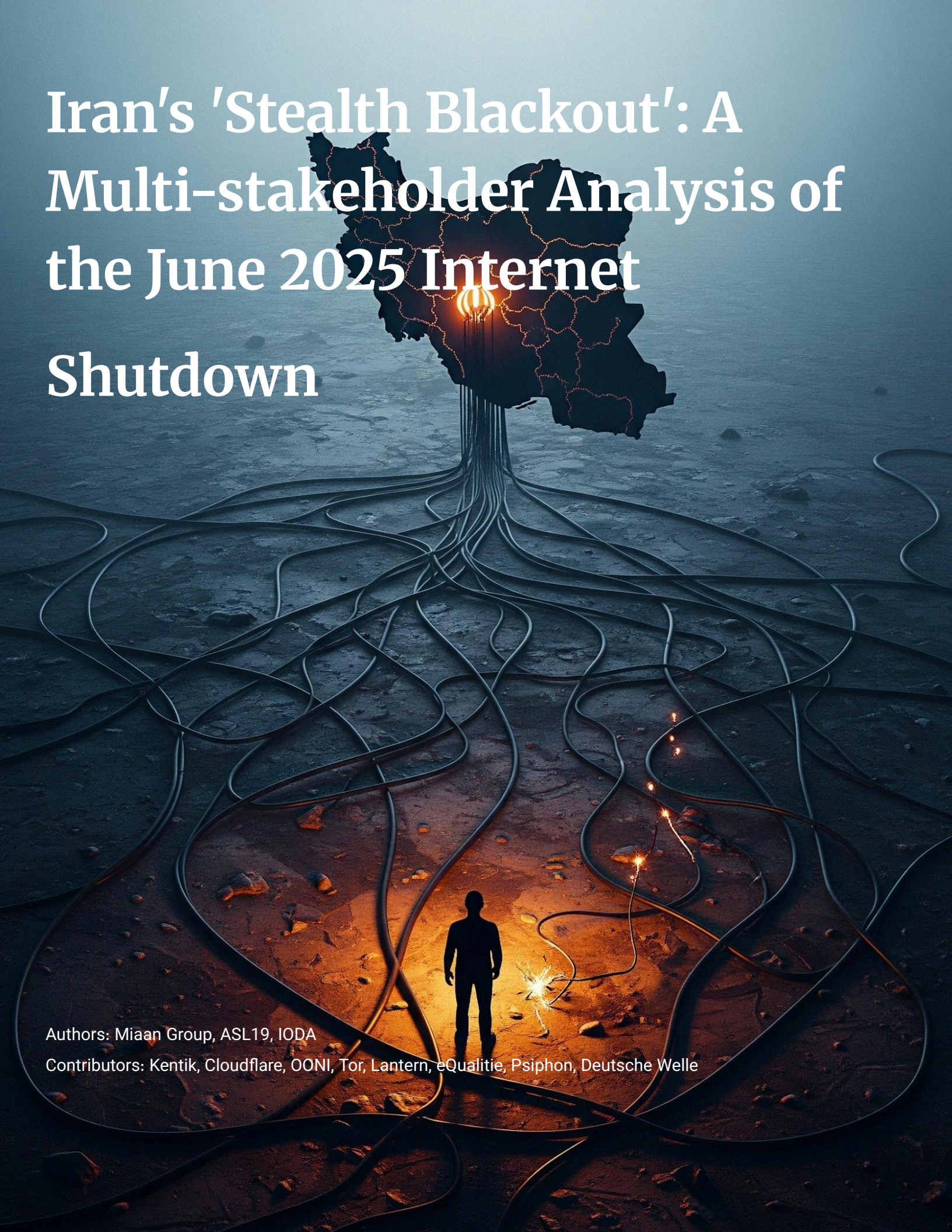
Iran's 'Stealth Blackout': A Multi-stakeholder Analysis of the June 2025 Internet Shutdown



Authors: Miaan Group, ASL19, IODA

Contributors: Kentik, Cloudflare, OONI, Tor, Lantern, eQualitie, Psiphon, Deutsche Welle

Authors: Miaan Group, ASL19, IODA

Contributors (in alphabetical order):

- **Cloudflare**
- **Deutsche Welle**
- **eQualitie**
- **Kentik**
- **Lantern**
- **OONI**
- **Psiphon**
- **Tor**

I. Executive Summary

The June 2025 Internet shutdown in Iran, carried out during the war with Israel, marked a significant and strategically distinct moment in digital repression. This operation, which we term the "stealth blackout," differed sharply from earlier shutdowns that relied on simple, brute-force disconnections. Instead, it was a carefully planned, phased effort to sever the Iranian population's connection to the global Internet while maintaining the illusion of normal connectivity for outside observers. This approach highlights a calculated evolution in the Islamic Republic's efforts to control information and consolidate a state-controlled digital ecosystem through the National Information Network (NIN).

The Stealth Blackout: Technical and Strategic Evolution

The June 2025 operation differed sharply, both technically and strategically, from previous shutdowns. In 2019, the Iranian government cut the country off from the global Internet by simply taking down Border Gateway Protocol (BGP) routes. This method was highly visible and served as a clear indicator of an imminent total blackout, though it took over 24 hours to be implemented nationwide because each provider implemented it separately. The 2019 method was crude and inflicted enormous collateral damage.

In contrast, the June 2025 shutdown did not involve severing BGP routes, which allowed the country to retain an outward appearance of normal connectivity for traditional monitoring tools. Instead, authorities employed a more sophisticated and centralized system at the national border. This approach combined several advanced methods, including DNS poisoning to redirect or block requests for foreign websites, protocol whitelisting to allow only pre-approved domestic services, and Deep Packet Inspection (DPI) to aggressively filter and block traffic from specific tools. Together, these layers of control neutralized many circumvention tools without fully halting domestic services. As a result, during this shutdown, Iran's traffic and connectivity to the global Internet plummeted by about 90%.

While the 2019 and 2025 shutdowns involved both cellular and fixed-line networks, the 2022 shutdown during civil protests utilized different tactics. In 2022, authorities imposed a nightly curfew on cellular operators, affecting the same networks as 2019. However, the duration of the

disruptions in 2022 and 2025 were similar, each lasting for nearly two weeks, while the 2019 shutdown lasted six days. The 2025 shutdown's wartime context was also unique, with the government justifying the restrictions as a means of deterring cyberattacks from Israel.

The Resilient Response: Tools and Community Adaptation:

The June 2025 shutdown had a significant impact on circumvention tools, revealing a new level of sophistication in government interference. Data shows that even when users could connect, their data traffic was often throttled, which in many cases rendered these tools functionally useless for anything more than basic text communication.

Nevertheless, the Internet freedom community reacted quickly, sharing information and deploying technologies that succeeded in keeping millions of Iranians online. They accessed international internet and foreign-hosted content with a greater variety of VPNs and peer-to-peer solutions than in the prior 2019 near-total shutdown. The community relied in part on lessons learned from past shutdowns and closer coordination. The overall success demonstrated that utilizing different technologies, methodologies, and networks increases the possibility of sustained connection even during the most severe internet shutdowns.

Individual tool performance offered critical data on adaptation:

- **Psiphon's** multi-protocol design was crucial in maintaining access for 1.5 million users at the height of the shutdown, roughly one third of its normal user base.
- **Lantern** saw moderate success with its proxyless protocol, which accounts for about 40% of its traffic.
- **BeePass VPN** contributed to censorship tactic research by experimenting with different VPN access key configurations (different combination of network ports and traffic obfuscation prefixes) to investigate the parameters' relevance to the intense blocking. BeePass was providing access to over half a million daily users inside Iran at the start of the war.
- The **Ceno Browser**, with its decentralized, peer-to-peer network, saw a significant increase in active peers, from 600 on June 13 to nearly 8,000 by July 11. Notably, even during the blackout, some Ceno connections remained online.
- **Tor** usage quickly rebounded after the shutdown was lifted, with bridge connections surging during the blackout, indicating users' rapid adaptation.

The goal of this report is not to offer a direct comparison of individual circumvention tool performances. Instead, we explore the evolving tactics of digital repression wielded by the Iranian government, demonstrate the impact of the shutdown on Iranian users, and document the response of the international tool developer community in supporting access solutions for Iranians. Ultimately, the successful outcome—where more Iranians found their way online during this shutdown than the 2019 near-total blackout—underscores a crucial conclusion: a wider variety of tools and tactics will succeed at different times and against different censorship methods, reinforcing the necessity of a diverse and resilient internet freedom ecosystem.

Human Rights Implications

The shutdown's human rights implications were profound and directly linked to a surge in physical persecution. The government exploited the wartime atmosphere to create communication barriers that endangered lives by blocking access to essential services like Google Maps, which led to people getting lost while trying to flee to safety. The government also blocked international One-Time Passwords (OTPs), crippling new sign-ins to secure communication platforms and VPNs. This forced many citizens onto government-approved domestic platforms that have security and privacy vulnerabilities. This deliberate silencing of communication channels suppressed documentation and reporting of human rights abuses, fueled fear, and disproportionately affected journalists, ethnic minority groups, and human rights defenders.

Key Takeaways and Policy Blueprint

The June 2025 Internet shutdown serves as a crucial case study in the evolution of digital authoritarianism. The Iranian government's ability to orchestrate a rapid, centralized, and covert blackout provides a dangerous blueprint that other authoritarian states may seek to emulate. The contrast to the blunt methods of the 2019 shutdown highlights the necessity of sustained investment in resilient circumvention tools, not only to stand up for freedom of expression and access to information, but as a key component of foreign policy. This development underscores the urgent need for coordinated international policy and technological responses to counter these threats and safeguard digital rights.

II. Context

The June war between Iran and Israel prompted an unprecedented period of digital repression and Internet isolation within the Islamic Republic. This was not merely a temporary disruption but a strategic, multi-faceted effort to gain total control over information flows and reshape the country's digital landscape.

During the war, the Iranian government leveraged the wartime atmosphere to tighten its grip on the digital space. The Iranian parliament passed a bill "Intensifying Punishment for Cooperation with Hostile Regimes,"which dramatically expands the scope of criminal acts. Critically, it categorizes the use of satellite Internet services like Starlink as "corruption on earth" (Mofsed-e-Fel-Arz), a charge that can carry the death penalty. This legislation signals the government's determination to criminalize tools for free information access and expand penalties to include technological and media activities linked to "hostile governments."

The government justifies these measures by citing cybersecurity threats—such as satellite-controlled drones, cyberattacks, and foreign media dissemination. Yet the narratives of government officials are often contradictory. For example, Deputy Minister of Communications, Ehsan Chitsaz, publicly challenged this rationale, noting that a downed drone used independent satellite communication, rendering domestic Internet restrictions ineffective against such threats. His remarks reinforce the view that "cybersecurity" served more as a pretext for broader information control, rather than a genuine technical necessity. The official acknowledgment of "temporary restrictions" without a clear explanation from the relevant authorities, further highlights the lack of transparency and the fragmented way the crisis was managed.

Iran's National Information Network (NIN)

Starting in the early 2010s, Iran has pursued the development and adoption of a "National Information Network (NIN)," where essential domestic services, websites, and platforms are hosted on a state-controlled intranet, alongside homegrown apps developed for the Iranian market. Officially, the NIN is promoted as a way to strengthen digital sovereignty, enhance cybersecurity, and reduce reliance on international bandwidth. In practice, however, it functions

as a censorship tool that grants the state the ability to further surveil and restrict people's access to uncensored content, foreign platforms, and secure communication tools.

By keeping the NIN active for banking, government, and e-commerce services, Iran can "switch off" or throttle international Internet connectivity with far less disruptions and costs. This erodes the effectiveness of what is usually referred to as the "collateral freedom,"[1] which relies on governments being reluctant to block the Internet because of the damage it causes to essential services. The June 2025 shutdown is a clear example of how NIN has changed the game. Unlike the nation-wide blackout in 2019, this recent incident showed how Iran has the capacity and will to easily sever international connectivity, stopping information from entering and exiting the country, while keeping the NIN running.

[1] The "collateral freedom" strategy is an approach to Internet freedom that seeks to bypass censorship by making it too costly for a government to block access to information. The idea is that instead of hosting independent news sites, human rights content, or circumvention tools on easily blockable servers, these services are embedded within major cloud platforms or content delivery networks that the government and the country's businesses also rely on.

