ClientHello` messages to censor ECH. If server deployments accept flexible SNI values in the outer SNI, ECH censorship in Russia could be circumvented efficiently. The Chinese GFW's censorship can be circumvented by using an uncensored encrypted DNS provider such as NextDNS on its uncensored IP address or by proxying encrypted DNS traffic to a DNS server unaffected by SNI censorship. Similarly, Iranian censorship of ECH must also be circumvented using uncensored encrypted DNS services: for instance, DoQ and DoH3 are not affected by Iranian SNI censorship. The censors' ability to censor ECH—and users' ability to circumvent this censorship—interplays with server owners' deployment of ECH and censors' ability to censor encrypted DNS.

Outer SNI. When using ECH, the SNI extension in the unencrypted outer `ClientHello` message still allows the censor to infer details about the connection's destination: Russian TSPU devices block ECH traffic to Cloudflares' servers by analyzing the outer SNI field. Non-CDN servers that deploy ECH face an additional problem: the domain name advertised in their ECH configuration can be mapped to their original—censored—domain name as they do not share their ECH configuration with other servers. This enables censors to block the advertised domain name with no potential overblocking. Allowing clients to place different domain names in the unencrypted SNI extension in a ECH extension would prevent censors from utilizing it for censorship decisions. As of now, the RFC draft specifies that clients SHOULD include the advertised domain name in the unencrypted SNI extension, and Cloudflare rejects ECH connections with an incorrect outer SNI. Discussions about the content of the outer SNI are still ongoing in the IETF [24], with a consensus that ECH does not prioritize censorship circumvention in its goals [25]. We advertise that censorship circumvention becomes a goal during protocol specification to aid affected people and to prevent censors from utilizing the protocols' properties.

Role of DNS for ECH. Access to DNS is vital for ECH to work: Without a server's HTTPS record, the client cannot handshake using ECH. Our findings show that censorship of unencrypted and encrypted DNS effectively prevents the usage of ECH in China and Iran. This could be accidental as censoring DNS also prevents clients from connecting to a website in the first place; it could also be an active decision as blocking ECH directly can lead to overblocking—as done by TSPU devices. China exhibited censorship of the intermediate specification of ESNI [7, 22] but showed no sign of ECH censorship in our analysis. We see this as an indication of an active decision by the GFW to rely on encrypted DNS censorship to also prevent ECH. The importance of encrypted DNS for ESNI—now ECH—has previously been expressed by Hoang et al. [22]. We reinforce their claim and recommend future research to consider the interaction between different protocols, such as ECH and DNS, and to conduct a thorough analysis of DNS censorship in general.

Server Owners and Browsers. Server owners and browsers can aid censorship circumvention through ECH: Server owners can enable ECH and configure it so that incorrect outer SNI values are allowed on the server. Currently, non-Cloudflare deployments of ECH are almost non-existent, and Cloudflare's deployment of ECH requires a static outer SNI, enabling censorship. Browsers can attempt to handshake ECH with an incorrect hostname and provide greater customizability for their encrypted DNS protocol: Currently, browsers only handshake DoH and specify their default encrypted DNS providers over their hostname—this requires an additional unencrypted DNS request for the IP of the encrypted DNS provider by the browser.

6.1 Limitations

Encrypted DNS. In this paper, we highlight the importance of encrypted DNS for ECH. We analyze encrypted DNS censorship by measuring the censorship of Firefox's default encrypted DNS providers in China, Iran, and Russia. While we describe varying censorship of encrypted DNS in China and Iran, our analysis remains exemplary. We advocate for detailed evaluations of encrypted DNS censorship around the globe, such as the works by Lee et al. [29], and emphasize the need for circumvention tools that enable access to censored DNS resolvers.

Vantage Points. We executed our analyses from a single vantage point in China, Iran, and Russia. This methodology sufficiently revealed ECH censorship in all three countries. We are also confident that our results extend to other vantage points in China, Iran, and Russia, as all three countries are known to exhibit a centralized censorship architecture [4, 51, 52]. Despite this, analyses from additional vantage points would underline or challenge our results. Similarly, we advertise future research to evaluate ECH—and, to this end, encrypted DNS—censorship in other countries.

IP Censorship. In this paper, we detected and analyzed ECH censorship through SNI analysis and DNS censorship. In addition to these methods, censors can also block access to ECH by censoring IP ranges of ECH-providing hosts. For instance, censorship in China has been found to block access to all IP ranges of Cloudflare [34]. Contrasting this crude approach, we detected that Russia explicitly limits its ECH censorship to Cloudflare's IP ranges (cf. Section 5). As we believe ECH censorship to be driven by CDNs—until now, only Cloudflare supports it—we advertise future research to consider IP censorship of ECH providers, specifically CDNs.

