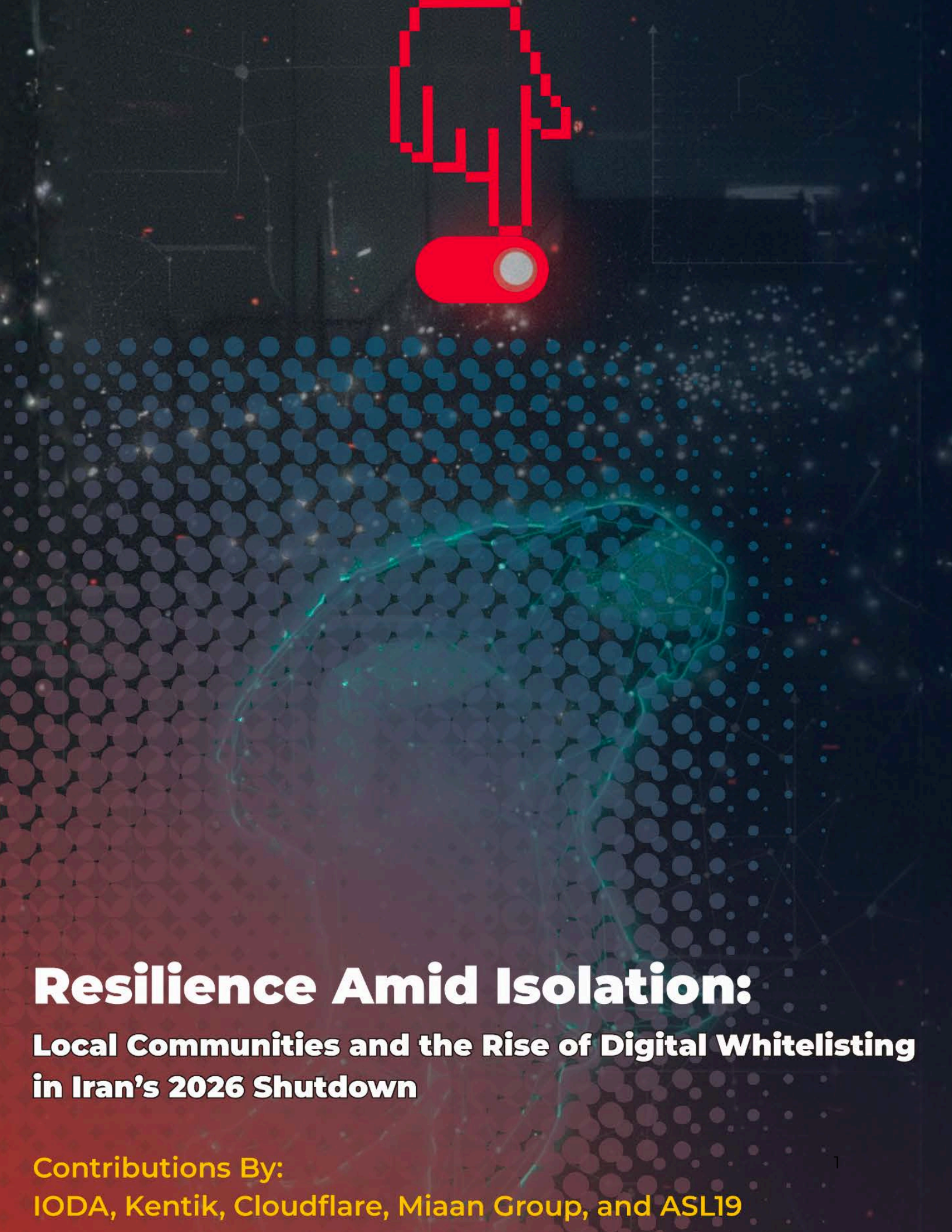


Resilience Amid Isolation:

Local Communities and the Rise of Digital Whitelisting in Iran's 2026 Shutdown

Contributions By:
IODA, Kentik, Cloudflare, Miaan Group, and ASL19

1. Executive Summary

The January 2026 internet shutdown in Iran marks a milestone in the state's doctrine of digital authoritarianism. Moving beyond the reactive, temporary measures of the past, Iranian authorities are operationalizing an architecture of digital isolation designed to transform the global internet from a public right into a state-granted privilege. This report, supported by internet measurement data from IODA, Kentik, and Cloudflare, details the four-phase engineering of this shutdown, the state's transition toward a whitelisting system, and the resilient local "Helper Community" that has emerged to challenge it. The following technical and policy developments illustrate the unprecedented scale and sophistication of this operation:

Technical Evidence of the Shutdown

- **Network Protocol Sabotage**: Prior to the nationwide blackout, authorities withdrew over 98% of IPv6 routes, forcing traffic onto older, more easily monitored infrastructure to maximize surveillance and filtering efficiency.
- **Total Severance**: At the peak of the blackout, international connectivity vanished, and domestic device responsiveness dropped to a baseline of just 3%, indicating a prioritization of absolute containment over all domestic economic and administrative functionality.
- **Verification of Whitelisting**: The state's transition toward a whitelisting architecture was technically confirmed when essential global services, such as specific search engines, were selectively restored while the broader internet remained blocked.
- **Asymmetric Restoration**: Since the more steady network re-establishment on January 27, traffic has remained roughly 40% below pre-shutdown levels. This indicates that while the infrastructure backbone is functional, a permanent "blocked-by-default" system continues to restrict access for the general population.

A New Doctrine of Information Control

- **The Dual-Tier Whitelisting Model:** Following a period of near-total isolation the state transitioned to a "blocked-by-default" architecture. This model is the culmination of a longer term roadmap designed to institutionalize tiered access. It functions through two distinct layers: a service-level tier for selective restoration of approved tools, and a user-level tier for an elite "digital aristocracy." By utilizing pre-existing whitelisting protocols and "white SIM cards" established long before the crisis, the regime ensured its own

communications remained resilient while the rest of the nation was plunged into darkness.

- **Segmented Access & Digital Stratification**: The internet has been redefined from a public right into a tiered privilege. By requiring physical verification and ideological alignment for global access, the state has institutionalized a "class-based internet". This model ensures that while the general population is isolated, a parallel infrastructure remains available to those who amplify regime narratives.
- **Institutional Militarization:** The replacement of civilian telecom leadership with figures from the defense sector indicates that digital infrastructure is now managed as a strategic asset. This shift ensures that network disruptions are executed as coordinated operations, prioritizing state security and narrative dominance over universal access.
- **Calculated Policy Evolution:** The transition from a total blackout to a "blocked-by-default" whitelist indicates a strategic recalibration by the state. This shift can be seen as a response to compounding pressures, including unprecedented domestic social and political unrest, intensifying international diplomatic condemnation, and a critical economic "resilience threshold." By selectively reopening specific digital pathways, authorities aim to mitigate devastating economic losses—estimated at 5 trillion Tomans daily—and manage the country's international image without surrendering fundamental gatekeeping authority over the flow of information.

Resilience Amid Isolation: The Helper Community

Despite these restrictions, the blackout revealed a powerful domestic counter-force. During the January shutdown, decentralized "Helper Communities" successfully utilized in-country Starlink terminals to provide connectivity to thousands and leveraged operational domestic digital infrastructure to support peer-to-peer messaging for hundreds of thousands to potentially millions of users. These volunteer-led efforts have proven to be a vital lifeline and a resilient alternative to surveillance-heavy domestic platforms.

Strategic Recommendations

- **Establish Resilient Digital Infrastructure**: Support the deployment of server and exit nodes inside the country that can mask traffic to blend in with whitelisted data.
- **Support Satellite and Decentralized Connectivity**: Provide configuration resources for secure satellite internet deployment and peer-to-peer distribution channels.

- **Strengthen Local Capacity**: Equip the Helper Community with rapid-response education and verified tool recommendations to counter state-sanctioned misinformation.

2. Introduction & Context

Following the onset of anti-government protests on December 28, 2025, Iranians experienced widespread and escalating disruptions to Internet connectivity. Initially, these disruptions utilized various forms of throttling and localized disruptions, allowing the Iranian government to largely frustrate communication without technically shutting the Internet down. During this period, Iran's domestic network of websites and services, the National Information Network (NIN), remained largely operational.

This approach shifted dramatically on January 8, 2026, when protests expanded sharply in size, intensity, and geographic reach. Iranian authorities responded with arguably the most comprehensive and total shutdown of the Internet and other communication tools in history. Beyond shutting down international traffic, authorities also shut down the NIN, privileged (unrestricted) sim cards, mobile phones, and even landline telephones.

This total blackout marked a fundamental turning point in the state's doctrine of control. By dismantling even the domestic infrastructure it had spent over a decade building, the government prioritized absolute information containment over economic and administrative functionality. However, as the total blackout proved unsustainable due to mounting economic costs, the state transitioned into a new, permanent phase of digital isolation. Instead of a full restoration, authorities implemented a sophisticated whitelisting architecture that transformed global connectivity into a state-granted privilege, creating a tiered system designed to keep the broader population permanently disconnected from the global web.

Yet, this unprecedented attempt at isolation was met with an equally unprecedented response. While the Iranian government has implemented its most sophisticated whitelist infrastructure to date to enforce digital isolation, the January 2026 blackout revealed a critical counter-force: a domestic Helper Community that leveraged years of capacity building to maintain the country's last tenuous links to the global web. This report details both the state's engineering of this blackout and the resilient community efforts that emerged to challenge it.

3. The Technical Breakdown

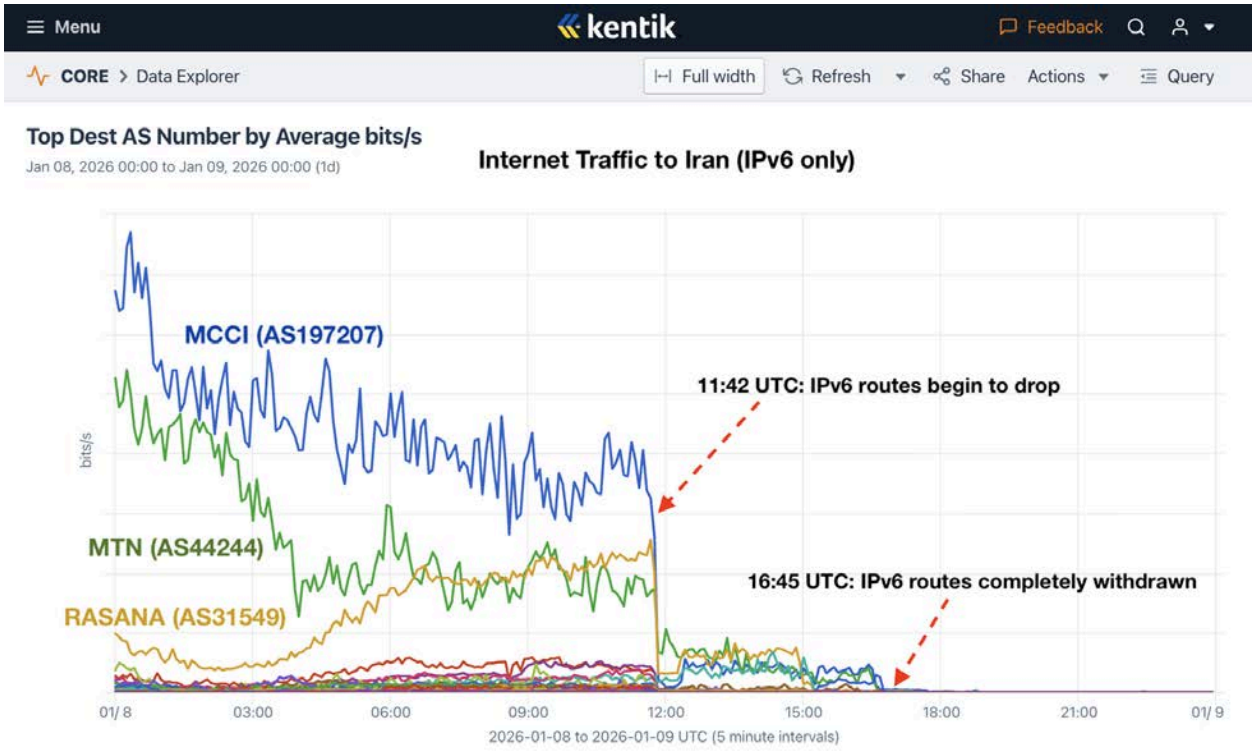
The technical analysis provided by Kentik, Cloudflare Radar, and IODA confirms that the January 2026 shutdown was a sophisticated, multi-phase operation. By weaving their data together, we can see a clear transition from protocol-level sabotage to a total blackout, and finally to a sophisticated whitelisting model of access. The following is a narrative analysis of these four distinct phases.