III. Chronological Overview of Internet Disruptions

In the early hours of June 13, 2025, Israel launched air strikes at Iran, starting what would later be called the Twelve-Day War between the two nations and some of the most aggressive Internet disruptions in Iran in recent years. Drawing from Cloudflare Radar, IODA, and Kentik data[2], the timeline of the disruptions could be broken down to four periods:

- **June 13–17:** Initial government-directed network disruptions
- **June 18–21:** Government-directed Internet shutdown resulting in near total blackout of international traffic
- **June 21–25:** Partial recovery in international connectivity and traffic
- **After June 25:** Recovery in international connectivity with the exception of a 4-hour blackout on July 5, 2025

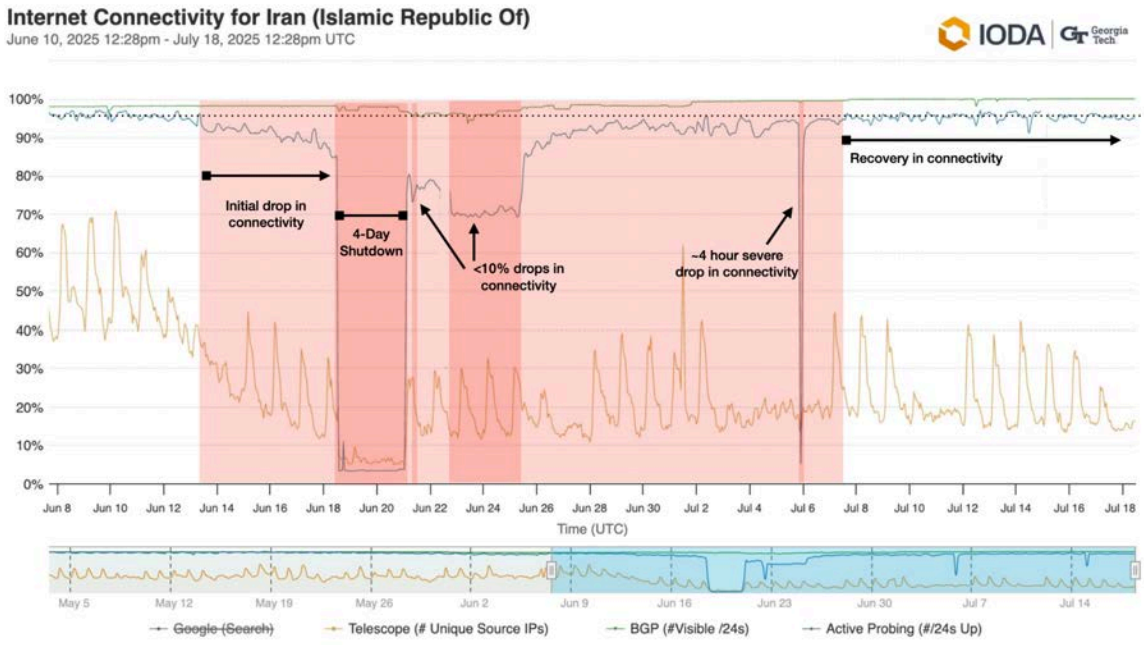


Figure 3.1: IODA data on Internet connectivity for Iran

[2] Cloudflare and Kentik provide traffic data. IODA provides data on Internet infrastructure connectivity.

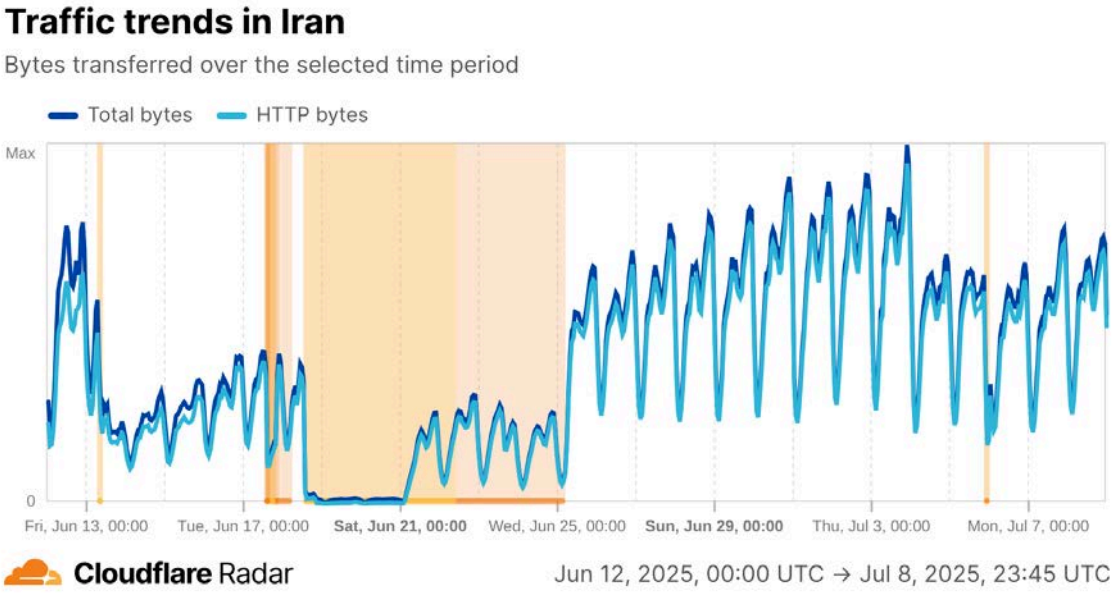


Figure 3.2: Cloudflare data on Internet traffic trends in Iran

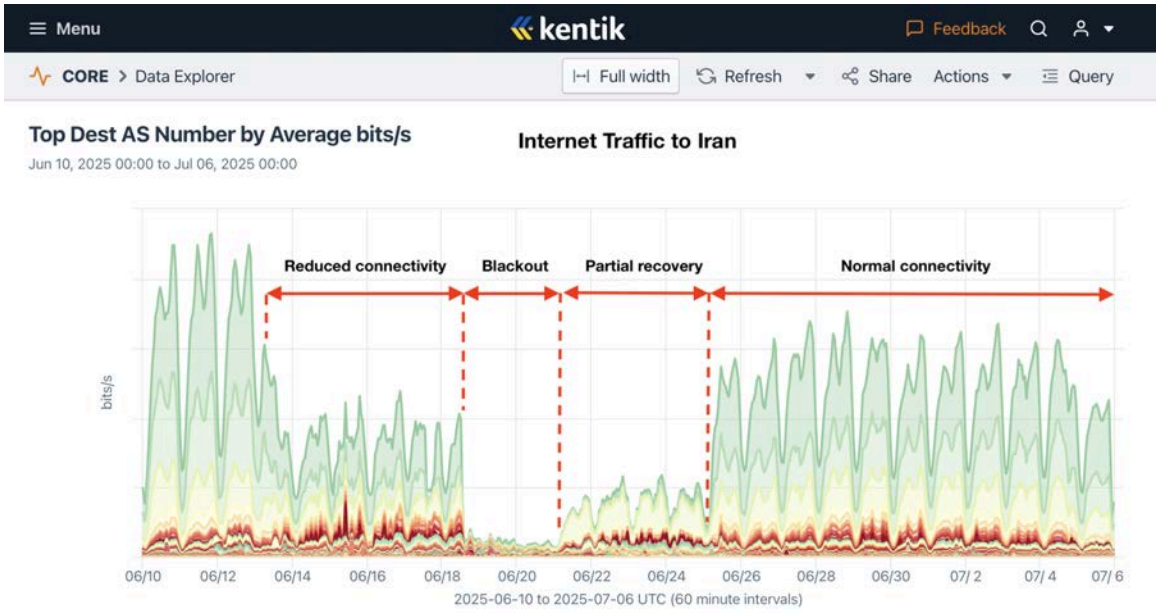


Figure 3.3: Kentik data on Internet traffic in Iran

Phase 1 (June 13-17, 2025): Initial government-directed network disruptions

On Friday, June 13, at approximately 7:00 UTC (10:30 local time), Iran experienced the start of reduced Internet connectivity and shutdowns to international destinations. During this time, the Internet Outage Detection and Analysis (IODA) project observed a slight drop in connectivity while Cloudflare Radar detected a drop in HTTP traffic and traffic to Cloudflare's 1.1.1.1 DNS resolver from Iran. At first glance, these could be attributed to several factors: government-mandated disruptions, damage to essential power and Internet infrastructure from bombings, or a decrease in online activity as residents evacuated urban areas.

On the same day, Iran's Ministry of Communications issued a statement announcing state-imposed Internet restrictions: "In light of the country's special circumstances and based on the measures taken by the competent authorities, temporary restrictions have been imposed on the country's Internet. These restrictions will be lifted once normal conditions are restored." Based on Cloudflare Radar data, this order specifically impacted a selection of network providers, including FanapTelecom (AS24631), Rasana (AS205647 and AS31549), MCCI (AS197207), and TCI (AS58224).

Figure 3.4: Cloudflare Radar data on HTTP traffic in Iran on June 13, 2025

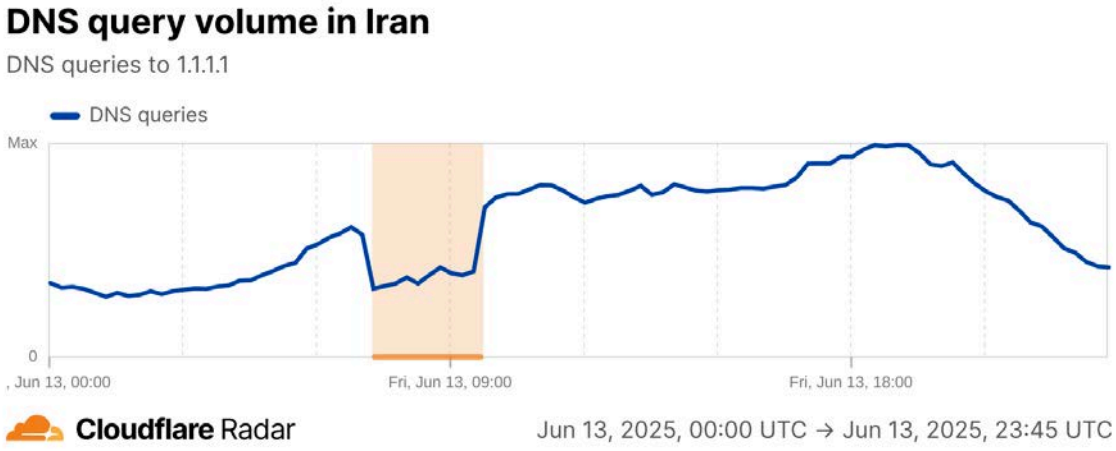


Figure 3.5: Cloudflare Radar data on DNS query (to 1.1.1.1) volume from Iran on June 13, 2025

A new round of restrictions was imposed on June 17, this time reportedly to "ward off cyber attacks," according to Iran's government spokesperson. This began at 14:00 UTC (17:30 local time), impacting multiple networks. Traffic recovered on some networks slowly afterwards. At 15:30 UTC (19:00 local time), FanapTelecom (AS24631) and Pars Online (AS16322) traffic recovered first. And then at 20:00 UTC (23:30 local time) on MCCI (AS197207) and IranCell (AS44244) networks, and subsequently on RighTel (AS57218) and Rasana (AS31549 and AS205647).

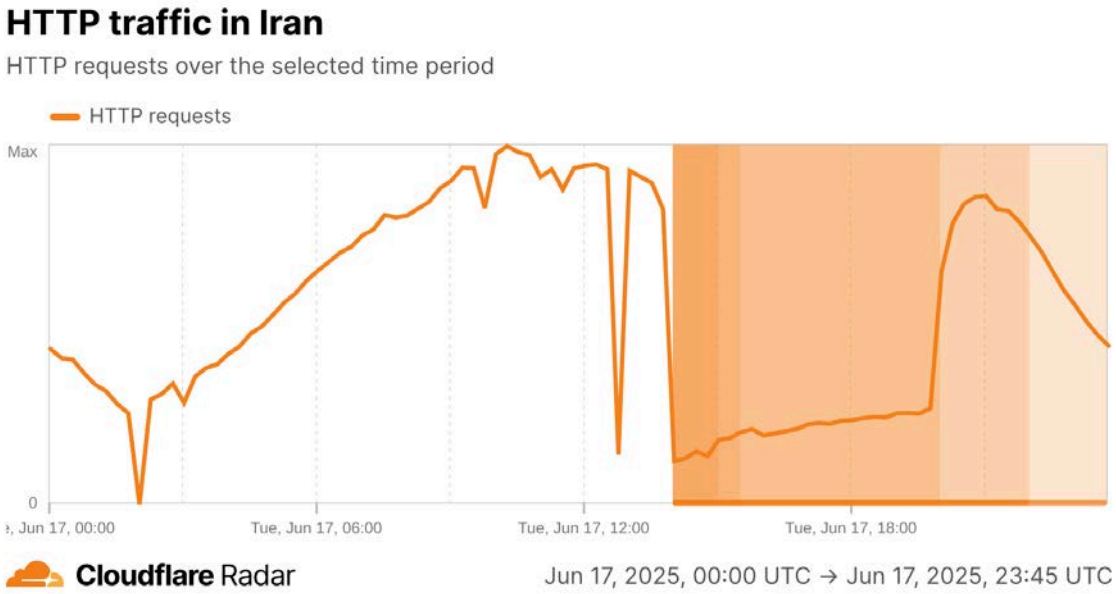


Figure 3.6: Cloudflare Radar data on HTTP traffic before and after the second wave of restrictions on June 17, 2025

Phase 2 (June 18-21): Internet shutdown resulting in near-total blackout of international traffic

A shutdown that cut off Iranians' access to the global Internet began on June 18, 2025. The shutdown was reportedly implemented as a means of "protection against cyberattacks," with a government spokesperson commenting, "We have previously stated that if necessary, we will certainly switch to a national Internet and restrict global Internet access. Security is our main concern, and we are witnessing cyberattacks on the country's critical infrastructure and disruptions in the functioning of banks. Many of the enemy's drones are managed and controlled via the Internet, and a large amount of information is exchanged this way. A cryptocurrency exchange was also hacked, and considering all these issues, we have decided to impose Internet restrictions."

According to Cloudflare Radar, HTTP traffic from Iran dropped sharply to near-zero around 12:00 UTC (15:30 local time) on June 18 and disappeared completely between 19:00-20:00 UTC (see Figure 3.7). Similarly, IODA data showed a drop in Internet infrastructure connectivity starting around 12:50 UTC (see Figure 3.8). And Kentik's Internet traffic data shows a drop off in IranCell (AS44244), TCI (AS58244) and MCCI (AS197207) traffic all around the same time (Figure 3.9). During this phase, Iran's traffic and connectivity to the global Internet plummeted by about 90%. The remaining around 3-10% of international traffic was likely limited to essential services maintained by the state for logistical, financial, and governance needs, or to technical services necessary for the operation of Iran's National Information Network (NIN) during the international shutdown.

