Insights into an Iranian Internet Shutdown

Anonymous
Paderborn University

Niklas Niere
Paderborn University

Felix Graf Lange
Paderborn University

Juraj Somorovsky
Paderborn University

Abstract

In June 2025, Iran enacted a nationwide Internet shutdown, culminating its already strict censorship apparatus. While Internet shutdowns happen regularly, insights into these shutdowns are notoriously difficult to obtain: their timing is hard to predict, and measurements are often impossible. In this paper, we present unique measurements surrounding Iran's 2025 Internet shutdown in June, which we acquired during a regular analysis of Iran's censorship apparatus. We contextualize our findings of Iranian DNS, HTTP, TLS, and QUIC censorship during the shutdown with measurements from platforms such as Cloudflare Radar and user reports. Our measurements show that Iranian censorship changed before and after the shutdown, marking preparation and recovery periods. For instance, QUIC censorship went into effect before and stayed in effect after the shutdown, while DNS over TCP censorship was only present briefly before the shutdown and resumed working afterwards. We also measured general network instabilities, especially for UDP, after the shutdown and the disabling of certain middleboxes. Our findings indicate that the Iranian censor enforced its shutdown using fine-grained techniques instead of relying on an all-or-nothing blackout. We advertise for continued measurements of the Iranian censor and hypothesize that future shutdowns in censoring countries could be detected during their preparation phase.

Keywords

Censorship, Iran, Shutdown

1 Introduction

Internet censorship is utilized to prevent free access to the Internet, and is prevalent in many countries [5, 25, 36, 39]. Censoring countries deploy long-running systems that dissect and block a plethora of protocols such as HTTP [17], DNS [2, 17], TLS [8, 28], and QUIC [13, 40]. Besides this so-called deep packet inspection (DPI), censors resort to disabling specific protocols or all Internet traffic during particularly sensitive events [4, 25, 30].

Censorship in Iran. Iran has a long history of censoring the Internet through restrictive DPI measures [5, 22, 25]. Previous research has analyzed Iran's censorship apparatus extensively [6–8, 17, 22, 28], with only China's censorship infrastructure receiving more attention [25]. Besides their long-running DPI censorship, Iran resorts increasingly to Internet shutdowns: since June 13, 2025, Iran has enacted 4 Internet outages [15, 16, 33, 37] across the country. In this paper, we present, contextualize, and interpret measurement results we acquired before, during, and after Iran's Internet outage from June 18, 2025 until June 25, 2025. Recent work by Cui et al. [11] shed light on the shutdown from an outside perspective; we provide unique evaluations from inside Iran.

Contributions. Censorship measurements surrounding Internet outages are challenging, as the beginning of an outage is usually difficult to predict, and access to vantage points during the outage is impossible. Data from long-running platforms such as OONI or Cloudflare, and user reports can be gathered after the blocking, but their insights are often limited in detail [10]. During Iran's Internet outage in June 2025, we ran unrelated tests of its DPI infrastructure. By chance, we were able to collect and record unique measurement results of Iran's HTTP, DNS, TLS, and QUIC censorship surrounding the Internet outage. Our measurements show that certain censorship events went into effect before the outage and stayed after it was lifted. For instance, QUIC has been blocked in Iran before the overall shutdown went into effect and persisted after it, while DNS over TCP was blocked before the shutdown but enabled when the block was lifted. Overall, our unique analysis shows that an Internet outage is not necessarily a *big switch* event, but can instead be preceded and succeeded by various censorship measures and long-term effects.

In summary, we contribute the following:

- We present unique censorship measurements of HTTP, DNS, TLS, and QUIC before and after Iran's Internet outage from June 18, 2025 until June 25, 2025.
- We show that large-scale censorship of DNS over TCP and QUIC was enabled before the outage, facilitating early detection of future shutdowns.
- We provide pcap files of our measurements for future analysis.[1]
- We contextualize our measurement results with other sources and user reports.

2 Iranian Internet Shutdown

The Internet shutdown in Iran lasted from June 18 to June 25, 2025, and followed Israel's attack on Iran on June 13. Initial network disruptions starting June 13 led to the complete shutdown on June 18. The effects on international Internet traffic are visible in Cloudflare Radar data (Figure 1), showing HTTP traffic reaching near-zero levels by June 18.