Phase 1: Preparatory Network Degradation (January 8)

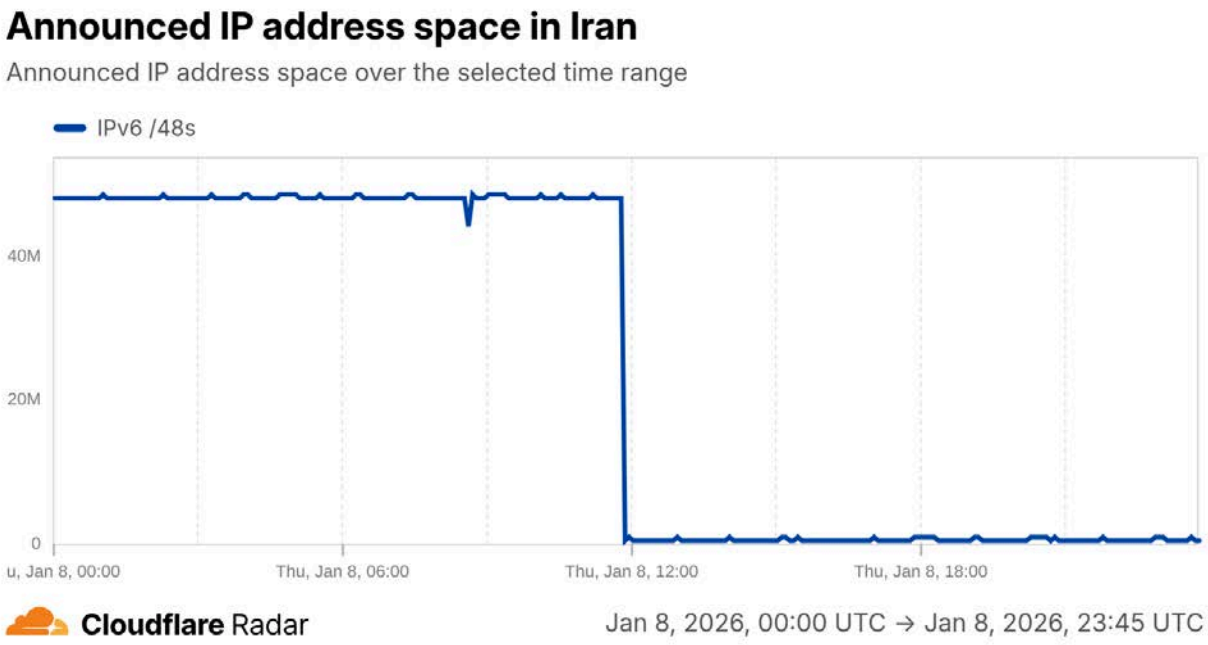
The first indicator of a shifting strategy appeared nearly seven hours before the total shutdown. At 11:42 UTC (15:12 local time), technical data from Kentik showed a significant drop in IPv6 routes, followed by a 98.5% withdrawal of Iranian IPv6 address space at 11:50 UTC. This strategic "pruning" reduced IPv6's share of human-generated traffic from 12% to 2% as confirmed by Cloudflare Radar.

A drop in announced IP address space (whether IPv6 or IPv4) means that the announcing networks are no longer telling the world how to reach those addresses. A major drop like this signaled an intentional disruption to Internet connectivity, as there is no longer a path to the clients or servers using those IP addresses.

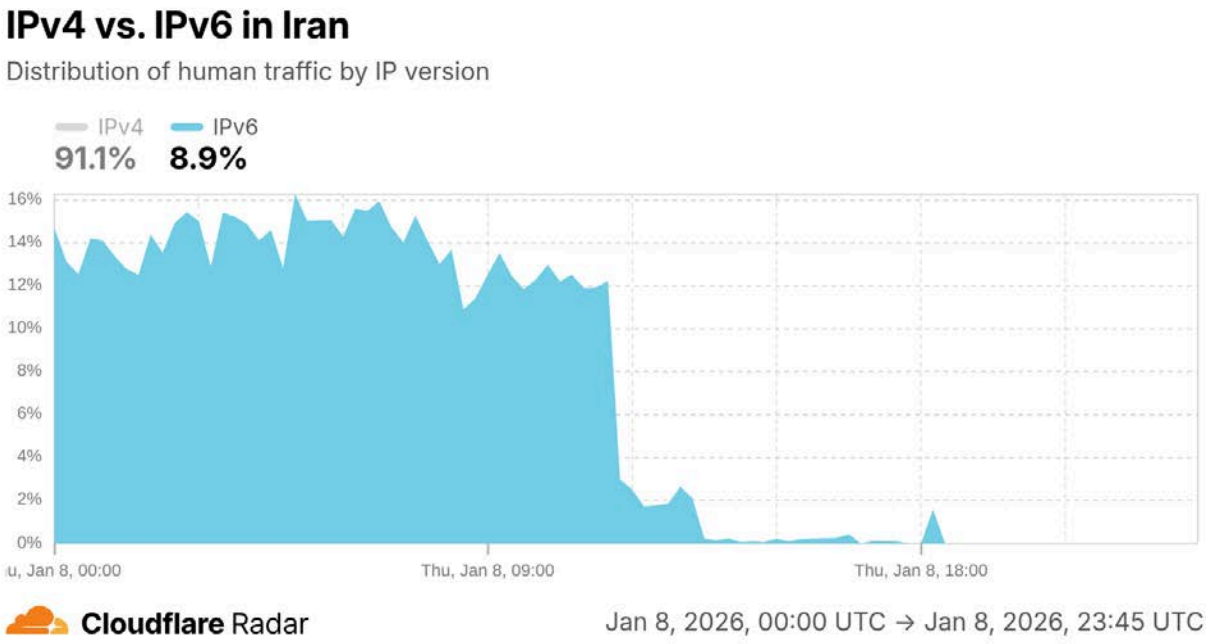
By specifically targeting IPv6—which is more difficult for existing Deep Packet Inspection (DPI) tools to monitor—the state effectively "herded" traffic onto older IPv4 infrastructure. This was a calculated move to ensure that their surveillance and filtering systems could function with maximum efficiency before the final "kill switch" was applied. Had these routes been withdrawn entirely from the start, the state would have lost the technical "plumbing" needed to later implement surgical whitelisting.



This Kentik graph shows IPv6 traffic began to drop at 11:42 UTC on January 8th as Iran's IPv6 routes were withdrawn from the global routing table. Many of these routes lingered with very low propagation for another five hours before disappearing completely as the main Internet shutdown began at 16:45 UTC.



This drop in announced IPv6 address space served to reduce IPv6's share of human-generated traffic from around 12% to around 2%.



As this Cloudflare Radar graph shows, the drop in announced IPv6 address space served to reduce IPv6's share of human-generated traffic from around 12% to around 2%.

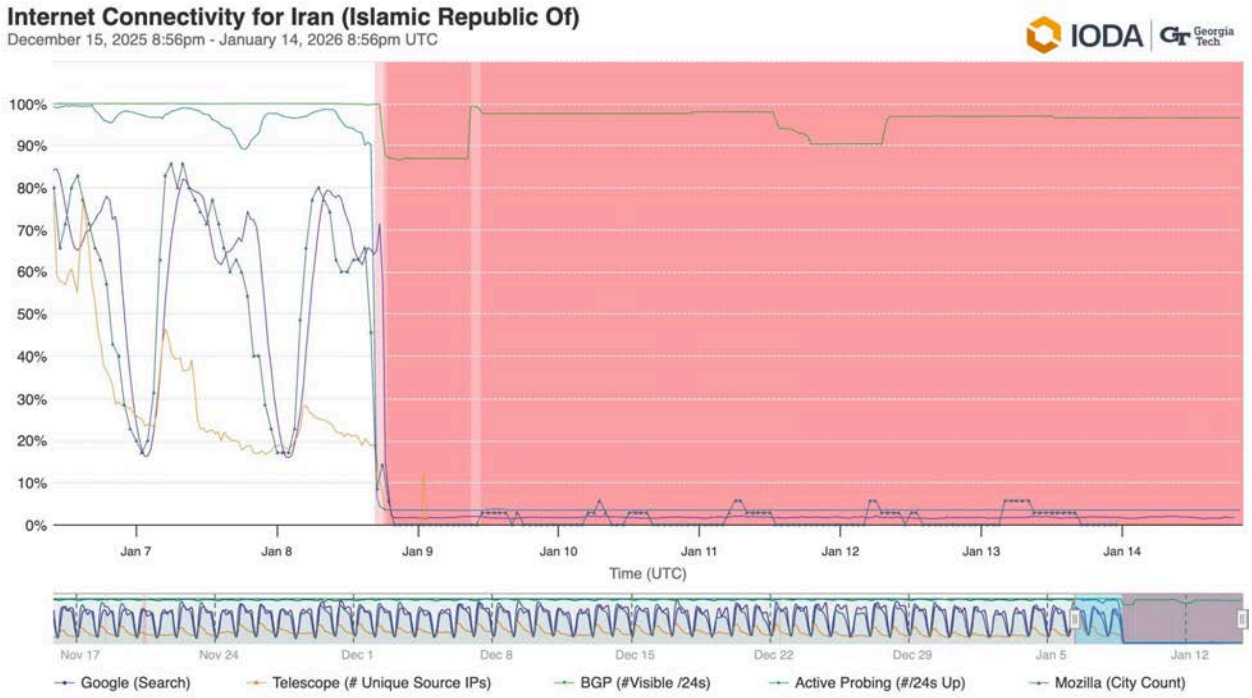
Phase 2: Near-Complete Nationwide Blackout (January 8-17)

On the evening of January 8, synchronized data confirmed that Iran entered its most severe and comprehensive communications blackout to date. Unlike previous disruptions, this phase represented a total severance of both international and domestic connectivity.

IODA: Active Probing and Physical Isolation

IODA's Active Probing signal—which continuously pings devices in millions of networks globally—showed a near-total collapse in responsiveness. While normal connectivity signals vanished on the evening of January 8, probing measurements dropped to a nominal 3%. This baseline likely represents lingering connectivity reserved exclusively for state-sanctioned actors, essential government services, or potentially others with whitelisted access. Outside of very limited whitelisted connectivity, digital human rights groups report severely limited access to the Internet both internationally and domestically. IODA integrates user statistics from Google and Mozilla Firefox, which also show near-zero connectivity.

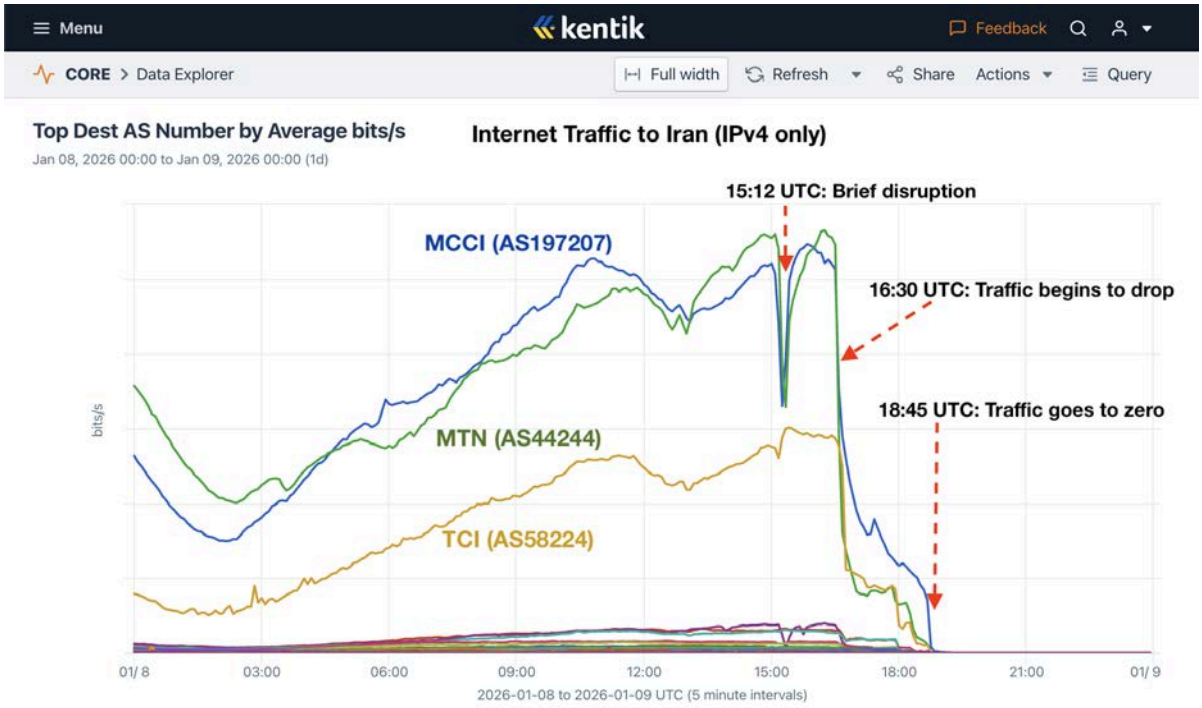
This "flatline" in probing data indicates that devices within Iran were not merely struggling with slow speeds but completely unresponsive to pings from the global web.