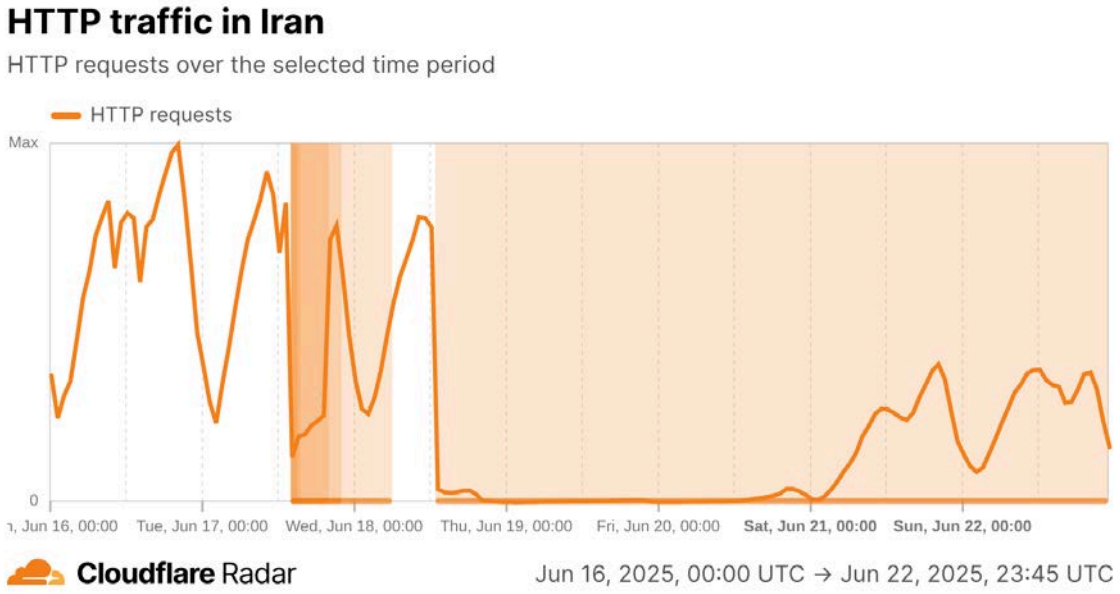


Figure 3.7: Cloudflare Radar data on HTTP traffic between June 16 and June 22, 2025

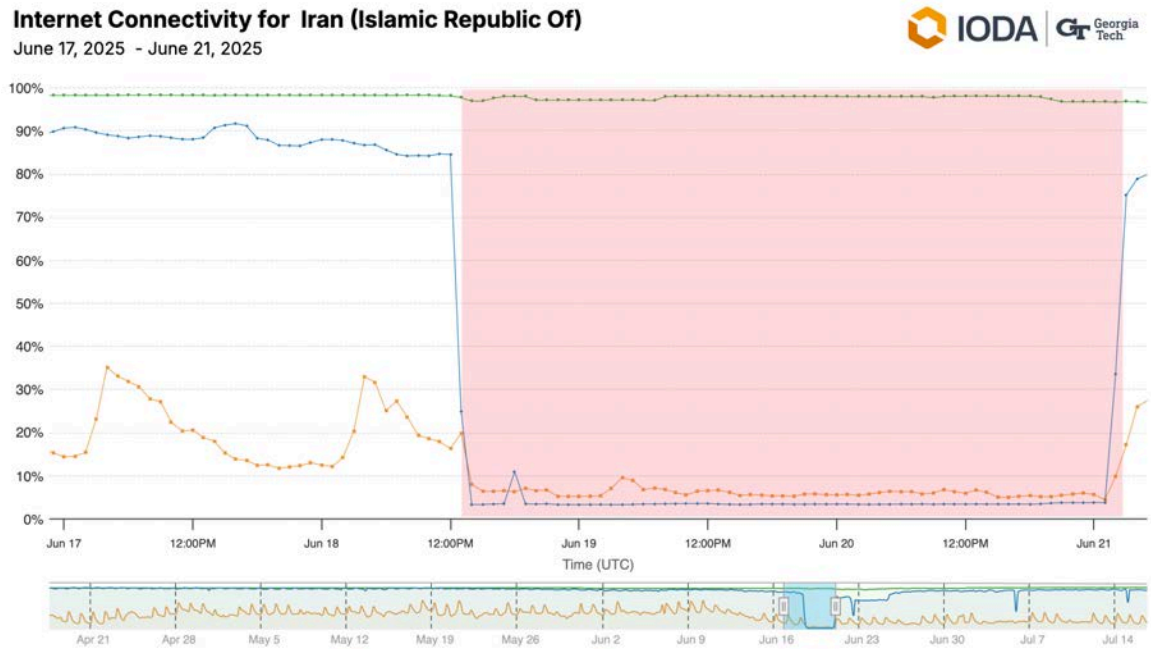


Figure 3.8: IODA Internet connectivity data between June 17 and June 21, 2025

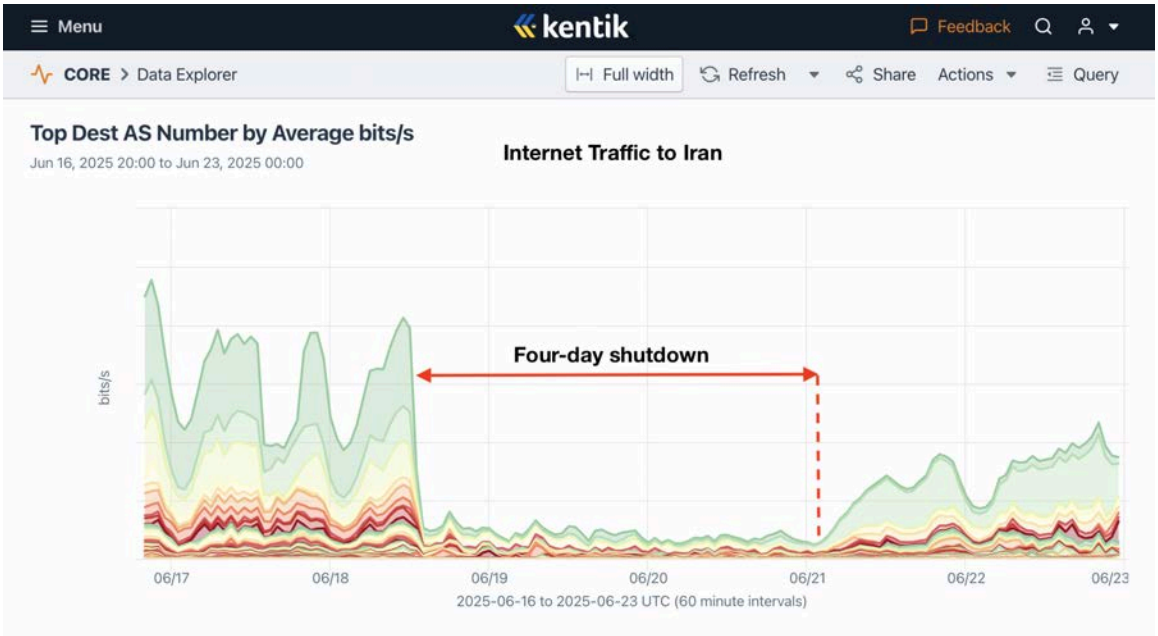


Figure 3.9: Kentik data on Internet traffic to Iran between June 17 and June 23, 2025

Phase 3 (June 21-25): Partial recovery in connectivity and traffic

The near-complete loss of traffic lasted through 02:00 UTC (05:30 local time) on June 21, 2025. Observable traffic recovery on June 21 was gradual and implemented unevenly. While there was an increase in traffic and Internet connectivity across the board (see Figure 3.1, 3.2, and 3.3), the levels remained well below the baselines before June 13. In fact, the early recovery observed on June 21, 2025 was mainly driven by traffic to a couple of networks – TCI (AS58224) and Rasana (AS31549), according to Kentik. The other major Iranian traffic destinations (MTN/Irancell and MCCI) recovered later.

Phase 4 (Post-June 25): Recovery but with temporary blackout on July 5

Traffic from the partial recovery phase settled into a consistent cycle for several days, until returning to expected levels on June 25. However, some post-recovery disruptions on global Internet connectivity occurred on Saturday July 5 between 20:00 and -00:00 UTC, which Iranian authorities claimed to be due to a DDoS attack. Our measurements could not confirm the cause of this blackout, but do show the scope of the disruption.

IV. Circumvention Tool Access and Connectivity

Examining performance data from circumvention tools provides valuable insights into Internet disruption events, complementing information on traffic and connectivity. This data not only illustrates user experience during a disruption but also provides clues about how shutdown efforts might have been executed.

A critical methodological caveat when analyzing circumvention tool data is the inherent lack of standardization in their reporting metrics. These platforms often use disparate measures—such as total data transfer volume, number of unique active users, or per-device throughput (the speed at which data is successfully delivered to an individual device)—which complicates direct, apples-to-apples performance comparisons across different tools during a disruption event. This variance necessitates cautious interpretation of comparative performance claims.

Psiphon

Psiphon played a significant role in maintaining connectivity during the June 2025 shutdown, demonstrating the importance of a multi-protocol approach in the face of sophisticated censorship. Notably, just before the Iranian government's partial shutdown on June 17, a significant increase in Psiphon users was observed. This is anecdotally attributed to more people turning to the tool as other circumvention tools reportedly began to fail.

At the height of the shutdown, as illustrated in figure 4.2, Psiphon enabled nearly 1.5 million Iranians to access the uncensored Internet and transferred over 330 terabytes of data through its network. This resilience shows that, despite aggressive blocking by authorities, certain design choices can still keep information flowing, and investment in such technology is well-warranted.

Psiphon's resilience stemmed from its multi-protocol design, which allowed it to find and exploit the "holes" left in the infrastructure. Because the Iranian authorities must maintain some level of connectivity for essential logistical, financial, and governance services, some channels remained open. Psiphon's ability to take advantage of these remaining channels allowed it to continue providing open Internet access at scale, even as other tools experienced severe blockages.

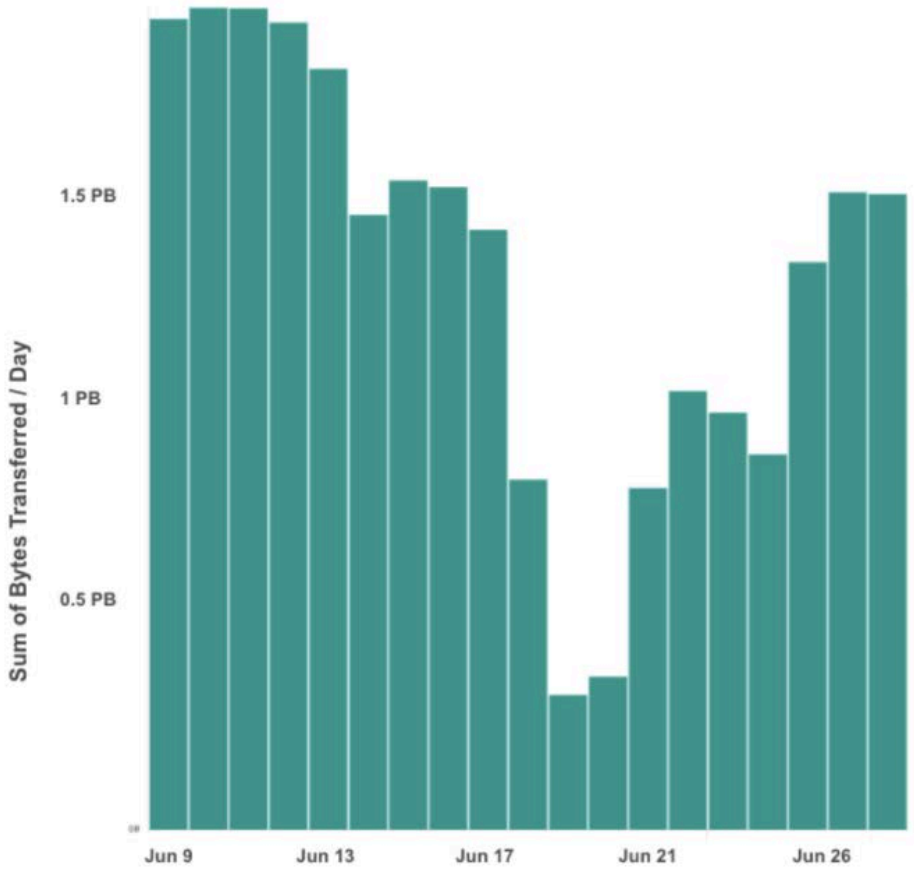


Figure 4.1: Number of Bytes Transferred per Day Through the Psiphon Network (June 9-30, 2025)

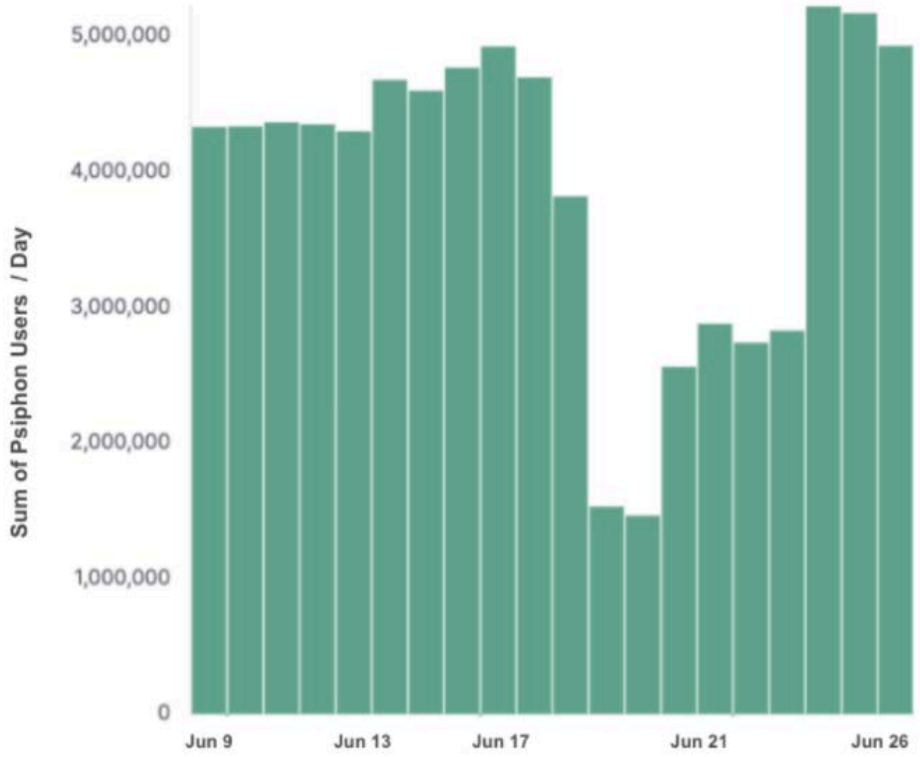


Figure 4.2: Number of Psiphon Users per Day (June 9-30, 2025)

Lantern

Beginning on June 18, Iran entered a near-total Internet shutdown that impacted both cellular and fixed-line networks. Lantern's traffic on MCI saw a significant drop during this period, as illustrated in Figure 4.4. Clients were unable to retrieve configuration files from Lantern servers, leading to a decline in throughput per device from 0.24 GB on June 12 to 0.01 GB by June 20 (Figures 4.5 and 4.6). By the end of June, Lantern's traffic had recovered to approximately 65% of its pre-shutdown levels.