6.2 Ethical Considerations

We rented our vantage points in accordance with the applicable export regulations and sanctions [14]. To this end, we consulted with our institution's export control officer. We verified that the hosting providers and their representatives are not sanctioned by the European Union (cf. Appendix A).

Our methodology collected only publicly available data from public DNS servers. In particular, this means that we did not collect user data. To our knowledge, our approach did not put individuals in the censored countries at risk. Further, we believe that publishing our findings benefits the community more than it potentially benefits censors who wish to tighten or implement ECH censorship.

We hope our findings help guide ECH and other protocols in a direction that strengthens them against censorship.

7 Related Work

ECH Support. In 2023, Zirngibl et al. [54] gathered HTTPS DNS records of 400 million domains. They collected 10.5 million HTTPS records from which they extracted 20 ECH configurations. Also in 2023, Tsiatsikas et al. [47] measured the support of ECH and its forebearer ESNI by servers on the Tranco Top 1M list. While detecting server support for the ESNI extension, they could not execute a TLS handshake with the single server that advertised an ECH configuration. In this paper, we describe an increase in ECH support by TLS servers following the continued standardization of the protocol. TLS server support for ESNI, the previous standardization of ECH, has been measured by Chai et al. [8] in 2019 and Hoang et al. [22] in 2022, and stayed below 15% during their analyses. We omitted ESNI from our analyses as it will not be standardized.

ECH Censorship. Censorship of the ESNI extension in China was reported by Bock et al. [7] in 2020. They detected that the GFW in China censors all TLS `ClientHello` messages containing an ESNI extension. In 2022, Hoang et al. [22] detected ESNI filtering in China, Iran, and Russia. We report that China and Iran did not extend their direct censorship of the ESNI extension to the ECH extension: we suspect that the GFW and Iranian censors deliberately allow ECH traffic to prevent overblocking, instead censoring ECH through encrypted DNS. On the contrary, TSPU devices started censoring ECH in May 2024 [48]. It was reported that Russian ECH censorship triggers when a TLS `ClientHello` contains a ECH extension and an SNI extension set to cloudflare-ech.com. In our paper, we discovered that TSPU devices only censor ECH when sent to servers in Cloudflare's advertised IP ranges.

Encrypted DNS. In 2024, Li et al. [31] measured encrypted DNS censorship across the globe. Of the 10 million encrypted DNS queries they sent to DNS resolvers, 5.92% were censored globally. When sending encrypted DNS queries from China, they faced a significantly higher censorship rate of 36.11%. At the same time, they detected lower censorship rates for DoQ than for DoH. We expect this trend to change as China has started censoring the SNI extension in QUIC connections [20]—we could verify this new type of censorship for a DoQ resolver in this paper. Also in 2024, Lee et al. [29] detected encrypted DNS filtering in 14 countries, including China, Iran, and Russia. We advertise for a continued analysis of encrypted DNS censorship in the future.

Censorship Circumvention. Several successful censorship circumvention techniques have been discovered in the past. Bock et al. [6] showcased the success of censorship circumvention through TCP manipulations, such as TCP segmentation. In 2023, Niere et al. [36] circumvented TLS censorship of the GFW with TLS record fragmentation. In this paper, we circumvented ECH censorship by TSPU devices with a combination of TCP segmentation and TLS record fragmentation. In 2021, Xue et al. [53] circumvented TSPU devices by inserting an additional TLS message into the handshake, and Harrity et al. [19] showed that alterations of unencrypted application-layer traffic can circumvent censorship—we consider similar changes possible for the TLS layer. To circumvent encrypted DNS censorship, Lee et al. [29] propose censorship circumvention mechanisms such as IP proxies and omitting the initial unencrypted DNS request for the domain name of the encrypted DNS server.

8 Conclusion

In this paper, we evaluated ECH's current role in censorship circumvention, determining servers' advertisement and support for ECH, and evaluating ECH censorship in China, Iran, and Russia. We find that ECH is almost exclusively supported by Cloudflare and that ECH connections to Cloudflare are distinguishable from non-ECH connections. We confirm ECH censorship in Russia and discovered IP proxies—Russian ECH censorship only affects Cloudflare IP ranges— and a combination of TCP segmentation and TLS record fragmentation as possible circumvention strategies. China and Iran do not censor ECH directly; instead, they rely on DNS censorship to effectively prohibit ECH usage. We consider this interplay of protocol censorship predictive for future censorship research. Due to limited deployment and evident censorship, we summarize that ECH's benefit for censorship circumvention is currently limited. We predict that other circumvention methods for SNI-based censorship remain important in the future and advertise a continued evaluation of ECH censorship.