IODA measurements show normal connectivity signals and the Internet shutdown starting the evening of January 8th.

Kentik: The Absolute Severance of Traffic

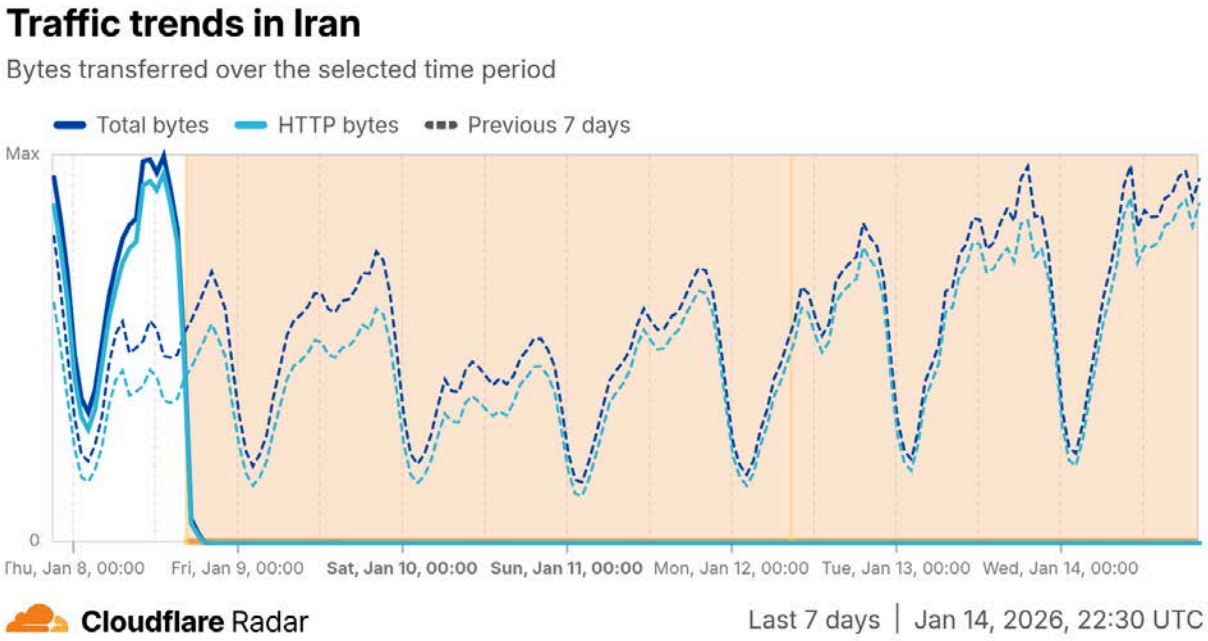
Data from Kentik provided primary evidence for the complete cessation of data flow. Their traffic analytics showed that at 18:45 UTC, total bytes transferred to and from the country plummeted to zero. Kentik's measurement of IPv4 traffic—the primary protocol still in use after the earlier IPv6 withdrawal—confirmed that the country had effectively severed itself from the global internet backbone. This near-zero traffic volume persisted throughout the blackout phase, demonstrating a disciplined and total enforcement of the shutdown.

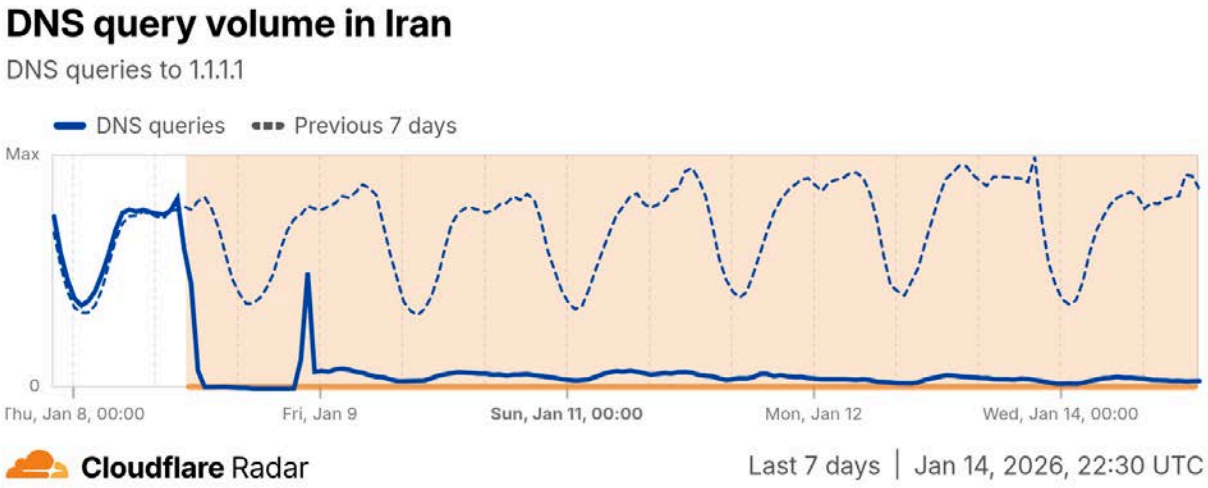

Menu
kentik
Feedback
CORE > Data Explorer
Full width
Refresh
Share
Actions
Query
Top Dest AS Number by Average bits/s
Jan 08, 2026 00:00 to Jan 09, 2026 00:00 (1d)
Internet Traffic to Iran (IPv4 only)
15:12 UTC: Brief disruption
MCCI (AS197207)
16:30 UTC: Traffic begins to drop
18:45 UTC: Traffic goes to zero
MTN (AS44244)
TCI (AS58224)
bits/s
01/ 8
03:00
06:00
09:00
12:00
15:00
18:00
21:00
01/ 9
2026-01-08 to 2026-01-09 UTC (5 minute intervals)


Menu
kentik
Feedback
CORE > Data Explorer
Full width
Refresh
Share
Actions
Query
Top Dest AS Number by Average bits/s
Last 2w
283 of 283 data sources
2 Filters
Internet Traffic to Iran
bits/s
Ongoing internet shutdown
01/ 1
01/ 3
01/ 5
01/ 7
01/ 9
01/11
01/13
01/15
2026-01-01 to 2026-01-15 UTC (60 minute intervals)

Cloudflare Radar: Vanishing Users and DNS Collapse

Cloudflare Radar analytics mirrored these findings, reporting that traffic volumes from Iran were reduced to a fraction of a percent of previous levels. Crucially, Cloudflare also observed the complete disappearance of traffic to its public DNS resolver (1.1.1.1). Because DNS acts as the "phonebook" of the internet, the absence of these queries confirms that users were not even attempting to resolve domain names, as they had lost all underlying network paths. While a negligible amount of DNS traffic became visible again on January 9, it remained at historically low levels, further corroborating the reports of a near-total information vacuum.



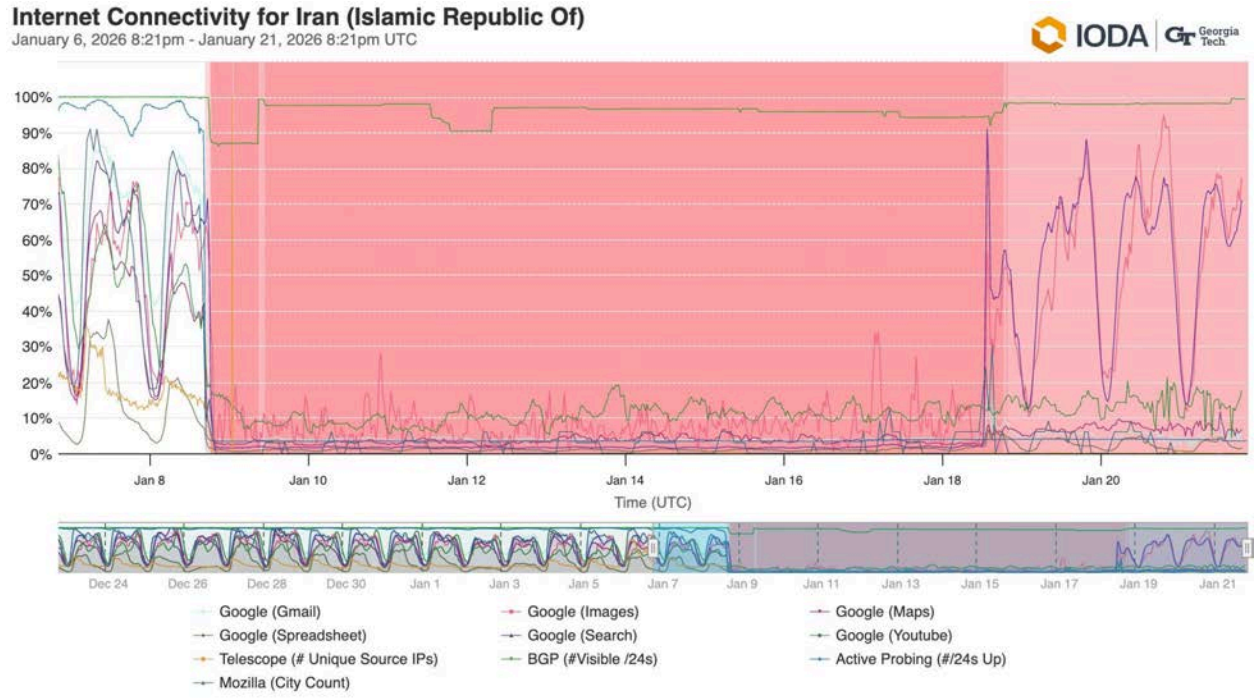


Traffic to 1.1.1.1, Cloudflare's public DNS resolver, from Iran also disappeared as the shutdown began, but a small amount of traffic has remained visible since January 9.

Phase 3: Managed Restoration and Whitelisting (January 18 – January 26)

By mid-January, various measurement groups began observing the first signs of recovery in Iran's network traffic. However, this did not represent a return to the open web. Technical data from IODA shows that while overall infrastructure responsiveness remained at a near-flatline—with the Active Probing signal staying significantly depressed—specific services began to diverge from the blackout.

The most definitive indicator of the state's transition to a whitelisting architecture is visible in the usage statistics for Google Search and Google Images, which flickered back to life on January 18th despite the broader network remaining dark. This indicates that rather than restoring the "pipes" of the internet, authorities were manually "unblocking" specific, pre-approved global services to allow for essential digital functionality while keeping the general population isolated.



User Reports and the Domestic Tiered Return

Beyond the technical measurements, user reports collected by Filterwatch reveal that this recovery followed a highly disciplined, tiered plan. The restoration began as early as January 15 and 16 with the return of domestic SMS services, marking the first step in a sequence previously signaled by state-affiliated media: first SMS, then domestic platforms, and finally international access.

By January 17, the National Information Network (NIN) became the primary gateway for digital life. During this period:

- Domestic Infrastructure: National messaging platforms and business services, such as the e-commerce site Banimode and the super-app Snapp, resumed operations and began sending SMS notifications again.
- Authenticated Access: The restoration of these platforms was notably selective. Initial access was granted to verified channels and government-authenticated accounts, suggesting that the long-discussed "Trusted Identity System" had entered an operational phase.
- Professional Whitelisting: Connectivity was restored to newsrooms and select businesses starting January 16, allowing the state to maintain a facade of normalcy in official sectors while the public remained largely disconnected.

The Divergence in Global Connectivity

Even as Google Search became accessible on mobile operators like MCI and Irancell by the afternoon of January 17, the restoration was inconsistent. Critical communications tools like Gmail and Google Meet remained blocked or experienced significant packet loss. For ordinary users, accessing any part of the international internet required complex technical workarounds, highlighting that for the average citizen, the state's "new normal" was a status of permanent, gated isolation.

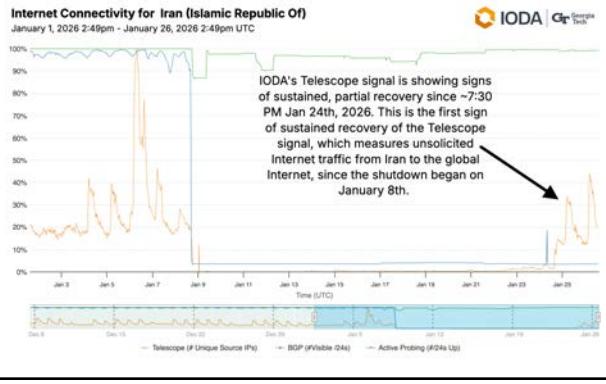
Phase 4: Sustained Restoration of Connectivity and the "New Normal"

The move toward a more consistent re-establishment of the network began tentatively on January 23, with a more definitive shift toward broad connectivity occurring on January 27. During this final phase, measurement groups observed that while the underlying architecture of the internet was largely restored, the actual user experience remained fractured by a permanent whitelisting regime.