An important finding was that the sharp drop in throughput per device coincided with a surge in users on June 13 (see Figure 4.7).This shows that even when users were able to connect, their data flow was minimal, likely due to aggressive throttling or only brief windows of connectivity.

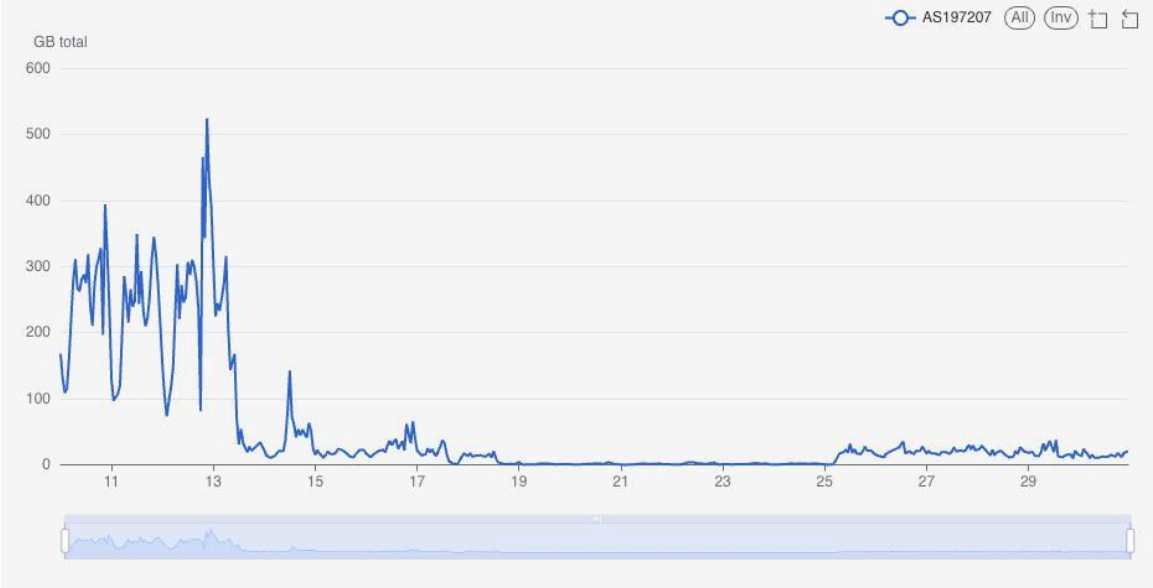


Figure 4.4: Lantern Traffic on MCI (June 10–30, 2025)

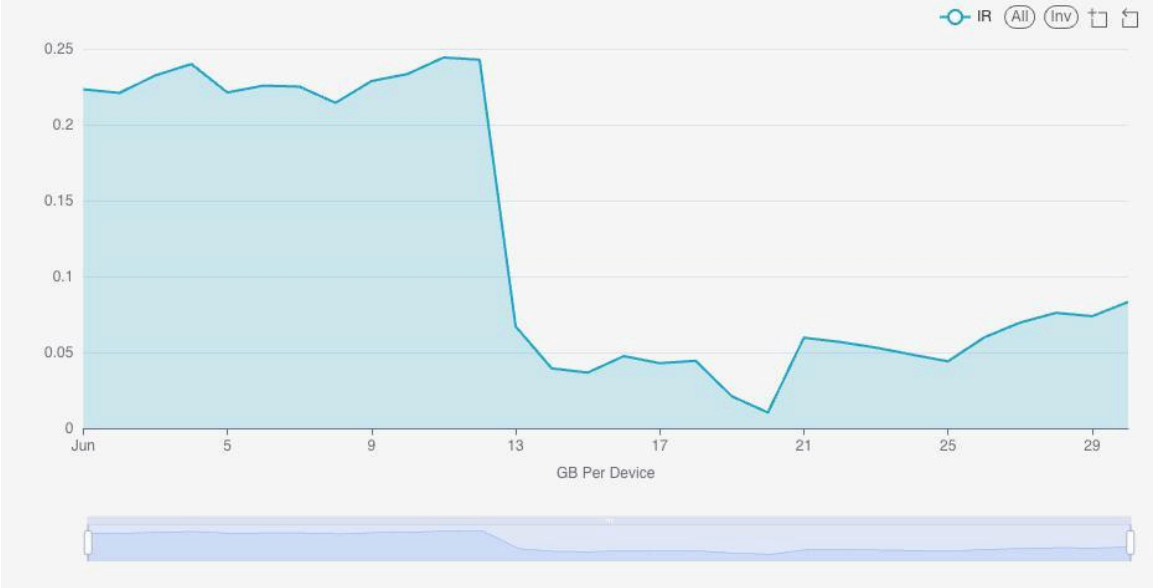


Figure 4.5: Lantern's per-device throughput in Iran during June 2025

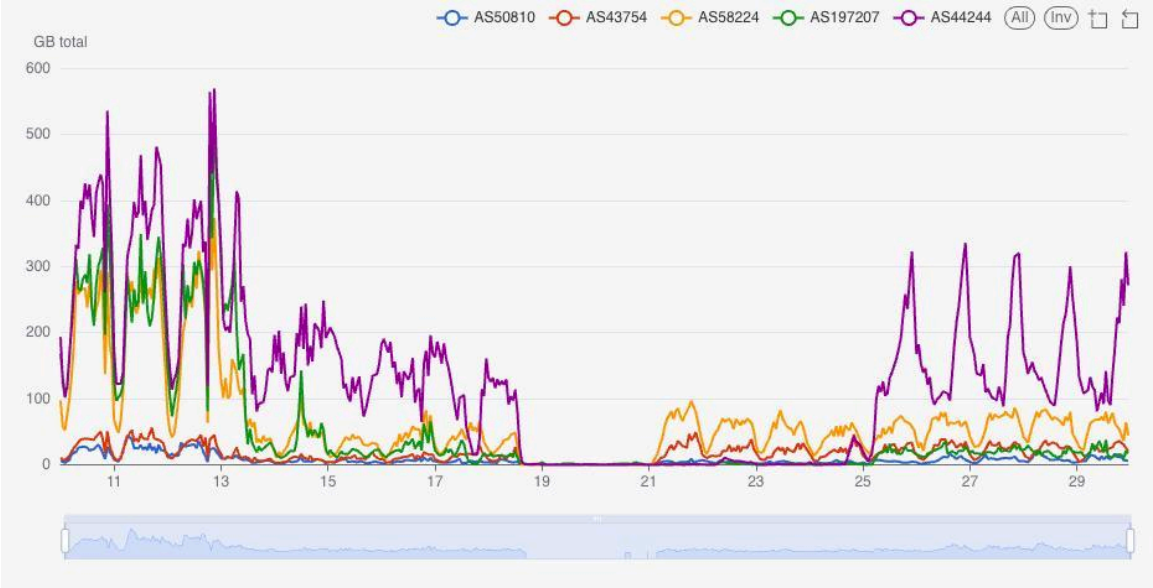


Figure 4.6: Lantern throughput in Iran by top 5 ASNs (June 10–30, 2025)

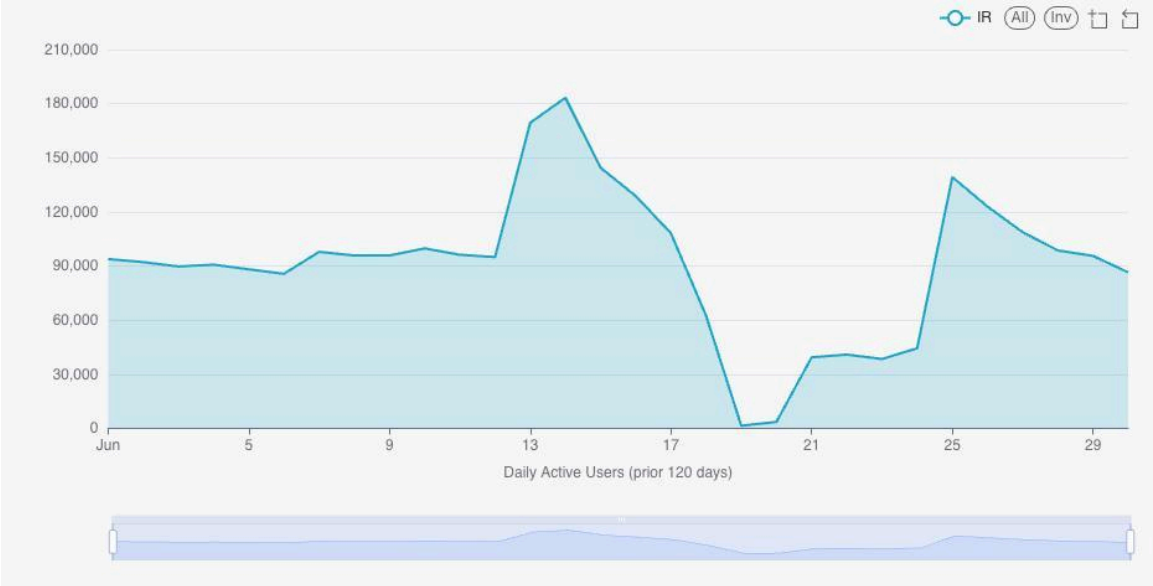


Figure 4.7: Daily Active Users in Iran during June 2025

During the outage, the Lantern team tested several mitigation strategies. They deployed Shadowsocks with DNS prefixes on a different port, after reports indicated that UDP traffic on that port was working for Psiphon. However, this did not significantly increase Lantern's traffic. The increase in traffic starting on June 21 was primarily due to existing Lantern protocols and

data centers regaining access. Similarly, the return of cellular networks, especially on MCI, saw TLS fragmentation strategies begin to work again.

One Lantern strategy that showed moderate success was its proxyless protocol, built on the Outline SDK that relies on Intra technology. Early in the shutdown, the Lantern team saw proxyless working for Instagram and YouTube in particular, though per-domain success rates are not available. Currently, about 40% of all traffic in the latest Lantern versions is sent via this proxyless method.

BeePass VPN

ASL19's BeePass VPN – built on Outline technology with the Shadowsocks protocol – saw similar patterns to other tools. As illustrated in Figures 4.8 and 4.9, the orange box "A" shows disruptions that had led to reduced traffic between June 13 and 17 (Phase 1). The red box "B" shows the blackout period and partial recovery (Phase 2+3) and the purple box "C" shows the sudden temporary shutdown on July 5 during the recovery phase.

Interestingly, a comparison of Figures 4.8 and 4.9 in Phase 1 (box "A") shows that the number of unique IPs connected to BeePass VPN servers did not drop as drastically as the egress (outbound) traffic volume. One way to interpret this is that BeePass users were still able to connect to the VPN servers, but they could not surf the web as before. In other words, at this phase, the authorities likely interfered with the traffic (connectivity quality) but not the connection itself, which is consistent with Lantern's findings as well.