2.1 Scan Timeline

We collected censorship data from a VPS located in Iran (AS57497) from June 1 to July 7, 2025, by issuing requests to a reference server under our control in Germany, following a similar approach to that of Jin et al. [21] and Lange et al. [22]. We scanned 9,000 domains[2]

Free and Open Communications on the Internet 2026(2), 47–51

[1] Collection of measured pcap files, https://github.com/UPB-SysSec/InsightsIntoAnIranianInternetShutdownPcaps

[2] We initially scanned all 100,000 domains but could only scan 9,000 domains right before the shutdown. We limit our results to those 9,000 domains.

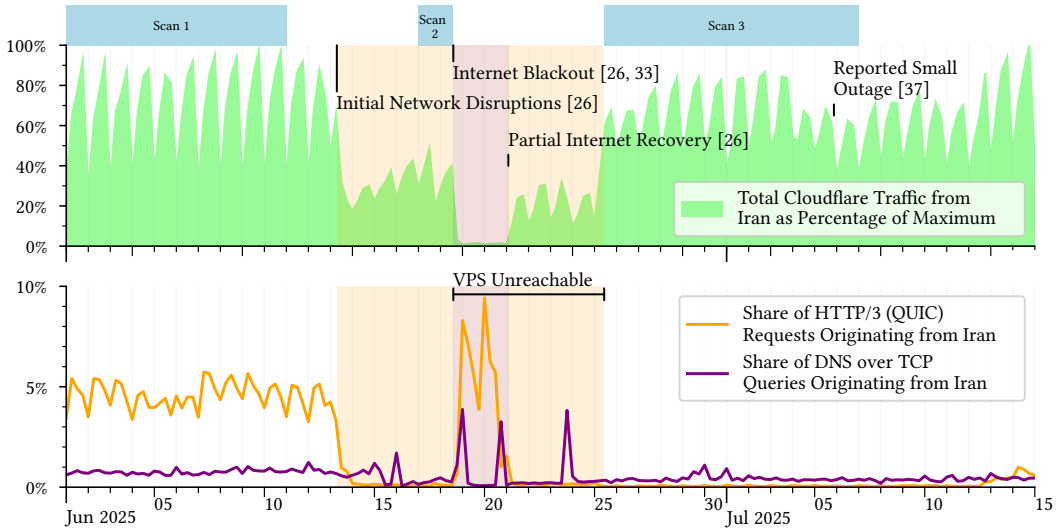

Figure 1: Timeline of the shutdown in June composed of Cloudflare Radar [9] data annotated with events surrounding the shutdown and the execution phases of Scan 1-3. The shaded red area denotes the total outage in Iran lasting two days. Initial network disruptions started five days prior, shaded in orange. During the partial recovery phase after the outage, the VPS remained unreachable.

from the Tranco top 100,000 domain list [23][3] for the protocols DNS [27], HTTP [14], TLS [12], and QUIC [20]. We included each domain in a DNS request, the HOST header of an HTTP GET request, and the SNI extension in a TLS ClientHello message, wrapped inside a QUIC Initial Packet when evaluating QUIC censorship. We sent our requests to our reference server and observed potential censorship behavior. Each of the 9,000 domains was scanned 25 times per protocol. However, due to an unexpected Internet shutdown during our scans, we had to split the scan executions around the shutdown. Divided by the Internet shutdown, we conducted two primary scans before and after the shutdown (Scan 1 and Scan 3), each with 15 and 10 repetitions per domain and per protocol, respectively. In addition to these scans, we also performed a scan of the 9,000 domains with 5 repetitions per domain and protocol right before the shutdown (Scan 2). In each scan, a domain was considered censored if we did not retrieve the expected byte sequence in more than 50% of the requests. Figure 1 compares the execution time of our scans with Internet shutdown events.