Acknowledgments

We want to thank the reviewers and shepherd for their insightful comments and constructive feedback. Niklas Niere and Felix Lange were supported by the German Federal Ministry of Research, Technology and Space (BMFTR) through the project KoTeBi (16KIS1556K). Nico Heitmann was supported by the research project "North-Rhine Westphalian Experts in Research on Digitalization (NERD II)", sponsored by the state of North Rhine-Westphalia – NERD II 005-2201-0014.

References

[1] Christopher Allen and Tim Dierks. 1999. The TLS Protocol Version 1.0. RFC 2246. https://doi.org/10.17487/RFC2246

[2] Anonymous. 2014. Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. In 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14). USENIX Association, San Diego, CA. https://www.usenix.org/conference/foci14/workshop-program/presentation/anonymous

[3] Apple. 2023. TLS Encrypted Client Hello #46. https://github.com/WebKit/standards-positions/issues/46

[4] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. 2013. Internet Censorship in Iran: A First Look. In 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13). USENIX Association, Washington, D.C. https://www.usenix.org/conference/foci13/workshop-program/presentation/aryan

[5] Kevin Bock, Yair Fax, Kyle Reese, Jasraj Singh, and Dave Levin. 2020. Detecting and Evading Censorship-in-Depth: A Case Study of Iran's Protocol Whitelister. In 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20). USENIX Association. https://www.usenix.org/conference/foci20/presentation/bock

[6] 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

[7] 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/

[8] Zimo Chai, Amirhossein Ghafari, and Amir Houmansadr. 2019. On the importance of Encrypted-SNI (ESNI) to censorship circumvention. In 9th USENIX workshop on free and open communications on the internet (FOCI 19). USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/foci19/presentation/chai

[9] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. 2006. Ignoring the Great Firewall of China. In Privacy Enhancing Technologies, George Danezis and Philippe Golle (Eds.). Springer, Berlin, Heidelberg, 20–35. https://doi.org/10.1007/11957454_2

[10] Cloudflare. 2024. Encrypted Client Hello (ECH) - Frequently asked questions. https://support.mozilla.org/en-US/kb/faq-encrypted-client-hello#w_how-will-ech-impact-enterprises-that-use-transparent-proxies

[11] Cloudflare. 2025. Cloudflare Docs, ECH Protocol. https://developers.cloudflare.com/ssl/edge-certificates/ech/#enable-ech

[12] Tim Dierks and Eric Rescorla. 2008. RFC 5246: The transport layer security (TLS) protocol version 1.2.

[13] D Eastlake 3rd. 2011. RFC 6066: Transport Layer Security (TLS) Extensions: Extension Definitions.

[14] European Commission. 2025. EU Sanctions Tracker. https://data.europa.eu/apps/eusanctionstracker/

[15] Shencha Fan, Jackson Sippe, Sakamoto San, Jade Sheffey, David Fifield, Amir Houmansadr, Elson Wedwards, and Eric Wustrow. 2025. Wallbleed: A Memory Disclosure Vulnerability in the Great Firewall of China. In Proceedings 2025 Network and Distributed System Security Symposium. Internet Society, San Diego, CA, USA. https://doi.org/10.14722/ndss.2025.230237

[16] Firefox. 2023. Firefox 119.0, Release Notes. https://www.mozilla.org/en-US/firefox/119.0/releasenotes/

[17] Stephan Friedl, Andrei Popov, Adam Langley, and Emile Stephan. 2014. Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension. RFC 7301. https://doi.org/10.17487/RFC7301

[18] Google. 2023. Chrome Platform Status, Feature: TLS Encrypted Client Hello (ECH). https://chromestatus.com/feature/6196703843581952

[19] 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

[20] Nico Heitmann, Anonymous, Felix Lange, and Niklas Niere. 2025. China extended its SNI censorship to QUIC. https://upb-syssec.github.io/blog/2025/quic-china/

[21] Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. 2021. How Great is the Great Firewall? Measuring China's DNS Censorship. In 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, 3381–3398. https://www.usenix.org/conference/usenixsecurity21/presentation/hoang

[22] Nguyen Phong Hoang, Michalis Polychronakis, and Phillipa Gill. 2022. Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering. In Passive and Active Measurement, Oliver Hohlfeld, Giovane Moura, and Cristel Pelsser (Eds.). Springer International Publishing, Cham, 518–536. https://doi.org/10.1007/978-3-030-98785-5_23