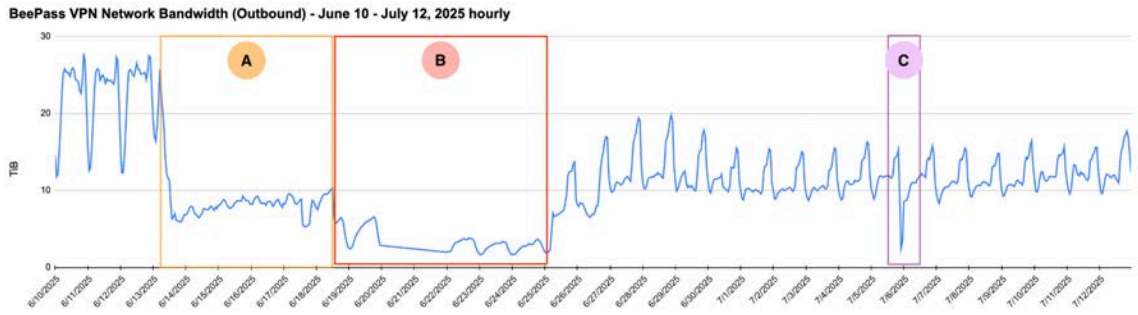


Figure 4.8: BeePass VPN network bandwidth (outbound)

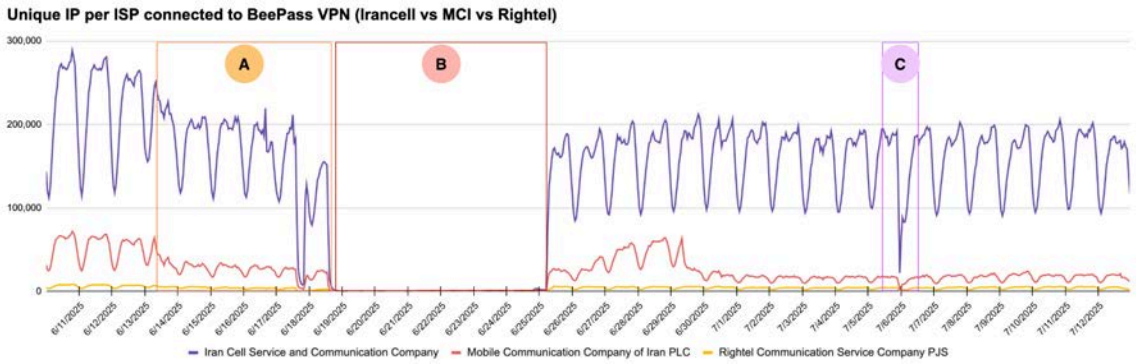


Figure 4.9: Unique IPs connected to BeePass VPN servers (Top 3 Iranian ISPs)

Following initial user feedback and collaborative discussions with other service providers, network engineers at BeePass tested various methods to circumvent the ongoing internet disruptions. They distributed a range of VPN access keys configured with different combinations of network ports, including 53 (DNS) and 443 (HTTPS), and utilized several traffic obfuscation prefixes such as HTTP Post requests, TLS ClientHello, and SSH. These configurations were evaluated across multiple Internet Service Providers in various cities. Unfortunately, they did not seem to make significant difference, suggesting the filtering mechanism was most likely not based on these specific connection parameters.

By June 25, BeePass VPN usage in Iran recovered to approximately 50% of its pre-shutdown levels. Plans are underway for further testing and improvements to the tool's circumvention features, aiming to enhance its resilience against future disruption events.

Ceno Browser

eQualitie's Ceno Browser is a mobile browser that uses BitTorrent technology to enable users to access and share web content during disruptions and shutdowns. With its offline, decentralized nature, measuring Ceno usage is inherently challenging. However, we could draw insights about Ceno's peer-to-peer network size and efficacy from a few metrics:

- **The number of active peers**[3]: "Active peers" is defined as Ceno users who have opted in to share content they have retrieved, making their devices available to others in the

[3] We estimate that 5–10% of Ceno users fall into this peer-sharing category. While many users are willing to share, not all devices are actually reachable on the network due to barriers like carrier-grade NAT.

network. There was a significant increase of active peers on Signal from 600 on June 13 to nearly 8,000 by July 11.

Figure 4.10: Cumulative statistics for active peers in Iran during the reporting period (The gap in data on June 17 indicates the most severe period of network isolation when we lost access to the Iranian segment of the BitTorrent network.)

- **The number of "check-in" requests completed**: eQualitie uses the "check-in" feature to push network announcements to users and to count the number of users that opened the Ceno browser. If a check-in request is completed, it means a Ceno user was able to reach eQualitie's website; in other words, they were able to retain some global Internet connectivity through the application. This is important because even if only a small number of users are able to connect to sources outside of Iran (via the Ceno bridge network or other means), their browsed data is automatically spread throughout Ceno's peer-to-peer network inside the country.

  As shown in Figure 4.11 below, some connectivity persisted during the shutdown period (June 18-21).Specifically, connections from Aria Shatel ISP, Hetzner and ASLine Limited held up while others seem to have failed. This signals the importance of having Ceno users on different networks worldwide, especially those who opt-in as bridges. This allows the usage of their device as a temporary proxy, enabling the Iranian diaspora community to come to the digital assistance of their friends and family back home.

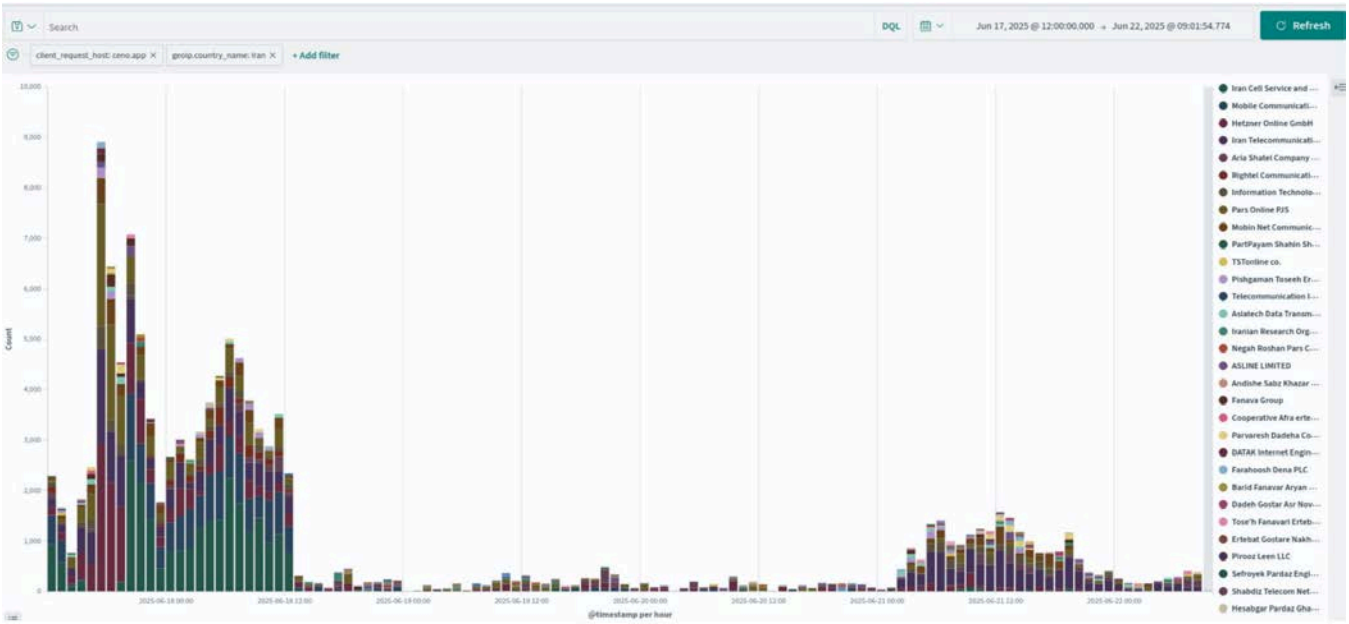


Figure 4.11: Number of Ceno connections per ISP from June 18 to 22, 2025

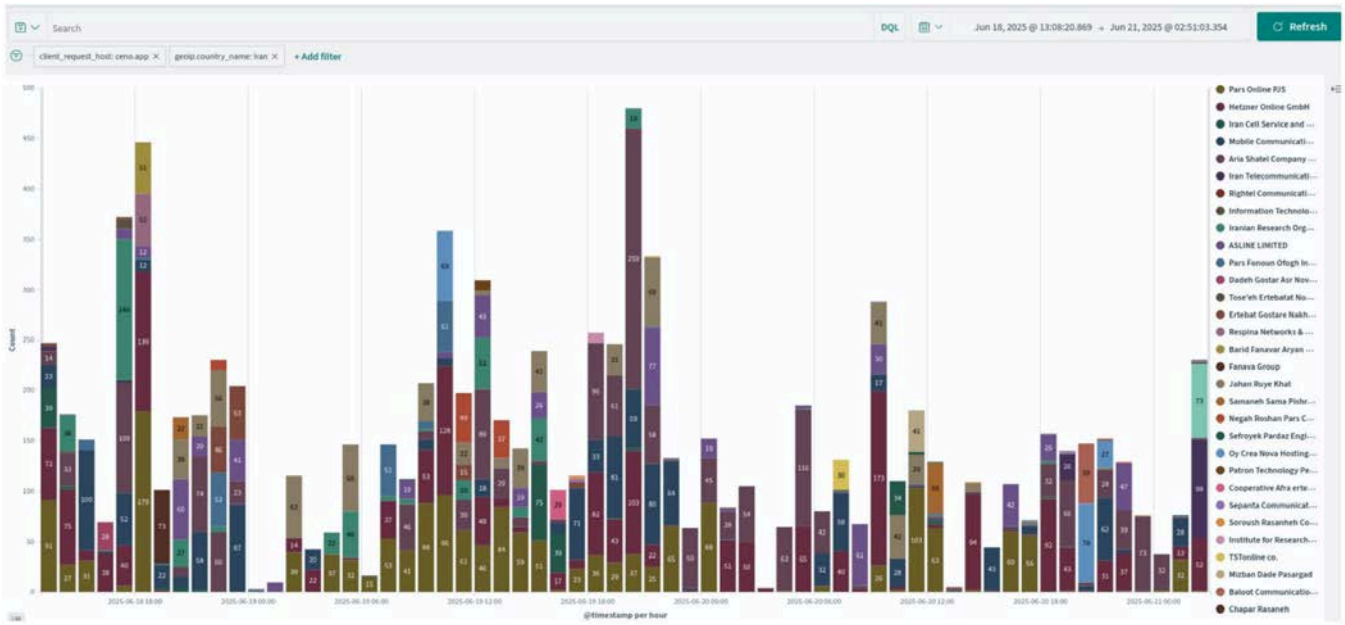


Figure 4.12: Number of Ceno connections per ISP during the shutdown period (zoomed in)

Tor

As early as June 13, when the Twelve-Day War started, Tor saw a drop in direct connections from Iran (Figure 4.13) and a surge in bridge connections from Iran (Figure 4.14). The latter signals that many people were trying to use tools like Tor to reach the uncensored Internet.

However, on June 18, once the Internet was cut off, very few people were able to connect to Tor bridges from Iran.

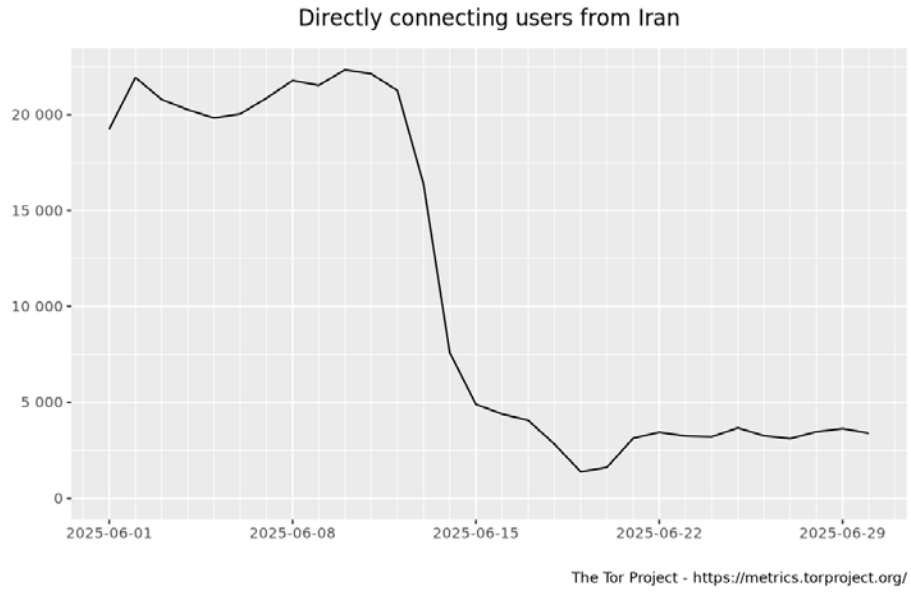


Figure 4.13: Direct Tor connections from Iran (June 2025)

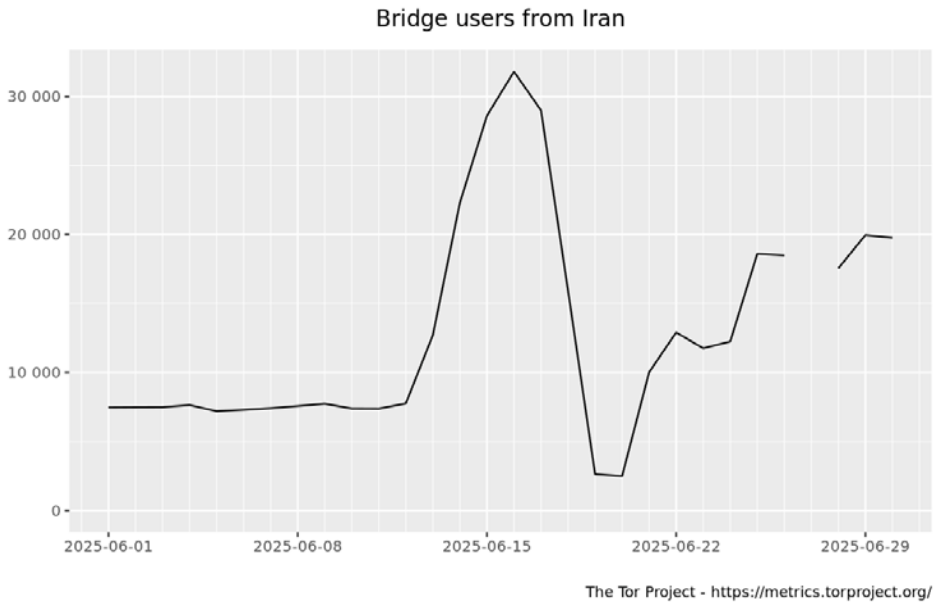


Figure 4.14: Tor Bridge users from Iran (June 2025)

Among bridge users in Iran, snowflake has usually been the preferred transport to connect to Tor. But as demand for Tor bridges surged during the war, data showed that many were also using obfs4. This likely reflects users searching for alternatives while the snowflake network was overloaded globally during the war.