After conducting the initial scan (Scan 1), we noticed the first connectivity issues to the VPS after Israel attacked Iran on June 13, resulting in unstable SSH sessions and scans exceeding runtime limitations. In the scan conducted right before the Internet shutdown (Scan 2), we scanned 9,000 domains of the Tranco top 10,000 list before completely losing access to the VPS on June 18 at approximately 14:00 UTC (17:30 local time in Iran). We regained access to the vantage point on June 25 at 10:30 UTC (14:00 local time in Iran) after periodically checking accessibility via ICMP ping and SSH since June 22. After regaining access, we conducted our final scan (Scan 3).

[3]https://tranco-list.eu/list/YLQQG/1000000, Accessed: 18 May 2025

2.2 Scan Results

In the following, we detail the results of our conducted scans (**Scan 1–3**) and relate them to each other in the context of the Internet shutdown. Table 1 depicts the number of domains that were censored during each scan period. Following the initial network disruptions between Scan 1 and Scan 2, we observed increased connection instability during our scans and outages of the DNS over TCP, DNS over UDP, and QUIC protocols.

*2.2.1 Before the Shutdown (**Scan 1**).* In Scan 1, we observed regular domain-dependent censorship behavior in Iran. For the protocols DNS, HTTP, and TLS, we observed about 15% of queried domains being censored. The censored domains mostly overlapped across protocols with a total of 1,216 domains (13.51%). In addition, we did not observe QUIC censorship in Scan 1.

*2.2.2 Initial Disruptions (**Scan 2**).* In the time after Israel's attack on Iran, up until the shutdown, we observed first censorship changes compared to previously captured traffic in Scan 1. In general, we observed increases in dropped TCP and UDP packets across the scanned protocols following Israel's attack on Iran. UDP packet drops were most pronounced for QUIC, with 100% of Initial packets dropped, resulting in a complete QUIC blockage. We also observed strict DNS over TCP blocking: 96.44% (8,680) of requested domains were not resolvable during Scan 2. The TCP handshakes of our requests were completed, indicating that the blockage targeted the DNS over TCP protocol. While most DNS over TCP requests were dropped, 320 domains received a server response, and requests to 21 domains were subject to active censorship via injected IP addresses. Table 1 shows a significant increase in censored domains in Scan 2 compared to Scan 1 for DNS over TCP and QUIC. For the remaining protocols, we observed temporary blockings, causing a

Table 1: Censorship development across Scan 1–3 for 9,000 domains of the top 10,000 Tranco list. This table depicts the percentage of domains we deem censored across multiple connection attempts. We observed different behavior: DNS/TCP was censored before the shutdown, while DNS/UDP was affected by UDP instabilities after the shutdown. QUIC was blocked entirely.

Protocol	Scan 1	Scan 2	Scan 3
DNS/UDP	1,361 (15.12%)	1,509 (16.77%)	**8,026 (89.18%)**†
DNS/TCP	1,361 (15.12%)	**8,701 (96.68%)***	1,384 (15.38%)
HTTP	1,375 (15.28%)	1,730 (19.22%)	1,412 (15.69%)
TLS	1,351 (15.01%)	1,555 (17.28%)	1,369 (15.21%)
QUIC	1 (0.01%)	**9,000 (100%)**‡	**9,000 (100%)**‡
Total	9,000	9,000	9,000

* No server response after successful TCP handshake
† Not domain-specific, caused by general UDP transport instabilities
‡ Complete QUIC blocking

slight increase in censored domains. During the temporary blockings, every scanned domain experienced packet drops, including domains otherwise censored by response injections.

The scan results of Scan 2 indicate that additional censorship measures were applied before the Internet shutdown on June 18. Thus, we postulate that these measures were preliminary steps towards the complete shutdown. Cui et al. [11] argue that localized shutdown drills are performed before the nationwide shutdown.