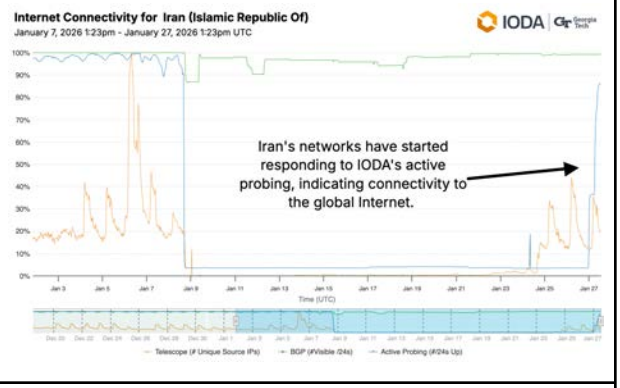
Technical Indicators of Infrastructure Recovery

Data from IODA captured the first significant signs of a structural return to the global web. On January 24th, IODA observed a sustained increase in the Telescope signal, which measures unsolicited internet traffic originating from Iranian devices. This was

the first time since the January 8th shutdown that this "background noise" of the internet was visible, suggesting that devices were once again communicating across the border. This was followed on January 27 by a sharp jump in the Active Probing signal, indicating that networks across the country had resumed responding to global probes at a baseline level. Kentik's traffic measurements corroborated these milestones, showing significant increases in data flow on both January 23rd and 27th.



Recovery of IODA Telescope signal on January 24th.



Recovery of IODA's Active Probing signal on January 27th.

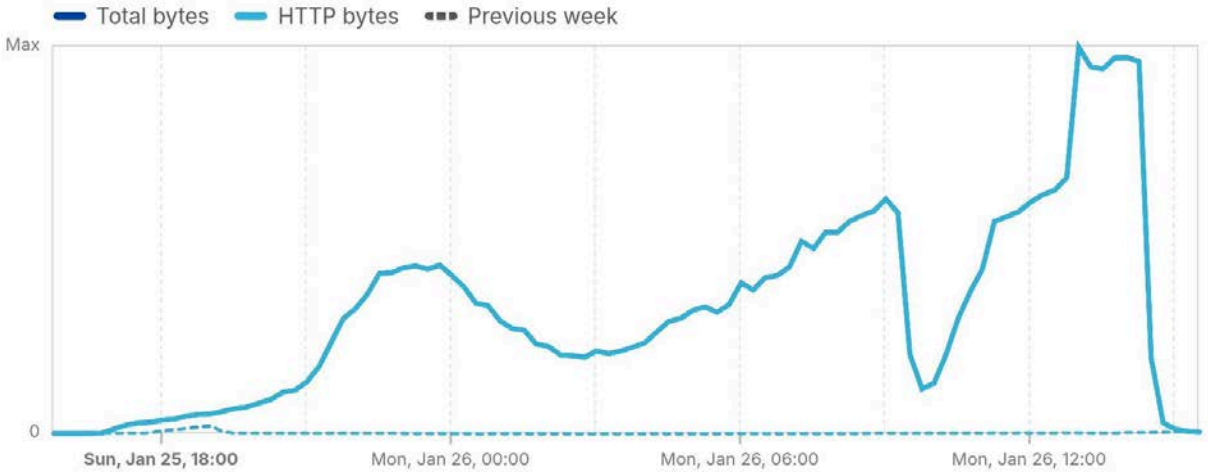
Cloudflare: Connection Volatility and User Reports

Despite these broad signals of systemwide restoration, connectivity remained exceptionally unstable in the days leading up to the January 27 jump. Cloudflare Radar data from January 25 and 26 revealed a highly volatile pattern where traffic was repeatedly restored and then blocked, often several times within a single day.

Reports from users during this period, corroborated by Filterwatch, described a "stalled" and erratic internet experience where connections were short-lived. This erratic behavior suggests that authorities were actively tuning their filtering regime in real-time—periodically opening and closing gateways as they finalized the transition to a permanent "blocked-by-default" architecture.

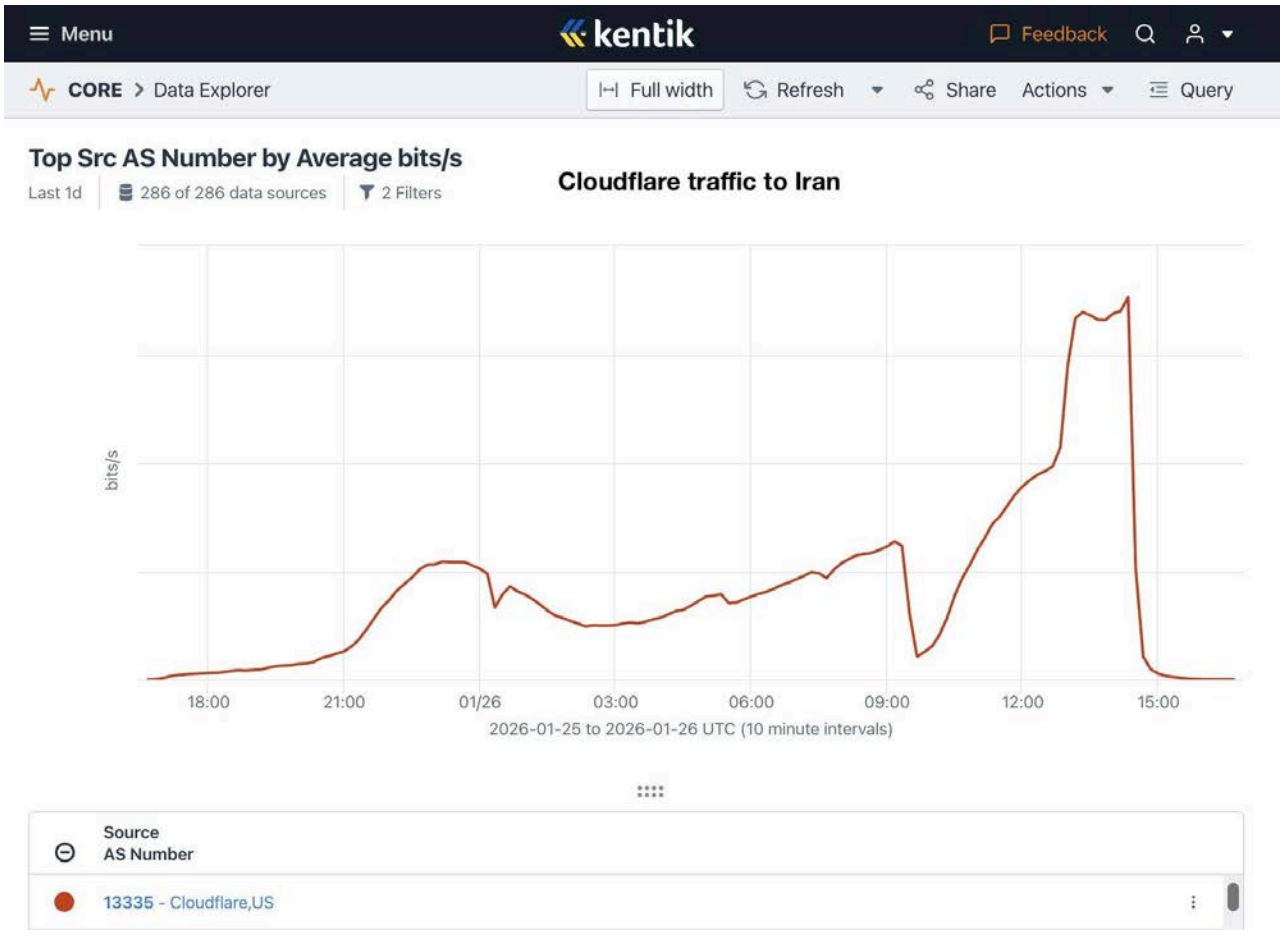
Traffic trends in Iran

Bytes transferred over the selected time period



Cloudflare Radar

Last 24 hours | Jan 26, 2026, 16:45 UTC

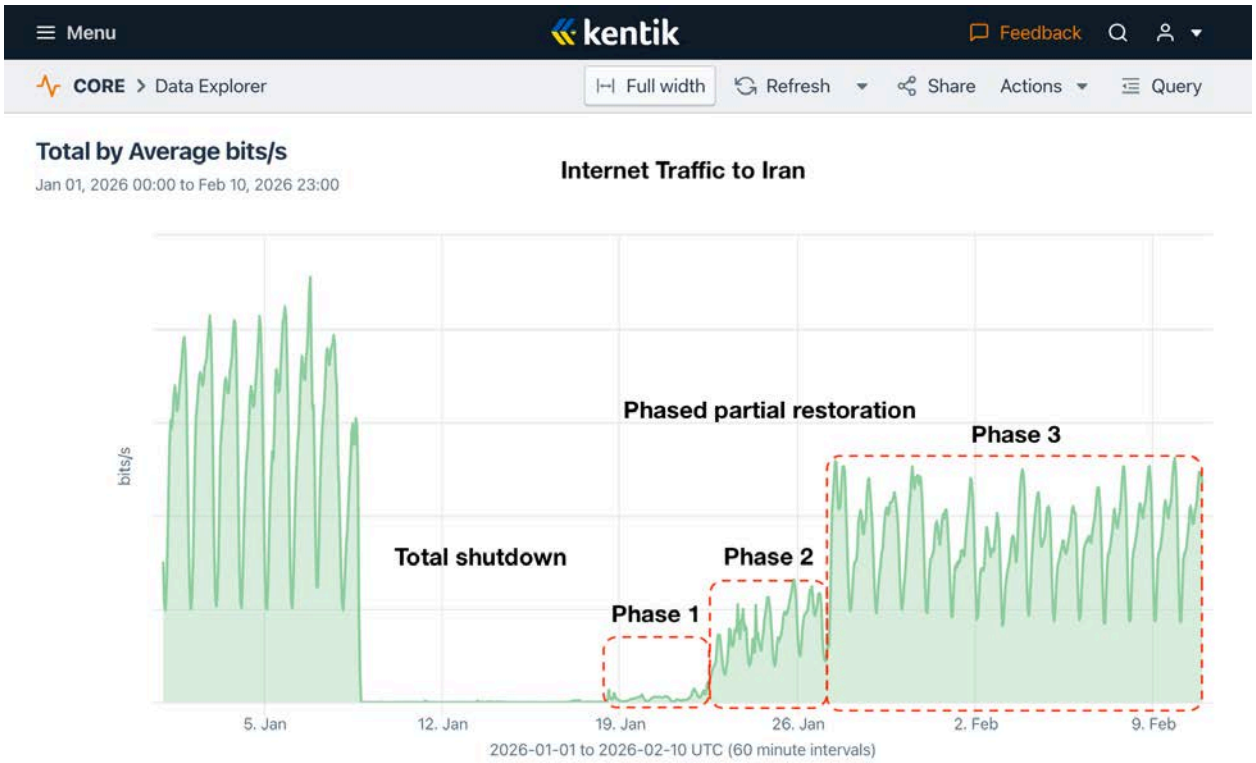


Ongoing Whitelisting and the Traffic Gap

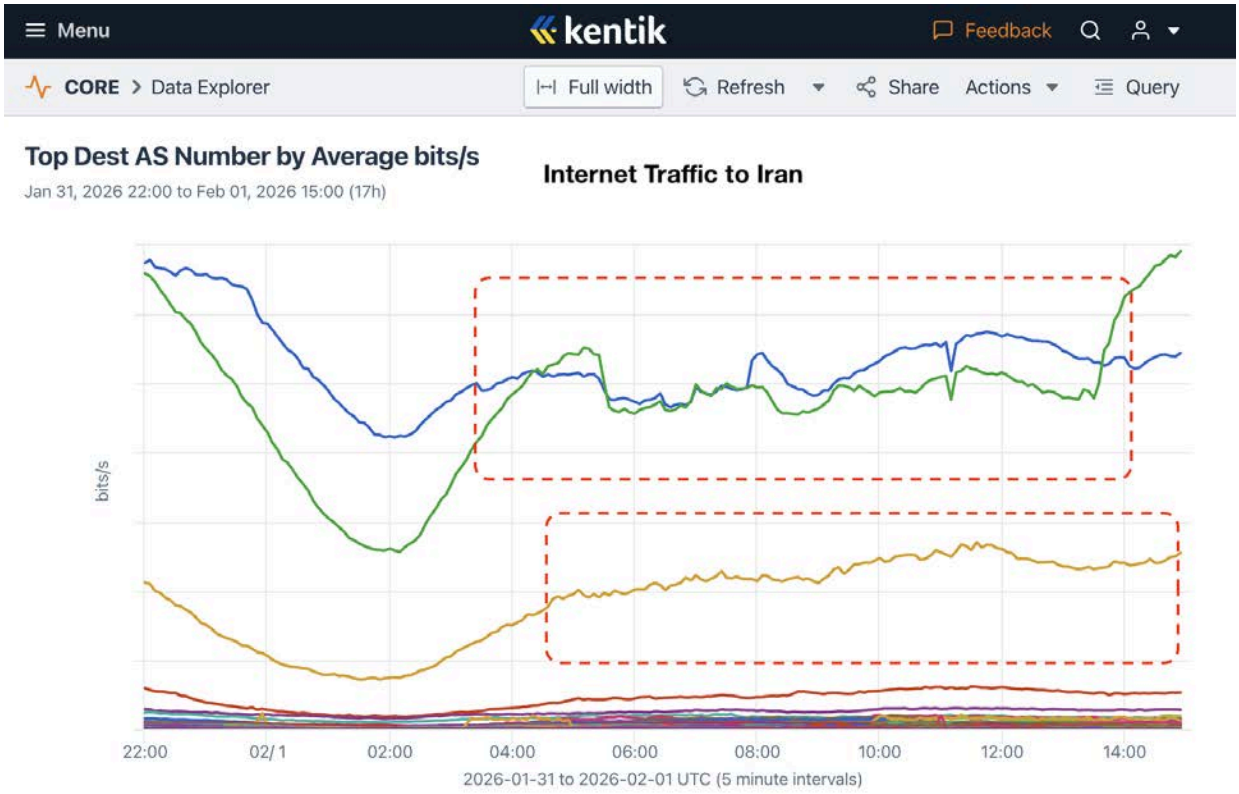
A comparison of traffic levels before the January 8th shutdown and after the early February restoration reveals that the network has not returned to its previous state of access. Technical data indicates that despite the partial restoration, traffic levels remain at only 58.9% of pre-shutdown levels (as of February 12).