To start a snowflake connection, clients would send a domain-fronted request to a broker. This request's purpose was to pair the client with a proxy, after which the client would connect to the designated proxy via WebRTC. During the initial phase of the war, a significant number of these connection attempts successfully reached Snowflake proxies but subsequently failed to establish a connection. This led to repeated requests for new proxies, quickly depleting the available proxy pool and placing a heavy burden on the broker with a high volume of requests.

From June 21-25 (Phase 3), the Internet shutdown was lifted, although abnormal network access persisted. We suspect some censorship of UDP traffic continued to occur, despite measurement difficulties. Ultimately, Tor bridge usage in Iran quickly rebounded after the shutdown, exceeding pre-war levels. This surge, mirroring increased downloads of other circumvention tools, suggests a heightened public awareness and demand for tools like VPNs and Tor following the war.

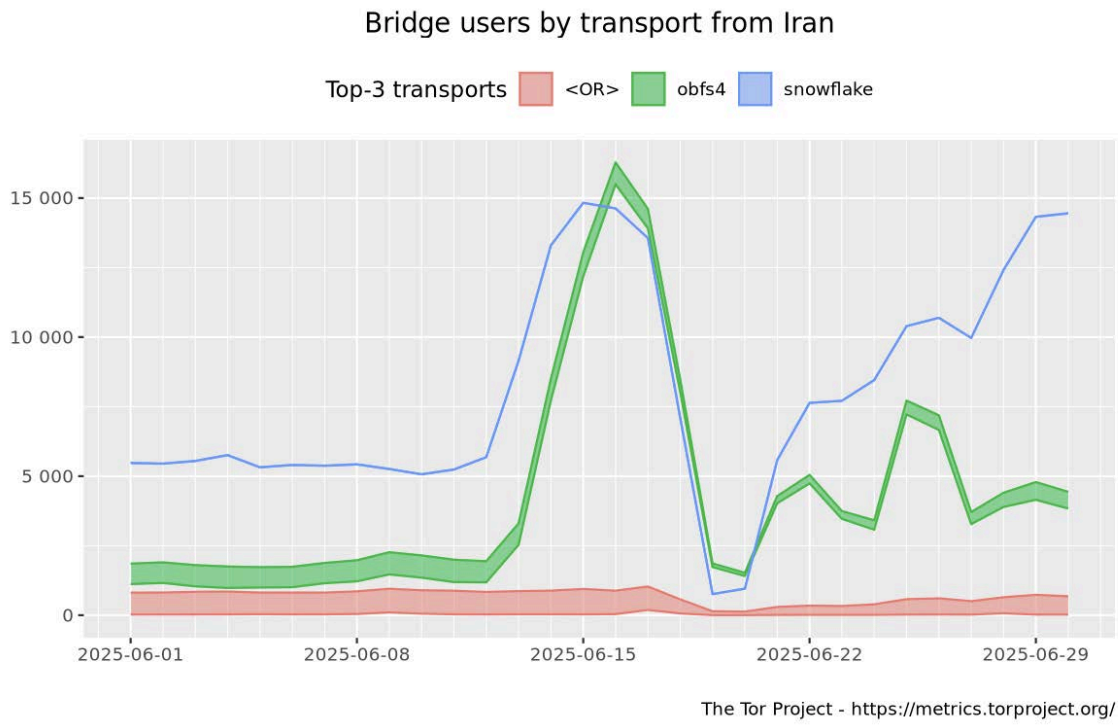


Figure 4.15: Bridge users by transport (top 3) from Iran (June 2025)

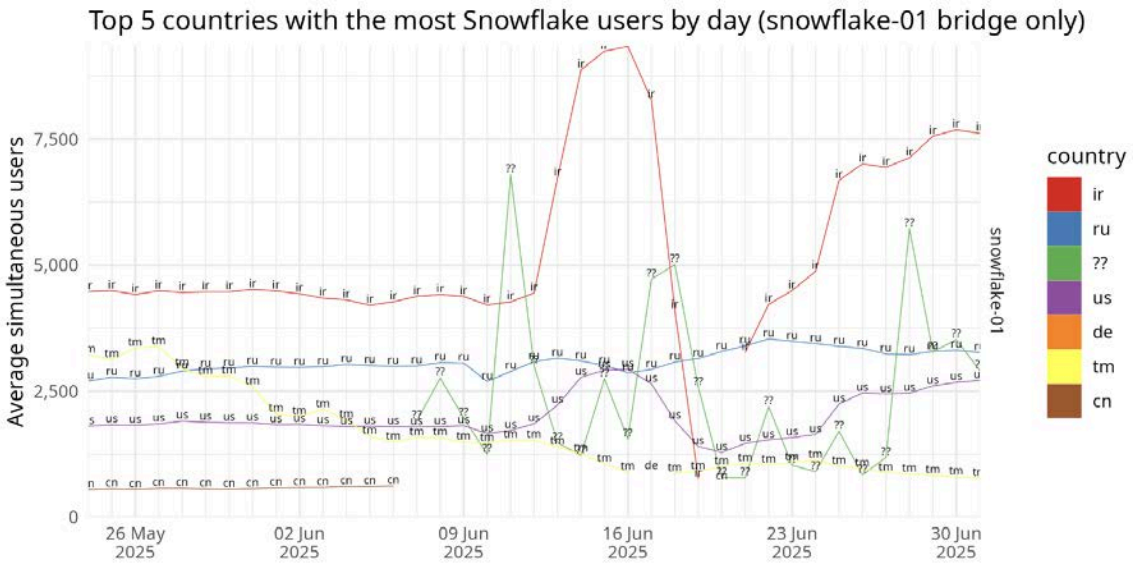


Figure 4.16: Snowflake-01 bridge users by country (June 2025)

V. Access to international platforms and media

Beginning on June 13, Iranians faced severe disruptions to international platforms and services, including WhatsApp and key Google services. While basic Google Search remained intermittently available, other essential platforms like Gmail, Google Maps, and the Google Play app store were blocked or rendered inaccessible. This also extended to other crucial app marketplaces, such as Samsung's Galaxy Store, preventing users from downloading or updating apps during the crisis.

The impact was immediate and personal. Users reported to Miaan's Filterwatch that the disruptions to GPS and Google Maps caused people to get lost while attempting to flee Tehran and other cities for safety.

Another layer of disruption involved the blocking of international One-Time Password (OTP) SMS codes as reported by many users to Filterwatch and Miaan's Digital Security Helpdesk. This tactic effectively crippled secure communication apps and VPNs that rely on these verification texts for registration or login. By preventing the delivery of OTPs from services like WhatsApp, Telegram, Signal, and Google, authorities effectively choked off access to secure and encrypted communications. The government offered no public explanation and denied any issues when users inquired, a deliberate policy to cripple encrypted communications under the

guise of security. While some apps like Signal and Telegram had been blocked prior to the war, users had found ways to circumvent these blocks. However, the OTP blocking prevented new users from downloading or updating these apps, effectively locking them out.

This inaccessibility of international services forced a migration to domestic platforms. Users, desperate to stay in contact with loved ones, shifted to government-approved messaging apps such as Rubika, SoroushPlus, and Bale. A joint Miaan-OTF report has highlighted significant security and privacy vulnerabilities in these applications, and their use is not recommended. This forced shift was a significant victory for the government's long-standing goal of promoting a national Internet, a feat that years of prior efforts failed to achieve.

Below, we delve deeper into the technical reasons for the inaccessibility of WhatsApp and Google products specifically.

WhatsApp

During the war, Iranian authorities urged residents to delete WhatsApp, citing concerns that data might be shared with Israel. Simultaneously, users within Iran began reporting that WhatsApp was being blocked.

To investigate this blocking, we referred to data from the Open Observatory of Network Interference (OONI).[4] Instant messaging apps like Telegram, Facebook Messenger, and Signal have been blocked in Iran for years, and remain blocked to this date. Access to WhatsApp was blocked during the 2022 Mahsa Amini protests, and the block remained in place for more than two years. Iran reportedly lifted the WhatsApp block in December 2024, and this is corroborated by OONI data.

Amid the war, OONI data showed signs of renewed interference with WhatsApp access. A high volume of anomalies was recorded in OONI Probe tests on multiple Iranian networks from June 15 to July 12, 2025, suggesting that access to the app may have been blocked on some networks.

[4] Since 2012, OONI has developed OONI Probe, a free and open-source software that measures Internet censorship, including the blocking of WhatsApp. With over two billion measurements from 29,000 unique Autonomous Systems (ASes) globally, OONI maintains the world's largest open dataset on Internet censorship.

The chart below, which aggregates OONI measurement coverage for WhatsApp, visually represents this interference.

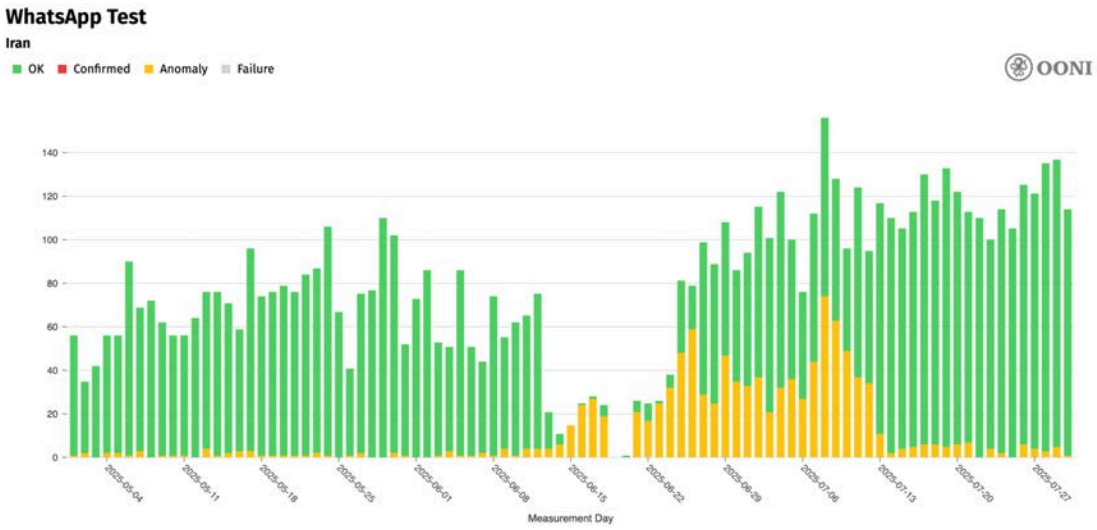


Chart: OONI Probe testing of WhatsApp on 48 ASes in Iran between 1st May 2025 to 31st July 2025 (source: OONI data).

This chart shows a significant drop in OONI WhatsApp measurement coverage from June 13-24, which correlates with the dates of the war. This period also corresponds with the Internet disruptions observed in IODA and Cloudflare Radar data.

Between June 13 and 18, the drop in coverage suggests a potential Internet disruption. However, the fact that some measurements were still recorded shows that Iran did not experience a total Internet blackout. This hypothesis of reduced connectivity is consistent with IODA data.

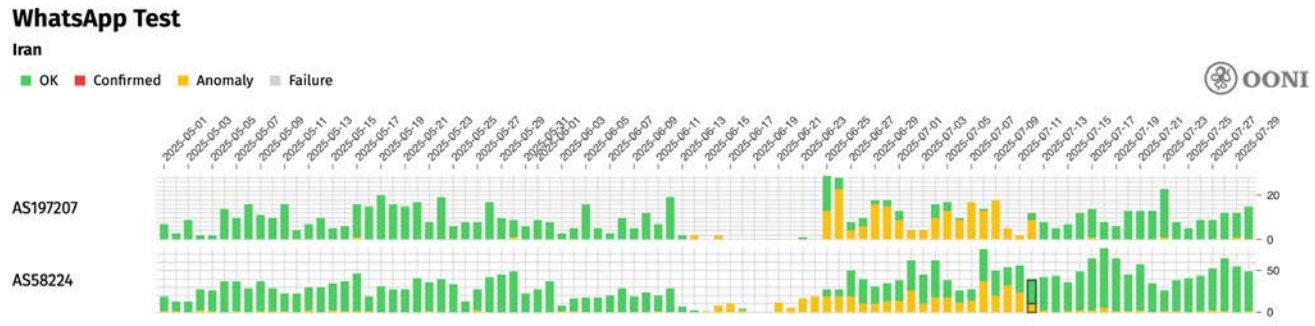
Between June 19 and 20, there was an almost complete absence of OONI measurements, indicating a severe Internet shutdown that prevented users from submitting data. This finding aligns with the near-total connectivity shutdown observed in both IODA and Cloudflare Radar data. OONI measurements also confirm that connectivity was gradually restored from June 21, and traffic had largely recovered by June 25.

Beyond general connectivity disruptions, OONI data also suggests that ISPs resumed the blocking of WhatsApp during this period. The chart above clearly shows a spike in anomalous measurements (annotated in orange) between June 15 and July 12, indicating that access to

WhatsApp may have been blocked on some networks. OONI's methodology classifies a measurement as an "anomaly" if key steps, such as TCP connections, DNS lookups, or HTTP requests, fail.

A high volume of anomalies provides a strong signal of blocking, especially when compared to the global context. OONI data confirms that WhatsApp was globally reachable during these dates, which rules out the possibility that the anomalies in Iran were due to a global outage.

Notably, disaggregating the data by network shows that the majority of anomalies occurred on the MCI (AS197207) and TCI (AS58224) networks.