2.2.3 Shutdown and Initial Recovery. Our vantage point in Iran was unreachable for 7 days from June 18 to June 25. The last scan results of Scan 2 were captured at approximately 13:10 UTC, which is 16:40 local time in Iran (UTC+3:30). We noticed the VPS being unreachable via SSH and ICMP ping at approximately 14:00 UTC, which implies that the vantage point was cut off from the Internet between 13:10 and 14:00 UTC on June 18. This matches Cloudflare Radar data [9], which shows a significant drop in HTTP traffic at 13:00 UTC on June 18, reaching near-zero levels by 20:00 UTC.[4] We regained access to the VPS on June 25 at 10:30 UTC after periodically checking reachability via SSH and ping since June 22. Although Cloudflare Radar shows partial recovery of traffic since June 21, SSH access to our VPS was unaffected. Reportedly, traffic did not recover for all Iranian networks at the same time [24, 26], which could explain the unreachability until June 25.

*2.2.4 Censorship After the Shutdown (**Scan 3**).* After gaining access to our vantage point on June 25, we continued our evaluations. Similar to Scan 2 before the shutdown, QUIC remained completely blocked after the shutdown. In contrast, DNS over TCP censorship returned to the levels we measured in Scan 1. For the other queried TCP-based protocols, HTTP and TLS, we also observed no significant difference compared to Scan 1. Our scan results suggest that TCP-based traffic was no longer significantly affected by measures induced by the Internet shutdown. In contrast, we observed a significant increase in packet drops for DNS over UDP requests in Scan 3.

[4] https://radar.cloudflare.com/ir?dateStart=2025-06-12&dateEnd=2025-06-28, Accessed: 20 April 2026

```
<title>NTL1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

(a) Observed TTL values: 53–55