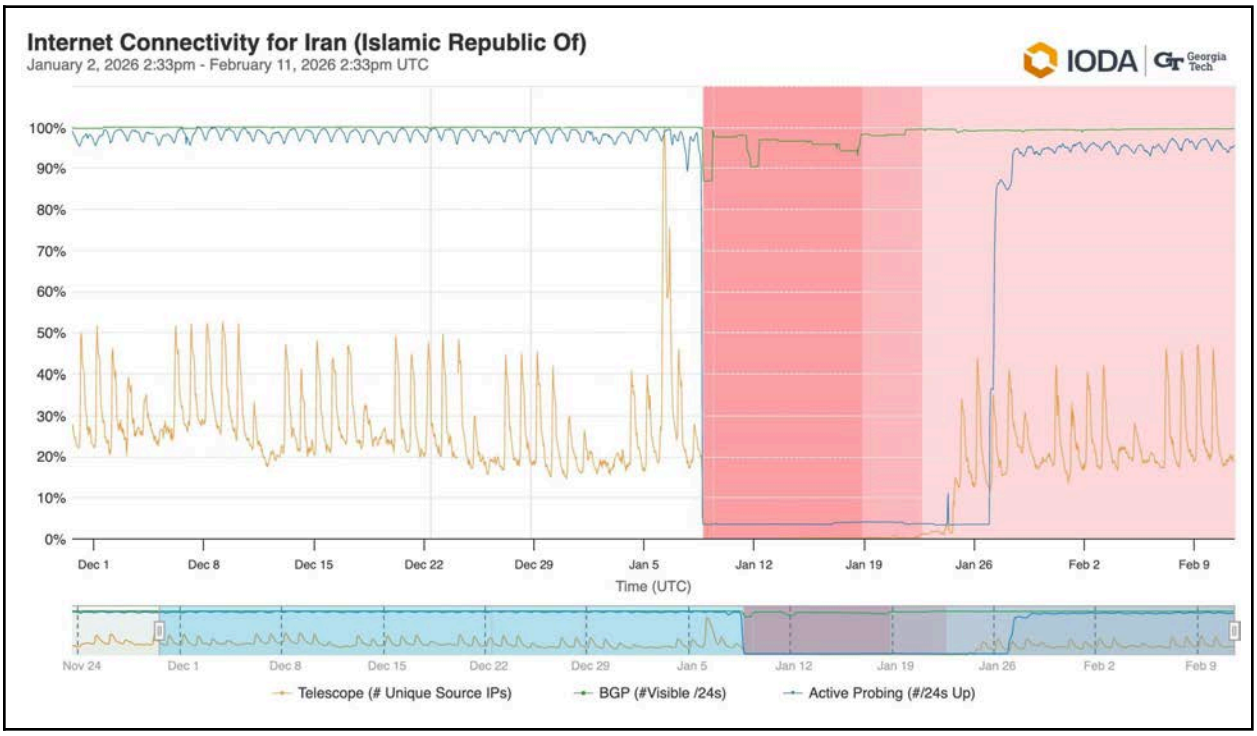
In addition, while usage of services like Gmail, Google Maps, and the Firefox browser eventually stabilized near pre-shutdown levels, YouTube usage continues to show no meaningful return. This persistent gap provides clear technical evidence that the whitelisting regime continues to suppress high-bandwidth global platforms even as the underlying network architecture appears functional.

The following sequence of charts from **IODA, Kentik, and Cloudflare Radar** illustrates these long-term traffic variations, comparing national connectivity levels from the period immediately preceding the January 8th shutdown through the stabilized recovery in mid-February.



As illustrated in the graph below, traffic data from Kentik reveals a higher rate of disruption during peak use hours. Traffic curves appear jagged, indicating connection disruptions, while they are smoother during off-peak hours.

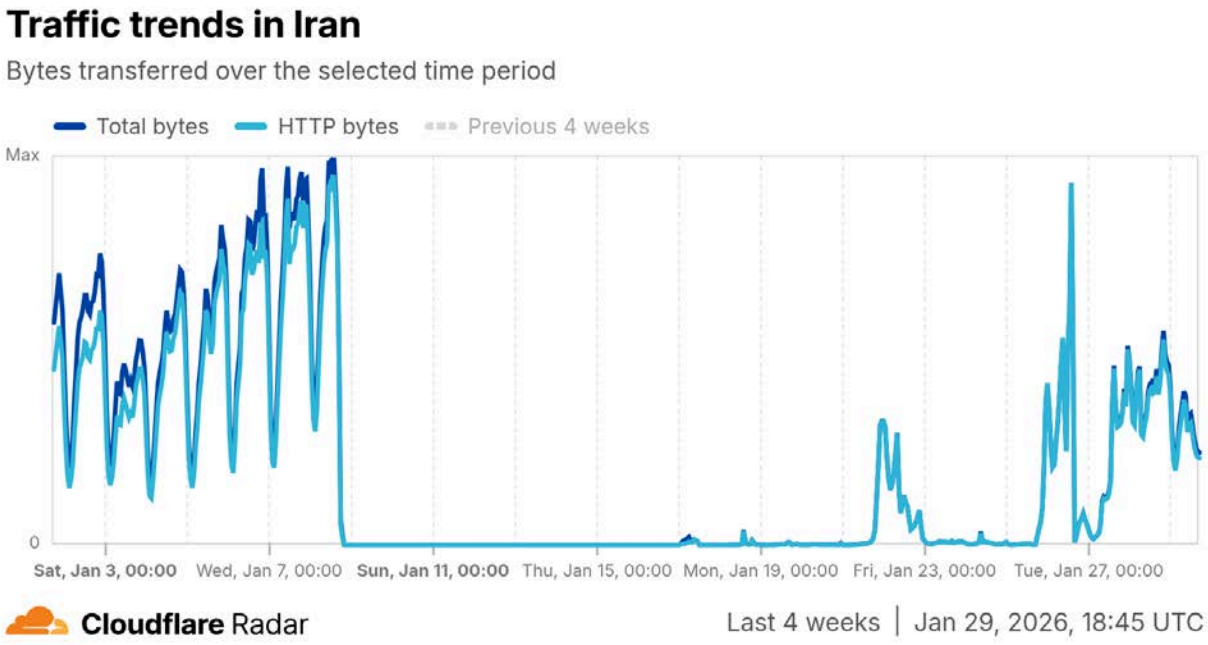

Menu
kentik
Feedback
CORE > Data Explorer
Full width
Refresh
Share
Actions
Query
Top Dest AS Number by Average bits/s
Jan 31, 2026 22:00 to Feb 01, 2026 15:00 (17h)
Internet Traffic to Iran
bits/s
22:00
02/1
02:00
04:00
06:00
08:00
10:00
12:00
14:00
2026-01-31 to 2026-02-01 UTC (5 minute intervals)


Internet Connectivity for Iran (Islamic Republic Of)
January 2, 2026 2:33pm - February 11, 2026 2:33pm UTC
IODA
Georgia Tech
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Dec 1
Dec 8
Dec 15
Dec 22
Dec 29
Jan 5
Jan 12
Jan 19
Jan 26
Feb 2
Feb 9
Time (UTC)
Nov 24
Telescope (# Unique Source IPs)
BGP (#Visible /24s)
Active Probing (#/24s Up)

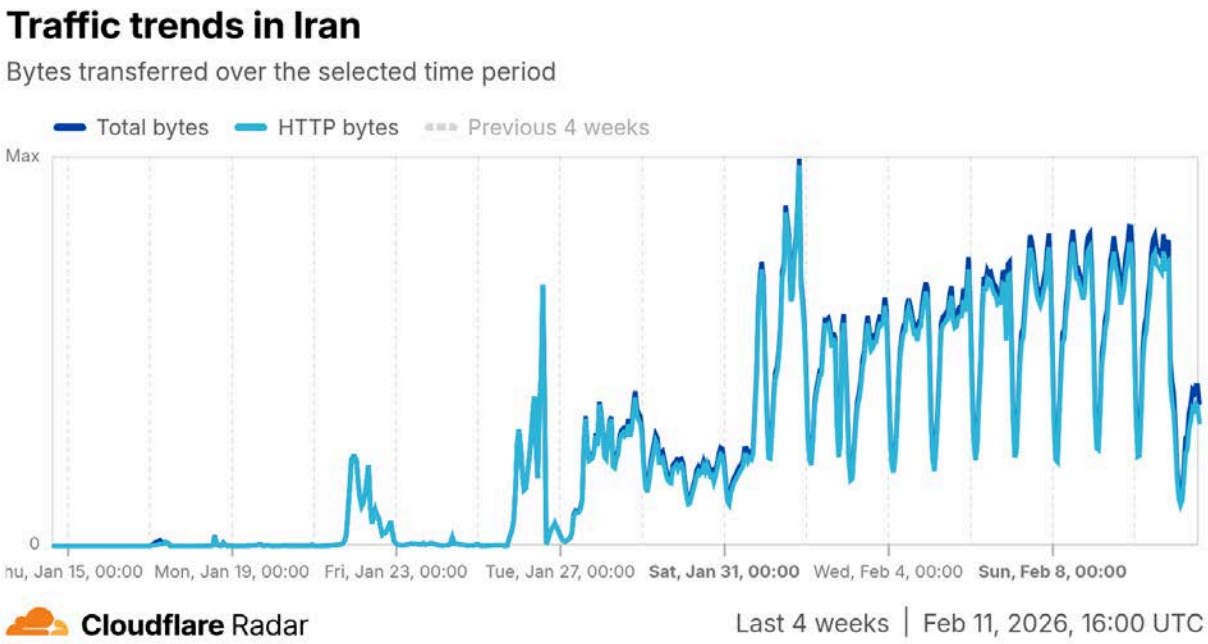
IODA signals show Iran's Internet infrastructure connectivity has nearly returned to pre-shutdown levels, with Active Probing still slightly lower than pre-shutdown levels. While these signals show "normal" levels of Iran's Internet infrastructure connectivity to the global Internet, we know that Iranian Internet users have not experienced a return to pre-shutdown connectivity.