The technical data from these anomalous measurements reveals a specific method of censorship. Instead of simply dropping all packets, which would suggest a complete connectivity failure, many TCP connections to WhatsApp endpoints were successful. However, the TLS handshakes for WhatsApp Web (web.whatsapp.com) and the WhatsApp registration service (v.whatsapp.net) consistently failed with timeout errors.

This is a key indicator of TLS interference. During a TLS connection, the initial "ClientHello" message is unencrypted and contains the Server Name Indication (SNI), which specifies the domain a user is trying to reach. Censors can read this unencrypted information using Deep Packet Inspection (DPI) technology and then block the connection if the SNI field matches a disallowed domain. The timeout errors observed in OONI data indicate that the connections were being intentionally stalled after the ClientHello message was sent, a classic sign of SNI-based filtering. This is consistent with censorship methods known to be adopted by Iranian ISPs.

Image: OONI network measurement data from the testing of WhatsApp on MCI in Iran on 23rd June 2025, showing that the TLS handshakes to WhatsApp Web (web.whatsapp.com) and the WhatsApp registration service (v.whatsapp.net) resulted in timeout errors (source: OONI data).

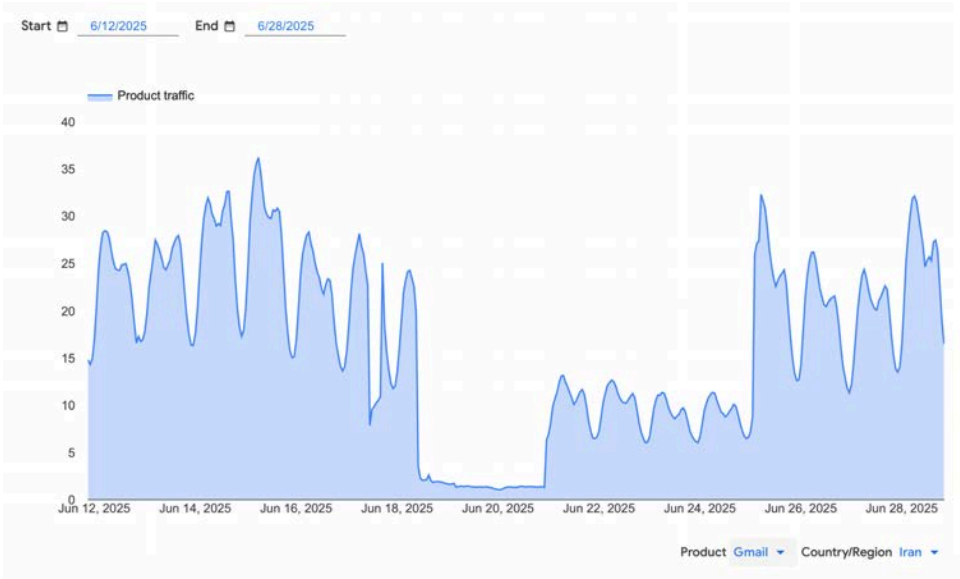
In conclusion, based on the OONI data, the disruption to WhatsApp in Iran was a two-pronged issue. It was a combination of both a widespread Internet shutdown that impacted all online services and a more specific, technical form of censorship targeting the app. The general Internet shutdowns, as evidenced by the drop in OONI measurements, made it difficult for users to connect and submit data. However, even when connectivity was available, the data shows that Iranian ISPs were actively blocking WhatsApp through SNI-based filtering, which caused TLS handshake timeouts. This indicates a deliberate and sophisticated method of state-level interference, separate from the broader connectivity disruptions caused by the war.

Google Services

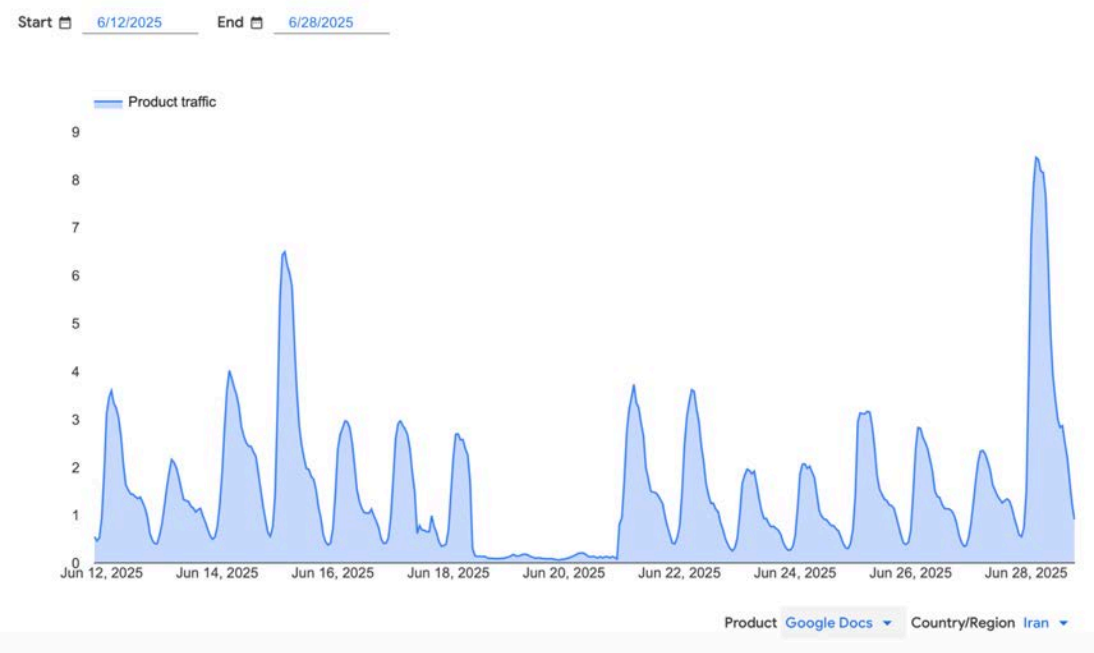
Based on Google's Transparency Report, Google services experienced different periods of disruption during the war.

Google Web Search went down for approximately 24 hours, starting at 9:00 AM UTC on June 18. Google Images experienced a similar timeline.

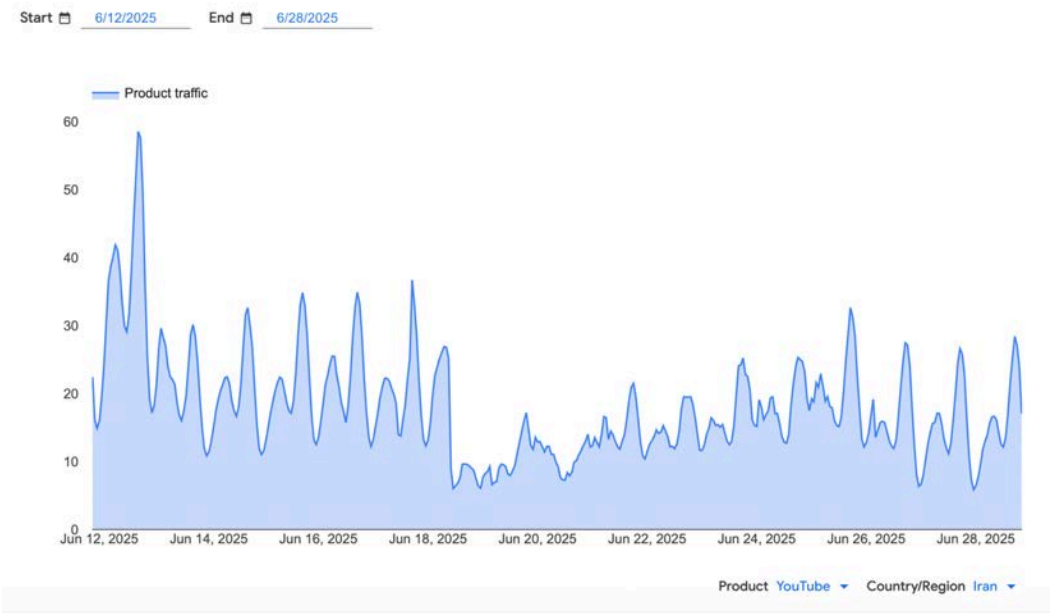
Gmail traffic declined around 9:00 AM UTC on June 18, partially recovered on June 20, and was fully restored on June 25. Google Maps and Google Translate experienced similar timelines.



Google Docs traffic declined around 9:00 AM on June 18 and recovered by 12:00 PM on June 21. Google Sheets and Google Earth experienced similar timelines.

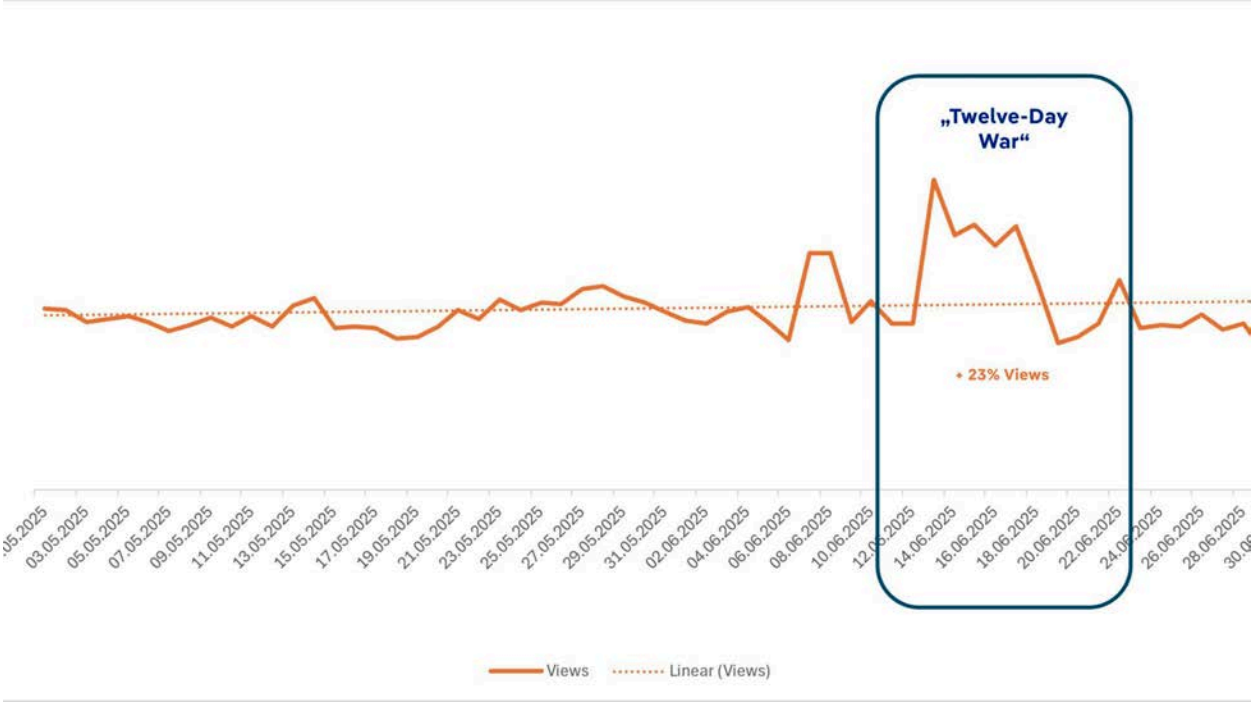


Youtube experienced a similar traffic decline on June 18 and gradually recovered thereafter.



Deutsche Welle

Following the start of the war and prior to the shutdown, demand for Deutsche Welle's media content in Persian surged, demonstrating the critical need for international media and credible sources of information at this time. However, this surge was quickly cut short. As the graph below illustrates, Deutsche Welle's reach plummeted—like that of other international platforms—when Iranian authorities implemented a widespread internet shutdown, effectively blocking Iranians' access to the global internet.



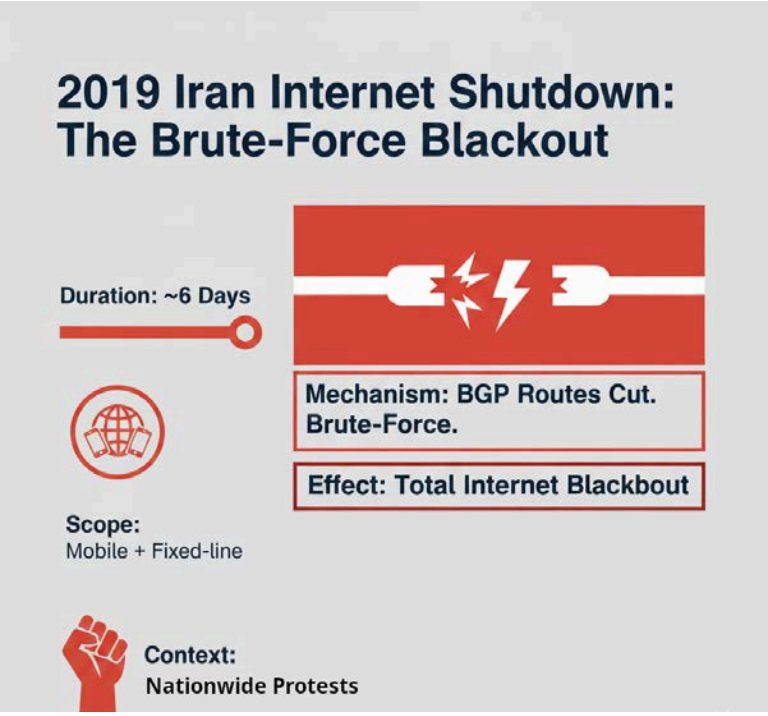
VI. Technical Evolution of Iran’s Internet Shutdowns: 2019, 2022, & 2025

Iran’s nationwide Internet shutdowns in November 2019 (“Bloody Aban”) and June 2025 (during the Iran–Israel war) illustrate a dramatic evolution in state censorship strategies, from blunt

disconnection to surgical precision. While both events cut citizens off from the global Internet, their technical mechanisms, speed, visibility, and strategic impact diverged sharply.