```
<title>NTE1</title>
...
<iframe src="http://
  10.10.34.36/?type=Invalid
  Keyword&policy=MainPolicy
   "...>
```

(b) Observed TTL values: 186–188

Figure 2: The two types of HTTP blockpages: Both include the same iframe, but use different HTML titles and IP TTLs. We did not encounter the NTE1 blockpage on June 11th.

This development is observable in Table 1 for the 9,000 domains scanned in Scan 2. Requests to the same domains at other times were not dropped.

We observed changing censorship policies across **Scan 1-3** for QUIC and DNS over TCP; the affected domains remained largely consistent. Across the queried protocols, we determined 5 domains whose censorship status changed between Scan 1 and Scan 3. We attribute the changing censorship behavior to common updates of the lists of censored domains.

2.2.5 Injection Patterns. During our scans, we observed two different HTTP blockpages injected by the Iranian censor (see Figure 2): One titled NTL1 and another titled NTE1. We noticed that the NTL1 and NTE1 blockpages also had unique IP TTL values of 53–55 and 186–188, respectively. TCP RST injections for censored TLS and DNS over TCP packets exhibited the same pattern of TTL values. We suggest that these two injection patterns stem from separate injectors, as was the case in previous work [2, 28, 38]. This claim is corroborated by the fact that we could only observe the NTL1 blockpage and injected TCP packets with a TTL of 53–55 on June 11th. We consider it more likely that a whole injector was inactive than that an injector disables an injection pattern for a single day. We could not discern similar patterns for DNS injections: all injected UDP packets had TTL values in the range 186–190.

2.3 Related Work

The impact of the Internet shutdown in Iran was observed from multiple perspectives, including user reports on GitHub, Cloudflare Radar data, and OONI measurements. A more comprehensive report is provided by Miaan Group et al. [26], gathering traffic and service usage data, as well as comparing the shutdown with previous shutdowns in Iran. In the following, we give an overview of related data and work regarding the Internet shutdown and compare them to our observations.

OONI. OONI measurement data[5] available via the OONI Explorer [29] shows a drop in probe executions for the web connectivity test in Iran from June 13 to June 26. This observation matches the reduced traffic to Cloudflare in this timeframe and coincides with our observations of reduced connectivity starting June 13, followed by the complete shutdown starting June 18. OONI probe executions dropped to zero after we lost access to the vantage point on June 19 and remained near-zero on June 20, with the last successful probe

[5] https://explorer.ooni.org/chart/mat?probe_cc=IR&since=2025-05-28&until=2025-07-09&time_grain=day&axis_x=measurement_start_day&test_name=web_connectivity, Accessed: 20 April 2026

execution on June 18 at 12:55 UTC. The number of OONI probe executions rose again on June 21, consistent with Cloudflare traffic partially recovering that day.

Miaan Group et al. Report. The report published by Miaan Group et al. [26] gathers data from Cloudflare, IODA, and Kentik and provides a detailed breakdown of the shutdown. It reports initial disruptions of Internet traffic from June 13 to June 17, with reduced connectivity observed by IODA and Cloudflare. They further report on the shutdown from June 18 to June 21 based on Cloudflare Radar, IODA, and Kentik data showing Internet traffic at a near-zero level. From June 21 to June 25, Miaan Group et al. report a partial recovery of international Internet traffic, staying below the levels of before June 13. Internet connectivity only recovered for a few networks, explaining why we did not notice any improvements at our vantage point. On June 25, Internet connectivity is again at expected levels, which matches our regaining access to the VPS. After the recovery, they report on a further disruption on July 5 from 20:00 to 0:00 UTC, which we, however, did not notice in our scans.

User Reports. During the shutdown, GitHub remained accessible through a whitelisted IP address [18]. This allowed Iranian citizens to communicate via GitHub and share their observations and experiences during the shutdown and afterwards. As most communication during the shutdown focused on circumventing restrictions, we focus on the reports regarding the network situation after the complete shutdown. While the Internet was accessible again after June 25, reports state that certain protocols were still disabled. This affected QUIC, which was still blocked after the shutdown [34, 35], as well as TLS `ServerHello` [34]. Also, UDP transport remained unstable [31]. In Scan 3, we observed QUIC being blocked completely and DNS over UDP experiencing severe packet drops, which matches the GitHub reports. For the ongoing TLS blockage, we can not verify the result, because we only sent `ClientHello` messages in our scans.