IODA integrates Google Product Usage data (Gmail, Images, Maps, Spreadsheet, Search, YouTube) and

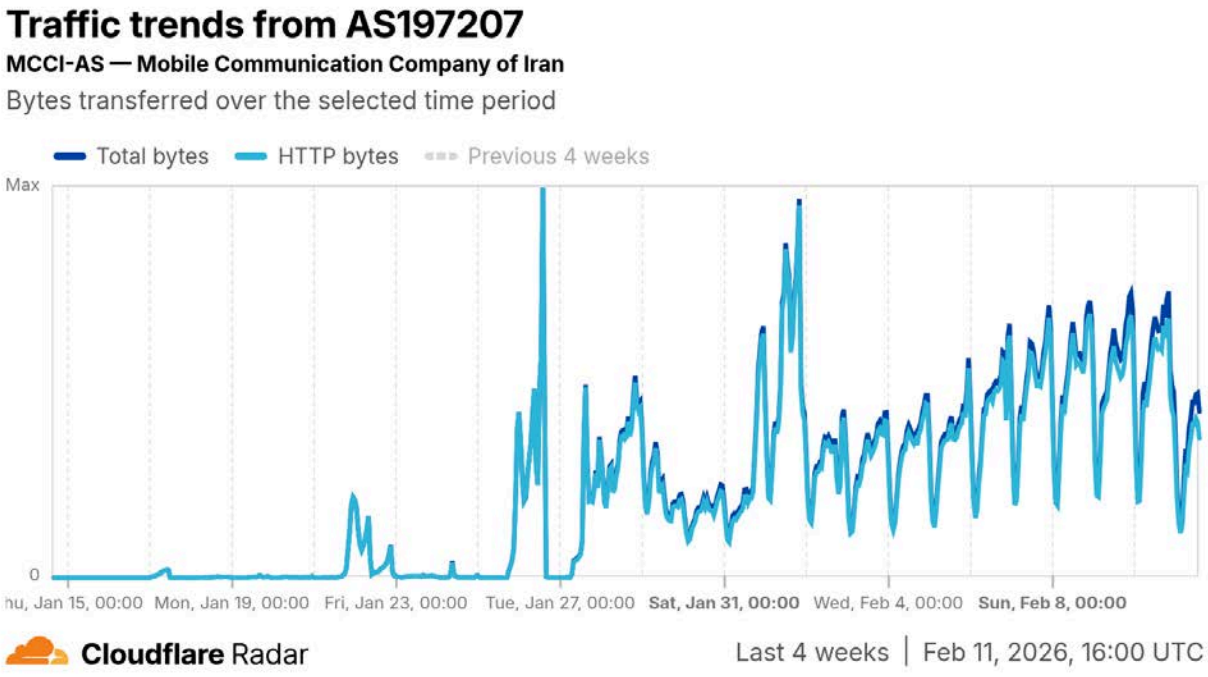
Mozilla Telemetry data from Firefox usage.

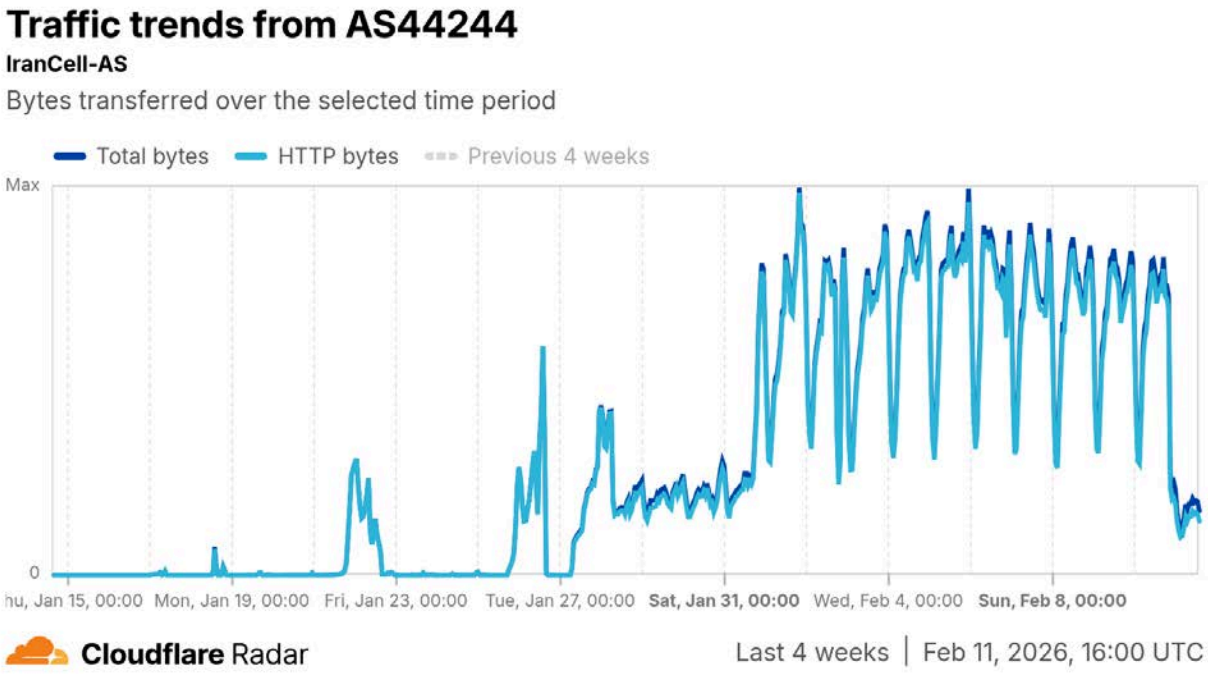


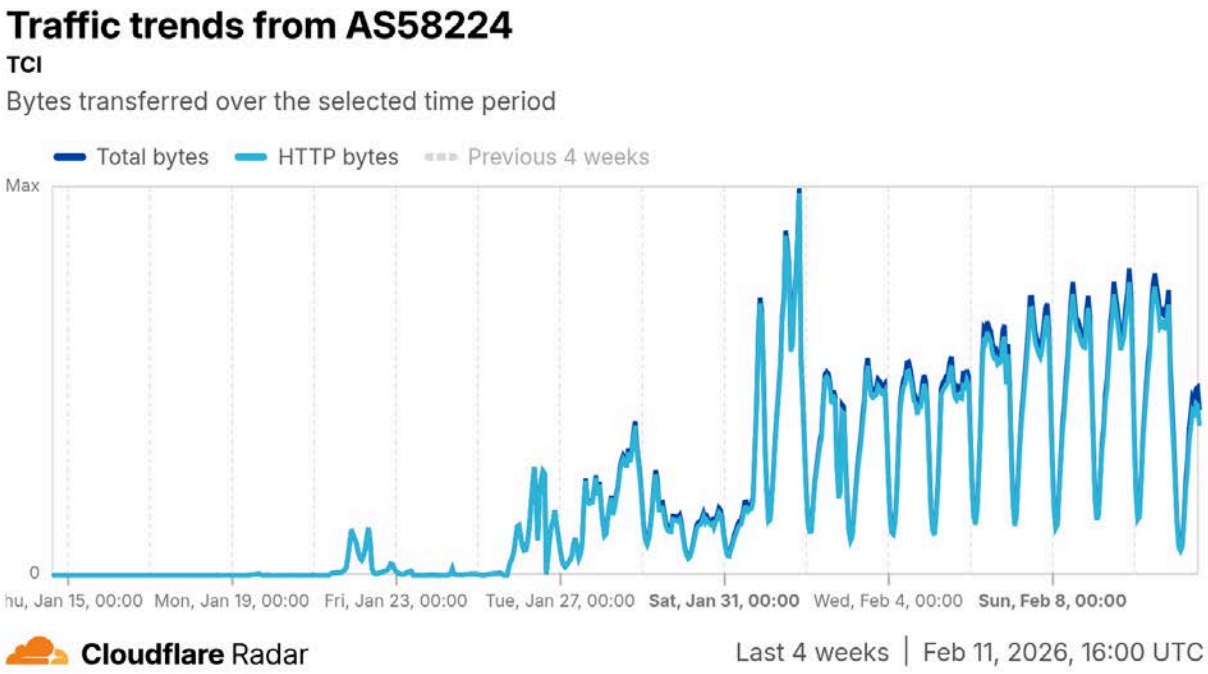
Cloudflare traffic for Iran, contrasting pre-shutdown levels and patterns to recent limited restoration.



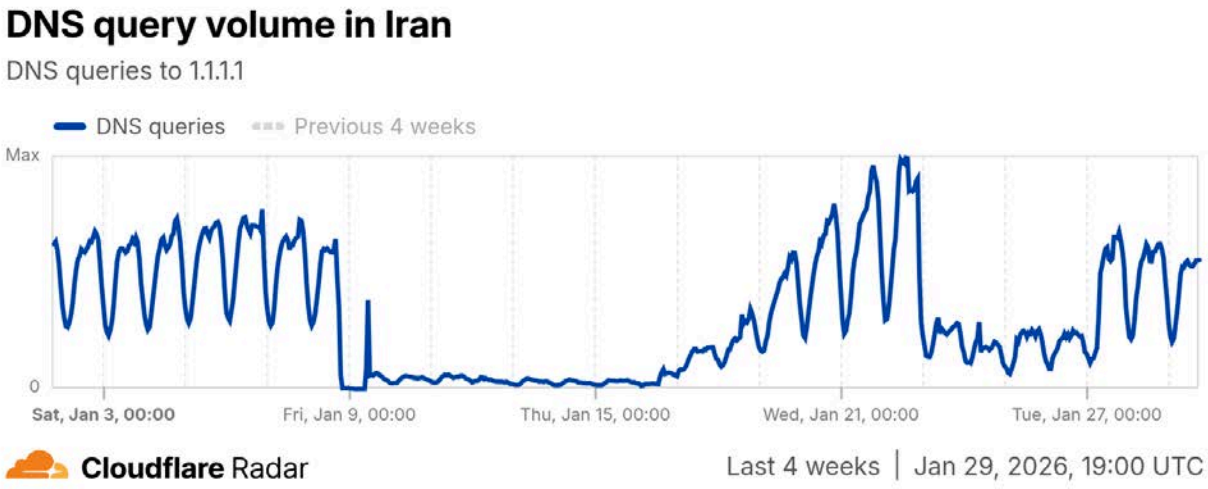
Cloudflare traffic for Iran, January 15-February 11. Brief, limited restoration visible on January 21-22 and again on January 25-26. More sustained restoration begins January 27.



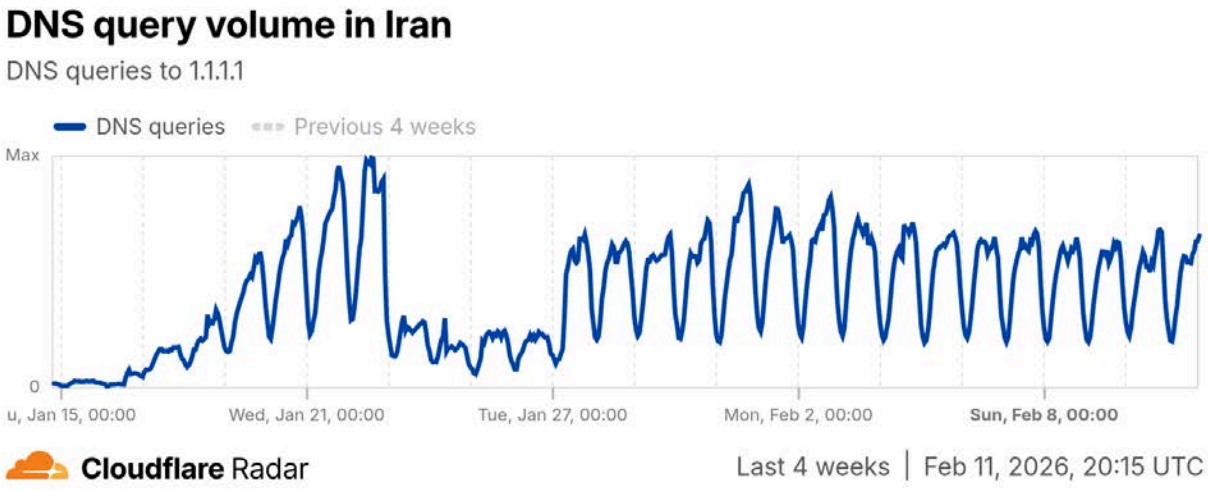




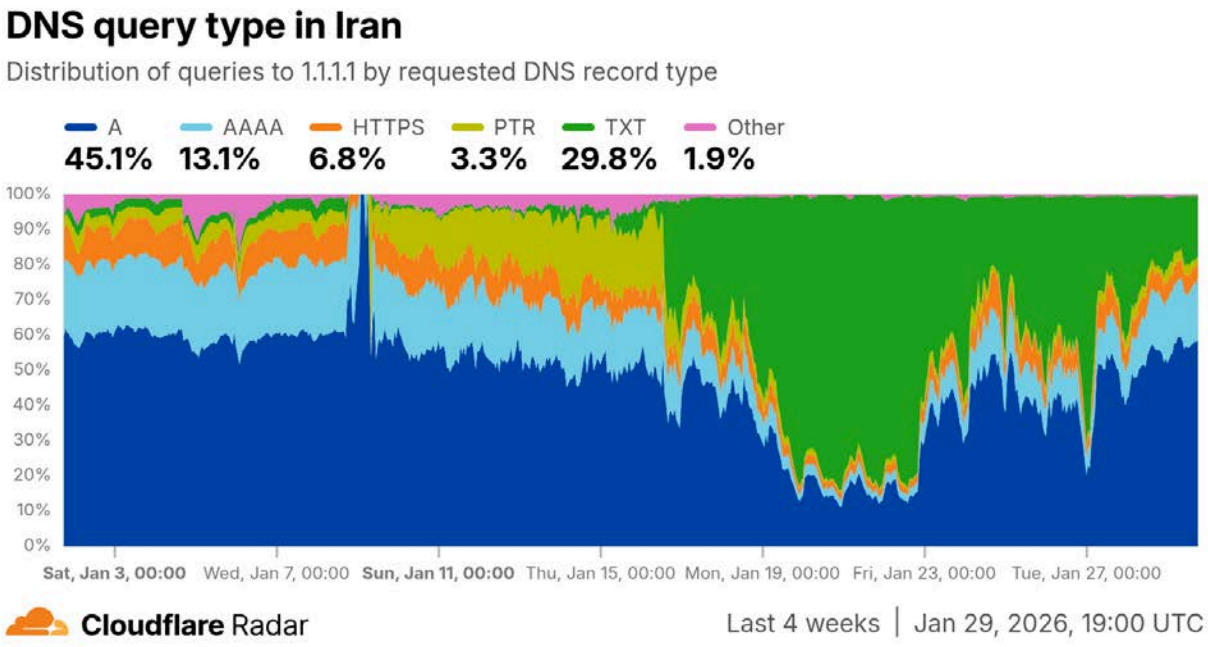
Cloudflare traffic for MCCI, IranCell, and TCI, January 15-February 11. These ASNs were the primary contributors to the traffic restoration visible at a country level.