[23] IETF. 2023. Encrypted Client Hello - the last puzzle piece to privacy. https://blog.cloudflare.com/announcing-encrypted-client-hello/

[24] IETF. 2025. IETF 122: Transport Layer Security (TLS). https://meetecho-player.ietf.org/playout/?session=IETF122-TLS-20250320-0230

[25] IETF. 2025. [TLS] Implicit ECH Config for TLS 1.3 – addressing public_name fingerprinting. https://www.mail-archive.com/tls@ietf.org/msg19355.html

[26] Liz Izhikevich, Gautam Akiwate, Briana Berger, Spencer Drakontaidis, Anna Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. ZDNS: a fast DNS toolkit for internet measurement. In Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22). Association for Computing Machinery, New York, NY, USA, 33–43. https://doi.org/10.1145/3517745.3561434

[27] Felix Lange, Niklas Niere, Jonathan von Niessen, Dennis Suermann, Nico Heitmann, and Juraj Somorovsky. 2025. I(ra)nconsistencies: Novel Insights into Iran's Censorship. Free and Open Communications on the Internet (2025). https://www.petsymposium.org/foci/2025/foci-2025-0002.php

[28] Victor Le Pochat, Tom van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczynski, and Wouter Joosen. 2019. Tranco: A research-oriented top sites ranking hardened against manipulation. In 26th annual network and distributed system security symposium san diego, california, USA, february 24-27, 2019 (NDSS 2019). The Internet Society, San Diego, CA, USA. https://www.ndss-symposium.org/ndss-paper/tranco-a-research-oriented-top-sites-ranking-hardened-against-manipulation/

[29] Jinseo Lee, David Mohaisen, and Min Suk Kang. 2024. Measuring DNS-over-HTTPS Downgrades: Prevalence, Techniques, and Bypass Strategies. Proc. ACM Netw. 2, CoNEXT4 (Nov. 2024), 28:1–28:22. https://doi.org/10.1145/3696385

[30] Let's Encrypt. 2023. Let's Encrypt Stats. https://letsencrypt.org/stats/

[31] 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

[32] 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

[33] Nima Nazeri and Collin Anderson. 2013. Citation Filtered: Iran's Censorship of Wikipedia. https://www.semanticscholar.org/paper/Citation-Filtered%3A-Iran%E2%80%99s-Censorship-of-Wikipedia-Nazeri-Anderson/15f13eb5c7fa7128cd6551d0fe1c285a7763c0ea

[34] net4people. 2015. 似乎有部分地区已经以反诈为借口屏蔽了 Cloudflare CDN 所有 IP 段. https://github.com/XIU2/CloudflareSpeedTest/discussions/383

[35] Henrik Nielsen, Jeffrey Mogul, Larry M Masinter, Roy T. Fielding, Jim Gettys, Paul J. Leach, and Tim Berners-Lee. 1999. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616. https://doi.org/10.17487/RFC2616

[36] Niklas Niere, Sven Hebrok, Juraj Somorovsky, and Robert Merget. 2023. Poster: Circumventing the GFW with TLS Record Fragmentation. CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (Nov. 2023), 3528–3530. https://doi.org/10.1145/3576915.3624372 ISBN: 9798400700507 Publisher: Association for Computing Machinery, Inc.

[37] Niklas Niere, Felix Lange, Robert Merget, and Juraj Somorovsky. 2025. Transport Layer Obscurity: Circumventing SNI Censorship on the TLS-Layer. IEEE Computer Society, 1344–1362. https://doi.org/10.1109/SP61157.2025.00151 ISSN: 2375-1207.

[38] Centre of Monitor and Control of the Internet. 2024. Рекомендуем отказаться от CDN-сервиса CloudFlare | Новости. https://portal.noc.gov.ru/ru/news/2024/11/07/%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D1%83%D0%B5%D0%BC-%D0%BE%D1%82%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D1%8C%D1%81%D1%8F-%D0%BE%D1%82-cdn-%D1%81%D0%B5%D1%80%D0%B2%D0%B8%D1%81%D0%B0-cloudflare/

[39] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global Measurement of DNS Manipulation. 307–323. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/pearce

[40] PQ.Hosting. 2024. Solutions for users facing ECH blocking in Russia. https://pq.hosting/en/news/solutions-for-users-facing-ech-blocking-in-russia

[41] 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

[42] 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. 2581–2598. https://www.usenix.org/conference/usenixsecurity23/presentation/ramesh-network-responses

[43] Eric Rescorla. 2018. Rfc 8446: The transport layer security (tls) protocol version 1.3.