Cui et al.'s Shutdown Characterization. Similar to our work, Cui et al. [11] analyzed and characterized the June shutdown by monitoring service-level activities. They categorized the shutdown into phases of localized shutdown drills that preceded the complete shutdown and recovered afterwards. They further point out the progressive nature of the shutdown by monitoring increasing numbers of affected services throughout the shutdown phases. We complement Cui et al.'s analysis of service-level traffic from outside Iran with measurements from inside Iran. We come to a similar conclusion: Iran's Shutdown in June 2025 was not a single event but a cascade of subsequent mechanisms.

3 Discussion

Vantage Point Limitation. As we executed our scans from a single vantage point inside Iran, our results do not necessarily apply to other networks inside Iran. For instance, our vantage point was not affected by the partial Internet recovery following the shutdown. The heterogeneity of Iranian censorship is further corroborated by the potential existence of multiple middleboxes (see Section 2.2.5). While we invite future work to analyze the heterogeneity of Iranian censorship, we stress the difficulty of acquiring vantage points.

Can Future Shutdowns Be Predicted? Our observations surrounding Iran's Internet shutdown in June 2025 suggest that Internet shutdowns are fine-grained. Instead of relying on BGP withdrawals or routing announcements, the Iranian censor applied sophisticated service-level measures [11, 19]. Before the total blackout, we noticed individual protocols (QUIC and DNS over TCP) being blocked in Scan 2, possibly as a preliminary step towards the complete shutdown. This means that long-term measurements could have found indications of this shutdown before it happened. Similar shutdown preparations were also noticed for Iran's Internet shutdown in January 2026 [1]. While we propose that future shutdowns could be detectable, we invite future work to explore this.

Further Shutdowns. Since the Internet shutdown in June 2025, the Iranian government has induced two further blackouts: one lasting from January 8 to February 1, 2026, and another lasting from February 28 until May 25, 2026. While the Internet shutdown in June 2025 shows an evolution of Internet censorship measures compared to previous Iranian Internet disruptions in 2019 and 2022 [26], the shutdowns that followed the shutdown discussed in this paper include further restrictions. This includes the disruptions of the domestic Iranian Internet (NIN), which remained unaffected during the June shutdown [19], and disruptions of satellite Internet access [3, 32]. These further shutdowns showed that even in the same country, not all shutdowns are implemented equally.

Ethical Considerations. We minimized the impact of our analyses on servers and infrastructure while maximizing the benefit to people affected by censorship. During our evaluation, we never sent potentially censored requests to real-world servers; instead, we exchanged them between our controlled vantage points. While renting our vantage point in Iran, we confirmed that neither the company nor any of its affiliates is on the sanctions list of the European Union. Our institutional sanctions officer approved our approach. We also strongly believe that our evaluations provide greater benefit to people affected by censorship than to censors.

4 Conclusions

In this paper, we present unique measurement insight into the Iranian Internet shutdown in June 2025. Our measurements show that DNS over TCP and QUIC were censored in preparation for the shutdown, with QUIC censorship persisting afterward. These behaviors align with independent measurements by Cloudflare Radar and user reports, which indicate that the complete shutdown lasted around two days, but the preparation and recovery period lasted four and five days, respectively. Due to its distinct preparation period, this shutdown—and potentially future shutdowns—could be predicted before coming into effect. As this would enable affected people to prepare for an otherwise spontaneous event, we hope to enable a discussion about the predictability of Internet shutdowns.

Acknowledgments

We thank the reviewers for their insightful comments and constructive feedback. The project was partially funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 555828767, 556138177.

References

[1] Giuseppe Aceto, V. Persico, and Antonio Pescapé. 2026. Iran's January 2026 Internet Shutdown: Public Data, Censorship Methods, and Circumvention Techniques. https://www.semanticscholar.org/paper/289dff849784c17d4729d914ae8ba941ccb55795

[2] Anonymous, Arian Akhavan Niaki, Nguyen Phong Hoang, Phillipa Gill, and Amir Houmansadr. 2020. Triplet censors: Demystifying great Firewall's DNS censorship behavior. In *10th USENIX workshop on free and open communications on the internet (FOCI 20)*. USENIX Association. https://www.usenix.org/conference/foci20/presentation/anonymous

[3] ARTICLE 19. 2026. Tightening the Net: China's Infrastructure of Oppression in Iran. https://www.article19.org/wp-content/uploads/2021/07/A19-Tightening-the-Net-China-Iran-Report.pdf

[4] Maria Xynou (OONI) Arturo Filastò (OONI), Arthur Gwagwa (CIPIT). 2016. *The Gambia: Internet Shutdown during 2016 Presidential Election | OONI*. https://ooni.org/post/gambia-internet-shutdown/

[5] 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

[6] Simone Basso. 2022. Measuring DoT/DoH Blocking Using OONI Probe: A Preliminary Study. https://ooni.org/post/2022-doh-dot-paper-dnsprivacy21/