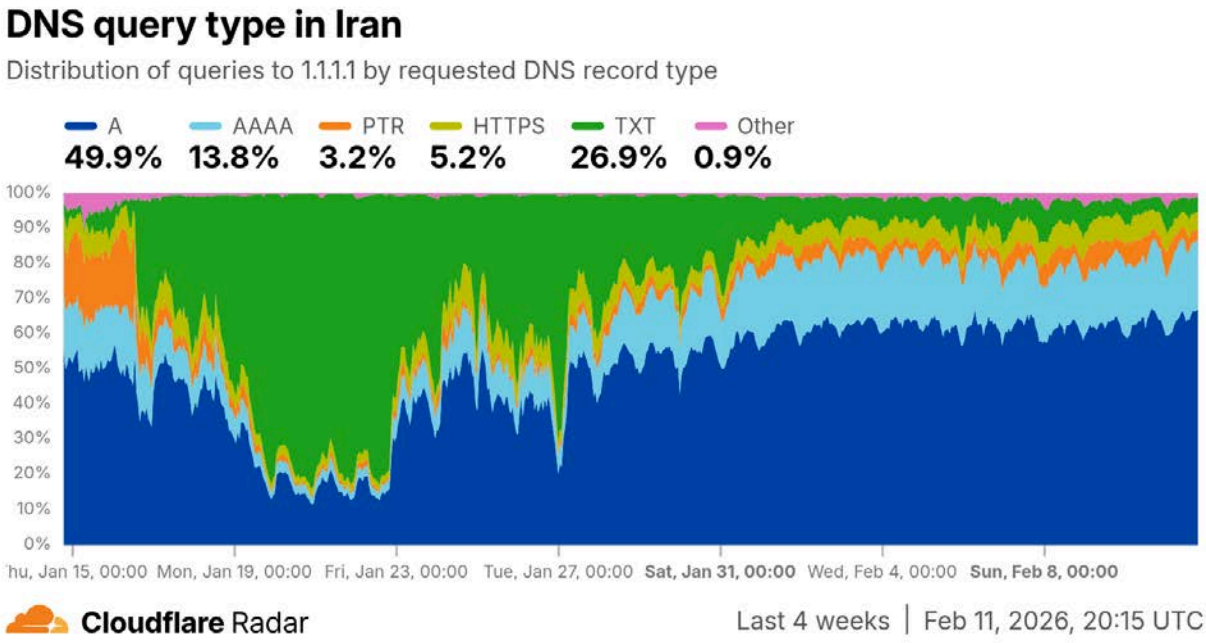
Query volume from Iran to Cloudflare's 1.1.1.1 public DNS resolver, January 1-29.



Query volume from Iran to Cloudflare's 1.1.1.1 public DNS resolver, January 15-February 11.



Distribution of DNS query types for requests from Iran to Cloudflare's 1.1.1.1 public DNS resolver, January 1-29. Note that the share of TXT record requests maps to the growth in query volume that starts on January 16.



Distribution of DNS query types for requests from Iran to Cloudflare's 1.1.1.1 public DNS resolver, January 15-February 11. Note that the share of TXT record requests maps to the growth in query volume that starts on January 16.

4. Social Digital Resilience: Stories and Needs

With the near-total communication blackout, more stories continue to emerge from within Iran about how people have relied on one another to form localized support networks. These networks, or as we call them the "helper community," form a social digital resilience against shutdowns and play a crucial role in distributing censorship circumvention and communication tools when no overseas support was reachable.

These communities of helpers inside the country are not new. In fact, they have long been an integral part of Iran's internet freedom rapid response ecosystem. According to ASL19 and Gazzetta's latest research on in-country response during the June 2025 shutdown, 76% of people reported helping others in some way: from providing hands-on technical assistance in tool setup and configuration to tool recommendations. This translates to millions of technical volunteers and informal helpers on the ground.

In the January internet shutdown, we saw in-country Starlink terminals providing access and connectivity to thousands of people and a more decentralized messaging app that leverages Iran's domestic digital infrastructure (which stayed operational under the blackout) supported hundreds of thousands of users to communicate

within the country. These successes are highly dependent on volunteer helpers on the ground that initiated training, tool installation, file sharing, and server setup. These tools and communication channels have proven to be a lifeline for many and an important alternative to surveillance-filled domestic messaging platforms.

"My family and I were able to install [the tool] for many people."

"With the help of this server, we were able to stay in touch with friends and acquaintances during this time—it was a lifesaver."

"Some people inside the country are trying to create tools suited to the current conditions on the national internet for secure communication with the outside world"

"One of my friends set up a server, and I'm using that."

While most VPNs did not work during the blackout, there were reports that a few protocols and proxy platforms had minor successes. Napsternet proxy configurations were frequently mentioned. People reported that the proxy configurations were shared via diverse communications channels, including VPN clients, Telegram channels, and some even reported seeing configurations being shared in online comments under state-sanctioned news articles. The security status of the proxies, however, was unclear and their effectiveness and performance vary according to user accounts.

Both the June 2025 shutdown and the recent blackout demonstrate a shift needed in how we support shutdown mitigation and preparedness–capacity building for the helper communities inside Iran will have exponential reach and effect in future shutdown resilience.

To effectively scale and offer customized support to their local networks, in-country helper communities require appropriate resources, digital infrastructure, and assistance. Drawing upon feedback from the ground and observations during the two most recent shutdown events, we propose the following key areas of focus:

Scale up alternative resilient digital infrastructure

1. **Preemptively establish in-country network infrastructure:** Many shutdown-resilient tools require nodes that can facilitate decentralized communications when the internet is not available. To scale up the performance and usability of this type of decentralized tools and maintain their security standards, internet freedom practitioners from overseas can help spring up server nodes and exit nodes inside Iran.

2. **Increase network redundancy for better performance and shorter down time:** During aggressive internet disruptions, we often see intensified server blocking that aims to paralyze data transfer across decentralized technologies. This means simply bringing up more servers is not enough; the network requires better “masking” to blend in with whitelisted traffic and the network architecture must be configured with adversaries in mind.

3. **Provide privacy-first configuration support and resources for satellite internet:** Following the blackout, more people inside Iran are using and sharing satellite internet with their neighbours and friends. Internet freedom practitioners from outside of the country can provide necessary resources on secure network setup for satellite internet deployment. This includes providing more obfuscatable satellite uplink and downlink channels, troubleshooting local area network (LAN) connections, configuring security features, and advising on best practices for managing shared network security and user access.

4. **Offer harder-to-block VPN service configurations:** In-country helper communities need a variety of resilient, secure and fast VPN services that could be safely utilized and distributed. Instead of simply providing users with a VPN app, internet freedom tool providers should try to provide proxy tunnel configuration URLs that can be used with third-party client apps to connect users to oversea servers.

5. **Scale up in-country tool distribution:** While help communities often leverage their own existing social network to offer help, we can set up more peer-to-peer tool distribution channels/mesh networking for easier tool sharing. This includes enabling offline data sync, opportunistic transfer, and local caching models that could be especially useful during a blackout.

Strengthen networks and community capacity

1. **Rapid response education:** Through proactive, targeted education programs, we can equip the Helper Community with the essential tools and skills to help more Iranians in moments where they have to rely on each other. The program could include tailored tutorials on topics such as security best practices, such as how to safely operate satellite internet and how to leverage domestic networks to deploy offline communication channels.

2. **Need for verified tool recommendations:** The in-country user communities highlighted a critical need for secure and verified tools. Many advertised proxy configurations and shutdown solutions have questionable security standards. It is essential to create resources and tools that enable in-country users and

helper communities to effectively distinguish between safe and malicious options.

3. **Digital security help desk:** A digital security help desk can provide urgent support for users and helpers that face security threats or are compromised. This also includes utilizing our trusted partnerships with big tech platforms, including Meta, Google, Telegram, and others, to expedite the resolution of security and account related issues (e.g., recovering hacked accounts, disabling accounts upon arrest, securing compromised profiles) for activists, journalists, and others connecting via satellite.

4. **Engage Helper Community in tool prototyping and testing:** Tool providers outside of Iran could engage the Helper Community as active collaborators in tool prototyping and testing, ensuring development is informed by real-world use and constraints. Building on these insights, we could develop playbooks that translate experimentation into on-the-ground deployment easily adoptable by the helper communities themselves.

5. Comparative Analysis

From an Internet connectivity measurement perspective, the January 2026 shutdown is more severe and more sophisticated than past shutdowns.

- During the roughly seven-day shutdown of “Bloody November” in November 2019, the situation on the ground was similar to that in 2026, both in the scope of the protests and the level of state repression and violence. Network measurement data indicated that the 2019 shutdown was achieved through a more blunt form of disconnection, with authorities leaving domestic connectivity to the NIN and limited access to the global Internet.
- In 2022, during the Women Life Freedom protests, only mobile networks were shut down nightly. This measure aimed to suppress mobilization while mitigating the economic, political, and social costs of a full Internet shutdown. Fixed line traffic increased during these mobile shutdowns. As such, the 2022 shutdown was relatively nuanced and surgical compared to the one in 2026.
- In the roughly 60.5-hour (2.5 days) shutdown in 2025, during the Israel-Iran War, Iranians still had access to the NIN and other forms of domestic communication. Circumvention tools remained relatively effective, enabling some users to navigate around the restrictions despite the loss of global connectivity.

June 2025 v.s. January 2026

With only six months apart, the scale and lengths of the shutdowns proved to be very different between what happened in June 2025 and in January 2026.

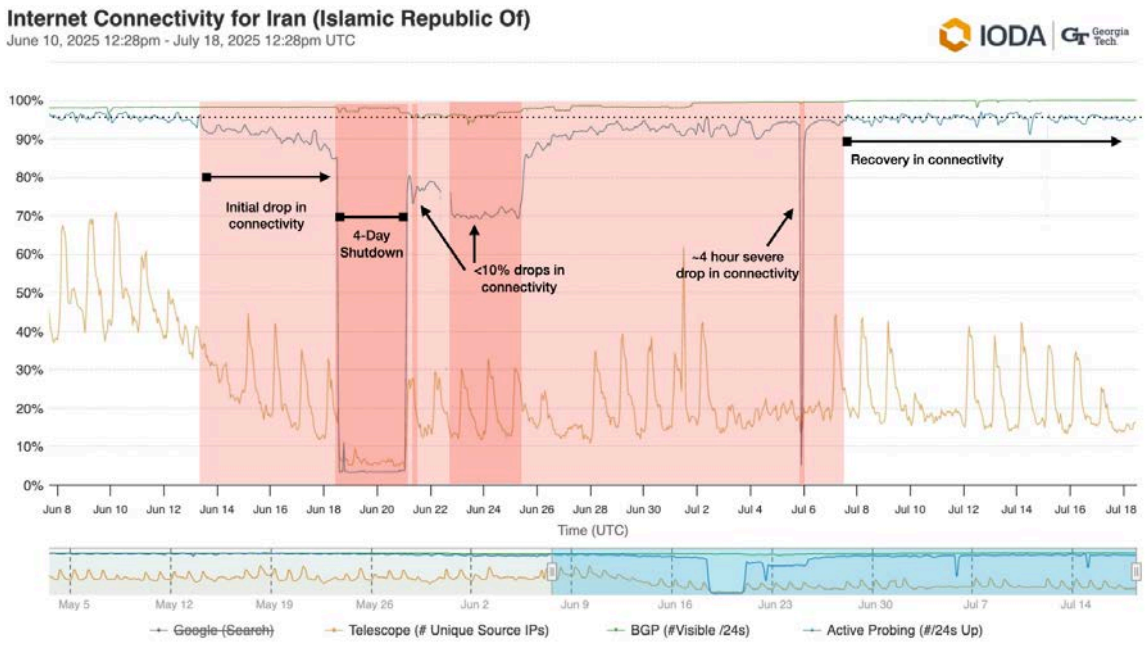
In June 2025, what was observed during the initial degradation in Internet connectivity mirrored what is often present during times of conflict when Internet and power infrastructure is impacted by missile attacks. Beginning on June 18, 2025, connectivity across the country plummeted, with Internet traffic dropping by as much as 97%. The Iranian regime shut down the Internet over 4 days and cited national security as the motivation. Unlike previous shutdown, Border Gateway Patrol (BGP) or Routing Announcements were not used to implement the shutdown in 2025, making it more covert and harder to detect early on.