2019 Shutdown: Brute-Force Disconnection

In 2019, the shutdown was carried out by ordering multiple Internet service providers (ISPs) and mobile operators to withdraw Border Gateway Protocol (BGP) routes, effectively severing international connectivity. The process was distributed and staggered: cellular networks were cut first, followed over several hours by other providers. Full nationwide isolation took more than 24 hours, with global traffic dropping to just 5% of normal.



This brute-force method was highly visible in global monitoring systems such as IODA, which recorded abrupt drops in routing, probing, and reachability data. Although crude, the disconnection was nearly absolute: citizens could not access foreign networks, and VPNs or circumvention tools were rendered useless because no international traffic could pass through. Only domestic services hosted on the National Information Network (NIN), such as banking and government apps, remained functional.

Strategically, the 2019 blackout succeeded in information quarantine but inflicted enormous collateral damage. Its slow rollout and reliance on decentralized compliance from ISPs also

highlighted operational inefficiencies.

2022 Shutdown: The "Digital Curfew" on Mobile Networks

Strategically, the 2019 blackout succeeded in information quarantine but inflicted enormous collateral damage. Its slow rollout and reliance on decentralized compliance from ISPs also highlighted operational inefficiencies.

In 2022, following the death of Mahsa Amini and ensuing mass protests, the Iranian state introduced a subtler but still powerful form of internet repression that FilterWatch calls a "digital curfew." Rather than a full blackout, the state imposed regular, recurring shutdowns on mobile networks, especially in the evenings from ~4 PM until midnight. Over the course of about 13 consecutive days (21 September to 3 October), the mobile providers Irancell, MCI (Hamrah-e-Aval), and RighTel were frequently disconnected for international traffic during protest hours. On specific later dates in October (8, 12, 15), further shutdowns occurred.

Mechanisms & Effects

The outages were time-limited and repeated, rather than continuous and they were lifted overnight and resumed the next day during peak protest windows.

- During the mobile shutdown windows, fixed-line (broadband) connectivity generally remained intact, albeit under heightened filtering or slowdown; this meant some users could still access international internet via wired connections.
- Measurement tools (IODA, Cloudflare, Kentik) registered drops in mobile network routing and traffic volume during the shutdown periods, confirming the pattern.
- Concurrently, many internet services and platforms were subject to targeted blocking (e.g. Instagram, WhatsApp, Skype, Viber, app stores), via DNS, TCP/IP or TLS-level filtering—censorship techniques intensified alongside the mobile network outages.
- As mobile networks went dark, traffic on fixed-line networks sometimes increased (or was less impacted), suggesting some traffic was diverted or shifted to wired connections where possible.

Strategic Positioning & Impacts

The 2022 shutdowns reflect a more calibrated, lower-risk censorship posture compared to

2019's brute-force blackout. Rather than sever the entire country's global connectivity, authorities selectively targeted mobile networks during protest hours, which are more critical for real-time coordination and mobilization. This allowed the regime to maintain some connectivity (especially for domestic services), reducing the economic and infrastructural costs of a total blackout.

Yet the mobile "digital curfew" still inflicted serious disruption on protest communication, impairing live reporting, coordination, and information flow from the street. The very regularity of the shutdowns also introduced uncertainty and chilling effects—users would not know in advance exactly when access would be cut.

Institutionally, the 2022 approach appears to build on legal and procedural frameworks developed after 2019: reports suggest provincial security councils and the Ministry of Interior (or the National Security Council) could request intermittent shutdowns, and that some of these orders have become routinized within internal policy mechanisms.

2025 Shutdown: The "Stealth Blackout"

In contrast, the 2025 shutdown marked a sophisticated leap. Instead of withdrawing BGP routes, the government preserved global routing visibility, creating the illusion of normal connectivity for external observers. This "stealth blackout" meant that traditional monitoring tools, which rely on BGP or ping-based data, did not immediately detect the outage, even as domestic users experienced a near-total collapse in international access.

The technical backbone was a centralized system at the national border, enforcing uniform policy across all ISPs. This chokepoint enabled instant and synchronized control, overcoming the fragmented implementation of 2019. Multi-layered censorship mechanisms were deployed:

- **DNS poisoning** redirected blocked domains to government-controlled pages.
- **Protocol whitelisting** restricted traffic to DNS, HTTP, and HTTPS, while blocking VPN, SSH, and peer-to-peer protocols.
- **Deep Packet Inspection (DPI)** inspected encrypted TLS handshakes, resetting connections to forbidden domains.

This layered approach neutralized many circumvention tools without fully halting domestic services. By preserving the NIN and internal applications, economic disruption was minimized, even as citizens were isolated from the outside world.

The 2019 shutdown was high-impact but unsophisticated: a blunt, distributed disconnection that was easy to detect globally but costly for Iran itself. The 2025 model, by contrast, was centralized, rapid, stealthy, and economically aware. Instead of destroying connectivity wholesale, it surgically separated domestic and international spheres.

Strategically, this shift reflects a maturation of Iran's censorship capabilities. The creation of a single chokepoint "kill switch" addressed the inefficiencies of 2019, while multi-layered DPI

targeted circumvention directly. Yet the 2025 blackout also demonstrated the resilience of citizens: reports indicate that covert satellite Internet (e.g., Starlink) provided some external links despite government controls.

Together, the two shutdowns show Iran's progression from brute-force disruption to advanced, stealthy, and sustainable control. The 2019 event exposed the costs of indiscriminate disconnection; the 2025 model exemplifies a new paradigm of centralized, application-aware censorship that other authoritarian regimes may emulate.

We compare the 2019, 2022, and 2025 shutdowns by looking at the kinds of network service affected (cellular versus fixed line), the duration, mechanisms of enforcement, and sociopolitical context. There are three primary qualities that contrast the 2019, 2022, and 2025 shutdowns. 2022 only involved cellular networks, while 2019 and 2025 included cellular and fixed line. 2019 lasted 6 days, while 2022 and 2025 events were extended over nearly 2 weeks. The context of the shutdowns was similar in 2019 and 2022 with the government ordering shutdowns due to civil society protests. In 2025, the shutdowns were in response to the war with Israel and the reported goal of deterring Israel from cyber warfare.

	November 2019 Shutdown	June 2025 Shutdown
Context	Protests	War
Duration	6 days of international connectivity shutdown	About 2 weeks (5 days of disruptions, 4 days of shutdown, and 4 days of slow recovery)
Scope	Mobile + Fixed-line	Mobile + Fixed-line
NIN	Some connectivity, inconsistent effectiveness	Remained connected
Method	Border Gateway Protocol (BGP) routes disconnected by ISPs and mobile operators	**Multi-layered mechanisms**
Control Model	Decentralized compliance from ISPs	**More centralized**, uniform actions across ISPs
Detectability	Easily detectable by global Internet monitoring systems (e.g, IODA)	**Harder to detect** if relying on BGP or ping-based data

VII. Human Rights Implications

The Internet blackouts, censorship, and surveillance tactics employed by the Iranian government during the war with Israel were not merely technical disruptions. They were a deliberate and systematic form of digital repression that had grave human rights consequences for the Iranian people. These actions directly violated the right to freedom of expression and access to information, as protected under Article 19 of the International Covenant on Civil and Political Rights (ICCPR). The government exploited the wartime environment to escalate long-standing policies of information control, with the ultimate goal of silencing dissent and solidifying a state-controlled Internet ecosystem.

Communications and Information Barriers

The most immediate impact was the creation of a profound communications barrier that endangered lives and amplified public panic. During the war, millions of Iranians were cut off from crucial updates on air raids, emergency services, and basic safety instructions. The widespread disruption of Internet and GPS access meant civilians trying to flee dangerous areas were essentially "driving blind". According to Filterwatch research, the inaccessibility of key services, such as Google Maps, resulted in many people getting lost during city evacuations.

In addition to limiting domestic communication, the shutdown severed connections with the outside world. The inability to receive international calls and the reports of calls being misrouted to automated voices or unknown recipients created immense anxiety and isolated families. As mentioned above, the government also actively prevented people from using secure communication channels by blocking international One-Time Password (OTP) SMS codes. This tactic crippled secure apps and VPNs that rely on these codes, effectively locking users out of platforms like WhatsApp, Signal, and Gmail at a time of critical need.

From Digital Repression to Physical Persecution

The digital crackdown was closely tied to a surge in physical persecution. The government used the climate of fear to intensify surveillance and crack down on perceived threats. The fact

that incoming international calls were rerouted to imposter voices or systems suggests security agencies were intercepting calls and attempting to spoof responses. This surveillance was a key part of the government's strategy.

The crackdown on digital communications was not just about control, it was a means of identifying and repressing dissent. The number of individuals executed on charges of spying for Israel reached six since the beginning of the war, including three Kurdish men. In some cases, WhatsApp messages were cited as evidence. This spy-hunting rhetoric was a form of psychological operations aimed at creating fear and justifying the government's actions.

Hundreds of individuals—including social media users, journalists, human rights defenders, foreign nationals - particularly Afghans, and members of ethnic and religious minorities such as Baha'is, Kurds, Balouchis, and Ahwazi Arabs—were detained on accusations of 'collaboration' or 'espionage.' UN Experts noted a surge in executions, arbitrary detentions, and online censorship following the war, urging Iranian authorities to protect individuals instead of persecuting them for exercising their rights.

Disproportionate Impact on Marginalized Communities

Analysis of Filterwatch investigative research and intake data from the Miaan's Digital Security Help Desk reveals a pattern of digital repression by the government that disproportionately harmed marginalized communities, such as journalists and ethnic and religious minorities.

- **Journalists:** Authorities intensified pressure on journalists working for foreign media, such as Iran International, BBC, and Manoto. Family members of these journalists inside Iran were threatened, summoned, and subjected to psychological pressure to force them to stop their activities abroad. In August, UN experts condemned these escalating threats, warning that they violate the rights to freedom of expression and media freedom.
- **Baha'is and other minorities:** The Internet shutdown, enacted during the war with Israel, intensified the systemic persecution of religious minorities, most notably the Baha'i community. Due to the location of one of their holiest sites in Israel, the wartime context was exploited to subject members of the Baha'i faith to an increased number of security threats, including arrests, detentions, and official summons. This demonstrates how the

digital blackout was strategically interwoven with intensified physical and legal repression against vulnerable groups.

- **Afghans:** Following the war, there was a surge of anti-Afghan sentiment promoted by government-affiliated media outlets online. This rhetoric accused Afghan immigrants of collaborating with Israel, calling for their expulsion and even execution. The resulting forced returns of Afghan nationals escalated dramatically, targeting not only undocumented people but also those with valid residency documentation.

Advancement of Digital Authoritarianism

The war with Israel provided the Iranian government with a pretext to advance its long-held goal of nationalizing the Internet. With foreign social apps blocked, officials and state media aggressively pushed citizens to migrate to government-approved domestic platforms like Rubika and SoroushPlus. This forced shift was a major victory for the government, despite the domestic services' inability to handle the sudden increase in traffic.

The government also attempted to codify its repressive tactics into law. A draft bill criminalizing the spread of "false or misleading information" and another bill criminalizing the use of services like Starlink with the potential for the death penalty signal a move to formalize a legal framework for digital control. Perhaps the most lasting legacy of the war is the institutionalization of a "tiered Internet" model, which rewards loyalty with uncensored access while the majority remains under surveillance and censorship.

This escalation of digital repression highlights the urgent need for tools and support that enable Iranians to bypass censorship, protect their privacy, and access a free and open Internet. This is not just a matter of technical access, but a critical component of human rights advocacy and a vital safeguard against the government’s increasingly sophisticated methods of digital authoritarianism.

VIII. Conclusion

The June 2025 Internet shutdown and disruptions in Iran represents a critical turning point in the evolution of digital authoritarianism. Unlike the brute-force disconnection tactics observed in 2019, this event showcased a highly sophisticated "stealth blackout" strategy. The Iranian regime meticulously engineered a system that severed its population's connection to the global Internet while maintaining an outward appearance of connectivity that was not as immediately visible to international internet monitoring platforms, thereby complicating external monitoring and immediate detection. This layered censorship effectively neutralized many circumvention tools by aggressively throttling data traffic. It also leveraged the public's need for communication and information during the war to coerce the population into using Iran's domestic platforms and apps.

Several VPN developers observed that before the shutdown, users could connect to VPN servers, but data flow was significantly reduced. This suggests that authorities might be aggressively throttling or undermining connectivity, rather than completely blocking VPN connections. At the same time, multi-protocol VPNs and proxyless circumvention strategies have demonstrated the ability to maintain connectivity for a significant number of users, at least during the throttling period. These useful insights are a testament to how internet freedom technologies have advanced over the years and how diversity in circumvention strategies is crucial to countering authoritarian regimes' fast-evolving information control tactics.

Digital repression during the war had profound and lasting human rights implications; in Iran's case, it directly endangered lives by blocking essential international services like WhatsApp and Google Maps. This digital crackdown was intertwined with increased physical persecution, detentions, and executions, with digital communications even used as evidence. These discriminatory policies disproportionately affected marginalized and vulnerable groups, including journalists and minorities.

In conclusion, the June 2025 Internet shutdown offers a stark case study in the advanced capabilities of digital authoritarianism. It highlights the urgent need for robust international policy and technological countermeasures to safeguard freedom of expression and access to

information. The strategic and technical differences from previous shutdowns emphasize the critical importance of continued investment in resilient circumvention tools as a vital component of foreign policy in the face of increasingly sophisticated methods of digital control.