[7] 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

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

[10] Anna Crowder, Daniel Olszewski, Patrick Traynor, and Kevin R. B. Butler. 2024. I Can Show You the World (of Censorship): Extracting Insights from Censorship Measurement Data Using Statistical Techniques. In *ACSAC '24: Proceedings of the 40th Annual Computer Security Applications Conference*. Hawaii.

[11] Shibo Cui, Mingxuan Liu, Baojun Liu, Haixin Duan, Ruixuan Li, Chaoyi Lu, Jin Zhang, Zhicheng Wang, and Jinghua Bai. 2026. Characterizing Iran's Phased National Internet Shutdown in 2025: A Progressive and Distributed Action. In *Proceedings of the ACM Web Conference 2026* (United Arab Emirates) *(WWW '26)*. Association for Computing Machinery, New York, NY, USA, 1830–1840. https://doi.org/10.1145/3774904.3792699

[12] T. Dierks and E. Rescorla. 2008. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246. IETF. https://www.rfc-editor.org/rfc/rfc5246.txt

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

[14] R. Fielding, M. Nottingham, and J. Reschke. 2022. *HTTP/1.1*. RFC 9112. IETF. https://www.rfc-editor.org/rfc/rfc9112.txt

[15] free_the_internet. 2026. Iran: Internet shutdown from 18:45 UTC 8 January 2026 · Issue #561 · net4people/bbs. https://github.com/net4people/bbs/issues/561

[16] gusgustavo. 2026. Iran: Internet shutdown from 7 UTC 28 February 2026 · Issue #586 · net4people/bbs. https://github.com/net4people/bbs/issues/586

[17] 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

[18] HoseanRC. 2025. Internet is completely blocked in Iran (2025-06-17 to 2025-06-26) · Issue #484 · net4people/bbs. https://github.com/net4people/bbs/issues/484#issuecomment-2987484989 Accessed: 2026-03-09.

[19] IODA. 2026. A Comparative Look at Internet Shutdowns in Iran: 2019, 2022, 2025, and 2026. https://ioda.inetintel.cc.gatech.edu/reports/a-comparative-look-at-internet-shutdowns-in-iran-2019-2022-2026-and-2026/ Accessed: 2026-06-12.

[20] J. Iyengar and M. Thomson. 2021. *QUIC: A UDP-Based Multiplexed and Secure Transport*. RFC 9000. IETF. https://www.rfc-editor.org/rfc/rfc9000.txt

[21] Lin Jin, Shuai Hao, Haining Wang, and Chase Cotton. 2021. Understanding the Practices of Global Censorship through Accurate, End-to-End Measurements. *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 5, 3 (Dec. 2021), 43:1–43:25. https://doi.org/10.1145/3491055

[22] 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

[23] 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/

[24] Doug Madory. 2025. Doug Madory: "In the 4th day of #Iran's govt…" - Infosec Exchange. https://infosec.exchange/@dougmadory/114722381235179054 Accessed: 2026-04-14.

[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] Miaan Group, ASL19, and IODA. 2025. Iran's 'Stealth Blackout': A Multi-stakeholder Analysis of the June 2025 Internet Shutdown - Filterwatch. https://filter.watch/english/2025/10/02/irans-stealth-blackout-a-multi-stakeholder-analysis-of-the-june-2025-internet-shutdown/ Accessed: 2025-11-08.

[27] P. Mockapetris. 1987. *Domain names - implementation and specification*. RFC 1035. IETF. https://www.rfc-editor.org/rfc/rfc1035.txt

[28] 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

[29] Open Observatory of Network Interference. 2026. OONI Explorer. https://explorer.ooni.org/ Accessed: 2026-03-23.

[30] Ramakrishna Padmanabhan, Arturo Filastò, Maria Xynou, Ram Sundara Raman, Kennedy Middleton, Mingwei Zhang, Doug Madory, Molly Roberts, and Alberto Dainotti. 2021. A multi-perspective view of Internet censorship in Myanmar. 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, 27–36. https://doi.org/10.1145/3473604.3474562

[31] Phoenix-999. 2025. Iran networks after the shutdowns (since 2025-06-25) · Issue #489 · net4people/bbs. https://github.com/net4people/bbs/issues/489#issuecomment-3067006744 Accessed: 2026-03-09.

[32] Phoenix-999. 2026. Iran: Internet shutdown from 18:45 UTC 8 January 2026 · Issue #561 · net4people/bbs. https://github.com/net4people/bbs/issues/561#issuecomment-3732887058 Accessed: 2026-04-01.

[33] pirooz gthb. 2025. Internet is completely blocked in Iran (2025-06-17 to 2025-06-26) · Issue #484 · net4people/bbs. https://github.com/net4people/bbs/issues/484

[34] ranthe21. 2025. Internet is completely blocked in Iran (2025-06-17 to 2025-06-26) · Issue #484 · net4people/bbs. https://github.com/net4people/bbs/issues/484#issuecomment-3011967607 Accessed: 2026-03-09.

[35] ranthe21. 2025. Iran networks after the shutdowns (since 2025-06-25) · Issue #489 · net4people/bbs. net4people/bbs. https://github.com/net4people/bbs/issues/489#issuecomment-3022773523 Accessed: 2026-03-09.

[36] Philipp Winter and Stefan Lindskog. 2012. How the Great Firewall of China is Blocking Tor. In *2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI 12)*. USENIX Association, Bellevue, WA. https://www.usenix.org/conference/foci12/workshop-program/presentation/Winter

[37] wkrp. 2025. Internet shutdown in Iran starting 2025-07-05 · Issue #497 · net4people/bbs. https://github.com/net4people/bbs/issues/497

[38] 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

[39] 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

[40] 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