[44] Eric Rescorla, Kazuho Oku, Nick Sullivan, and Christopher A. Wood. 2020. Encrypted Server Name Indication for TLS 1.3. Internet-Draft draft-ietf-tls-esni-06.

Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-tls-esni/06/ Work in Progress.

[45] Eric Rescorla, Kazuho Oku, Nick Sullivan, and Christopher A. Wood. 2025. TLS Encrypted Client Hello. Internet-Draft draft-ietf-tls-esni-24. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-tls-esni/24/ Work in Progress.

[46] Eric Rescorla, Kazuho Oku, Nick Sullivan, and Christopher A. Wood. 2025. TLS Encrypted Client Hello. Internet Draft draft-ietf-tls-esni-24. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-tls-esni Num Pages: 53.

[47] Zisis Tsiatsikas, Georgios Karopoulos, and Georgios Kambourakis. 2023. Measuring the Adoption of TLS Encrypted Client Hello Extension and Its Forebear in the Wild. In Computer Security. ESORICS 2022 International Workshops, Sokratis Katsikas, Frédéric Cuppens, Christos Kalloniatis, John Mylopoulos, Frank Pallas, Jörg Pohle, M. Angela Sasse, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Jorge Maestre Vidal, Marco Antonio Sotelo Monge, Massimiliano Albanese, Basel Katt, Sandeep Pirbhulal, and Ankur Shukla (Eds.). Springer International Publishing, Cham, 177–190. https://doi.org/10.1007/978-3-031-25460-4_10

[48] wkrp. 2024. Blocking of Cloudflare ECH in Russia, 2024-11-05 · Issue #417 · net4people/bbs. https://github.com/net4people/bbs/issues/417

[49] Mingshi Wu, Jackson Sippe, Danesh Sivakumar, Jack Burg, Peter Anderson, Xiaokang Wang, Kevin Bock, Amir Houmansadr, Dave Levin, and Eric Wustrow. 2023. How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic. 2653–2670. https://www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi

[50] Mingshi Wu, Ali Zohaib, Zakir Durumeric, Amir Houmansadr, and Eric Wustrow. 2025. A Wall Behind A Wall: Emerging Regional Censorship in China. IEEE Computer Society, 1363–1380. https://doi.org/10.1109/SP61157.2025.00152 ISSN: 2375-1207.

[51] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman. 2011. Internet Censorship in China: Where Does the Filtering Occur?. In Passive and Active Measurement, Neil Spring and George F. Riley (Eds.). Springer, Berlin, Heidelberg, 133–142. https://doi.org/10.1007/978-3-642-19260-9_14

[52] 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

[53] Diwen Xue, Reethika Ramesh, Valdik S S, Leonid Evdokimov, Andrey Viktorov, Arham Jain, Eric Wustrow, Simone Basso, and Roya Ensafi. 2021. Throttling Twitter: an emerging censorship technique in Russia. In Proceedings of the 21st ACM Internet Measurement Conference (IMC '21). Association for Computing Machinery, New York, NY, USA, 435–443. https://doi.org/10.1145/3487552.3487858

[54] Johannes Zirngibl, Patrick Sattler, and Georg Carle. 2023. A First Look at SVCB and HTTPS DNS Resource Records in the Wild. In 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, Delft, Netherlands, 470–474. https://doi.org/10.1109/EuroSPW59978.2023.00058

A Server Specifications

Table 2: Specifications of the server in Iran.

Location:	Mashhad, Iran
Autonomous System Number:	201295
Vendor:	Avanetco
URL:	https://www.avanetco.com/
Internet Service Provider:	Shabakeh Ertebatat Artak Towseeh PJSC (private)

Table 3: Specifications of the server in China.

Location:	Zhengzhou, China
Autonomous System Number:	45090
Vendor:	China VPS Hosting
URL:	https://chinavpshosting.com/
Internet Service Provider:	Tencent Cloud Computing (Beijing) Co., Ltd

Table 4: Specifications of the server in Russia.

Location:	Moscow, Russia
Autonomous System Number:	50867
Vendor:	Serverwala
URL:	https://www.serverwala.com/
Internet Service Provider:	HOSTKEY B.V. (private)

Table 5: Specifications of the server in Germany.

Location:	Berlin, Germany
Autonomous System Number:	201295
Vendor:	IONOS
URL:	https://www.ionos.de/
Internet Service Provider:	IONOS SE (private)