The January 2026 shutdown was carried out more swiftly and abruptly, with few detectable early signs. One of the signs was the drop of IPv6 traffic from Iran; by herding traffic onto older, more easily monitored infrastructure, the authorities can maximize surveillance and filtering efficiency. Within hours of the IPv6 traffic drop, Iran's kill switch severed both international connectivity and the NIN, even SMS services were cut, resulting in a nationwide communication blackout.

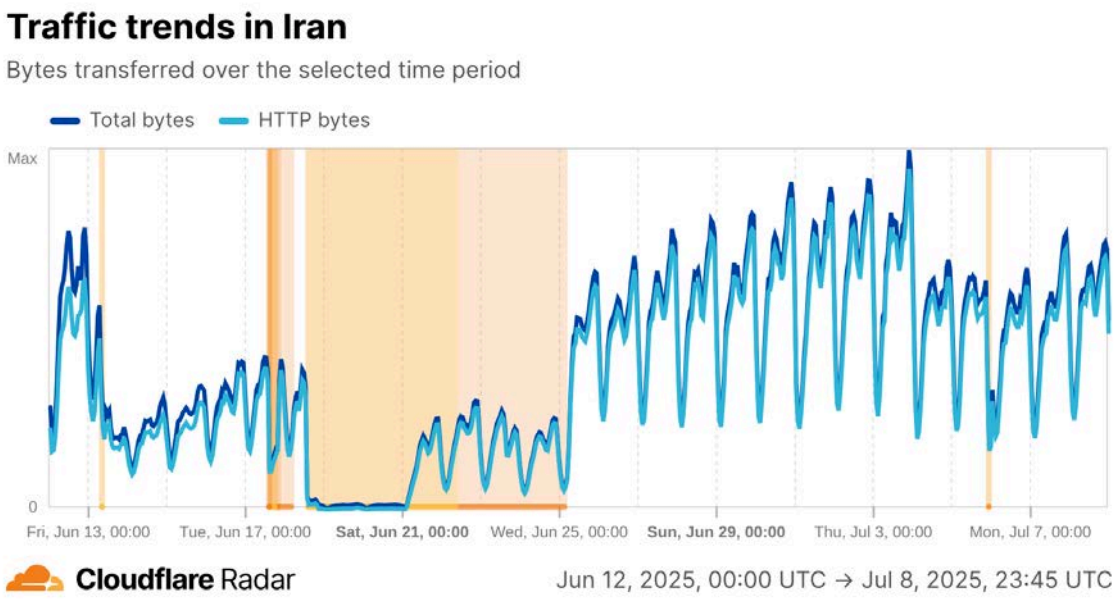
Starting mid-January (Phase 3), we noticed "early recovery" driven by whitelisting. Looking at Google Services (Search, Images, YouTube, Maps, Spreadsheet) and Mozilla Telemetry data from Firefox Browser users, we see that during the June 2025 shutdown, whitelisted services, specifically Google Search and Google Images get connectivity restored well before other services like Google Maps and Mozilla Firefox. We saw a similar pattern in the January 2026 shutdown where Google Search and Google Images recovered on January 18th. Access to Google Maps, Google Spreadsheet, and Mozilla Firefox recovered along with IODA's telescope signal on January 24th. We have not seen YouTube usage show a meaningful return to levels pre January 8th which suggests possibly ongoing whitelisting of access.

While the whitelist architecture is not new, the most recent internet disruption reveals a highly uneven distribution of access to whitelisted services. The slow restoration process and observed online activity point to a tiered access system. Under this system, government-trusted and authenticated accounts appear to be given priority, while the general public continues to experience highly volatile connectivity. Essentially, the state has established a digital hierarchy, which is likely the template for future control measures even during relatively stable times.

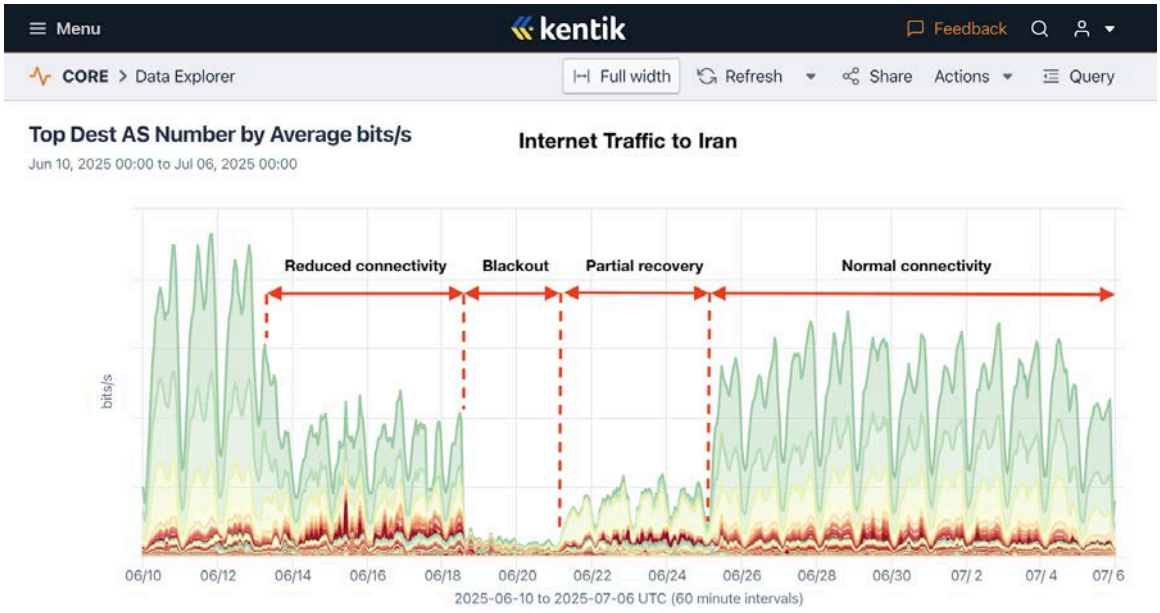
This comparative view of Google Product Usage data (Gmail, Images, Maps, Spreadsheet, Search, YouTube) and Mozilla Telemetry data from Firefox usage and IODA's Telescope signal between the June 2025 shutdown and the January 2026 shutdown shows a difference in how the shutdowns impacted access to these services in terms of duration, restoration, and levels of user traffic.



IODA data on Internet infrastructure connectivity for Iran during the Israel-Iran War



Cloudflare data on Internet traffic trends in Iran during the Israel-Iran War



Kentik data on Internet traffic to Iran during the Israel-Iran War

6. Policy Analysis: The Engineering of Digital Isolation

The January 2026 internet shutdown marks a landmark transition from reactive "kill switches" to a permanent architecture of segmented access. This was not a byproduct of crisis management, but the calculated operationalization of a multi-agency strategy to reclassify the global internet as a state-granted privilege rather than a public utility. By institutionalizing a "blocked-by-default" whitelisting system, the state has effectively replaced the social contract of universal access with a rigid digital hierarchy.

Phased Approach: Regional Disruptions and Digital Curfews

Between December 28 and January 7, the state's digital response was characterized by a localized, urban-centric campaign of repression. During this period, authorities deployed targeted disruptions in an attempt to suppress protests, utilizing a mix of mobile data cuts and fixed-line throttling to create a fragmented information environment. In Tehran, the disruptions were hyper-localized, focusing on high-friction districts such as the Grand Bazaar and Baharestan, alongside university areas like Enghelab and Valiasr Square. This pattern was mirrored across the country in cities including Sanandaj, Shiraz, Isfahan, Mashhad, and Ilam, where users faced localized outages while surrounding regions remained ostensibly online.

To suppress coordination as the protests emerged, authorities moved beyond blunt "kill switches" to a model of calculated network degradation. This resulted in the phenomenon of "zombie connections," where devices appeared technically connected to the network at the IP layer, but performance was sabotaged at higher-layer protocols. On January 2, OONI (Open Observatory of Network Interference) identified "protocol-level anomalies" affecting QUIC—a protocol essential for the speed and security of modern messaging, video streaming, and web browsing. OONI noted that these effects appeared across various operators over several days, suggesting a phased deployment of the interference across the national infrastructure.

Circumvention tool developers reported a "no-ping" phenomenon to Filterwatch, where VPNs would show a "connected" status but suffer from such extreme latency and packet loss that no data could actually pass through the tunnel. By destabilizing the handshake processes and hijacking encrypted traffic at the application layer, the state successfully isolated users from global platforms while maintaining a facade of connectivity, rendering the digital tools protesters relied on for real-time communication virtually useless.

January 8 Nationwide Blackout

On January 8, the policy shifted from localized pressure to a complete severance of global internet connectivity. The Supreme National Security Council (SNSC) issued a directive to the Telecommunication Infrastructure Company (TIC) to initiate a nationwide shutdown. The execution of this order began with a sudden withdrawal of 98.5% of IPv6 routes.

While IPv6 traffic accounts for a smaller portion of Iran's total data, targeting it first was a calculated administrative move. IPv6 is harder to monitor with the state's existing Deep Packet Inspection (DPI) tools, which were largely optimized for IPv4. By removing IPv6, authorities forced all remaining traffic onto IPv4 networks where their surveillance and filtering infrastructure is more mature. Hours later, at 10:15 PM local time, the "kill switch" was applied to IPv4 as well, reducing nationwide connectivity to less than 1% of ordinary levels. This marked the start of the total blackout phase, moving from protocol-level sabotage to an absolute severance of the national network from the global web.

The Dual-Tier Whitelisting Model

Following the peak of the total blackout, the state moved to a "blocked-by-default" model that operationalized a sophisticated, two-fold whitelisting strategy. This system transformed the internet from a public right into a state-granted privilege,

functioning through the simultaneous implementation of service-level and user-level access controls.

The period of total digital isolation was characterized by significant domestic and systemic strain. Reports indicated the national economy was losing approximately 5 trillion Tomans daily, with the livelihoods of an estimated 10 million people tied to the digital ecosystem. By mid-January, as the country approached a critical "resilience threshold," the broader implications of prolonged isolation became a central point of concern across domestic and international sectors.

Amid these compounding economic losses, coupled with heightened international pressure, domestic unrest, and a variety of other social and political factors, authorities began a selective restoration of connectivity on January 17 through service-level whitelisting. Under this model, instead of filtering specific "bad" websites, gatekeepers manually approved a limited number of "good" services for the general public while keeping the broader web inaccessible. Concrete examples of this policy appeared on January 18, when essential global tools like Google Search and Images flickered back to life despite the rest of the international internet remaining dark. This layer functioned as a controlled economic lifeline, restoring domestic services on the NIN—such as banking portals and the Snapp ride-hailing app—to prevent systemic economic collapse while maintaining a vacuum of independent information.

However, this restricted public access was paired with a far more privileged tier of user-level whitelisting. This second layer utilizes specialized network configurations and "white SIM cards" to grant unrestricted global connectivity to a select group of state-sanctioned individuals, officials, and loyalists. This system creates a profound political hierarchy where professional status or perceived loyalty determines one's level of connectivity. While ordinary Iranians were severed from the global web, state media operatives and public officials remained active on platforms like Twitter and Telegram to disseminate regime narratives—providing visible proof of the state's capacity to maintain high-bandwidth connections for its own propaganda needs while millions remained disconnected.

Implications: The Rise of Digital Stratification

This dual-tier architecture has institutionalized a "class-based internet," where an individual's level of connectivity is dictated by their perceived loyalty or utility to the state's administrative and propaganda framework. Empirical evidence for this stratification is found in the disparity of activity among domestic media outlets and elite figures during the shutdown. Analysis by Factnameh revealed that while the general public and independent journalists were entirely offline, state-aligned and

security-affiliated outlets—such as Fars News, Tasnim, and IRINN—maintained a continuous and uninterrupted presence on international platforms like Telegram and X.

The existence of this parallel, high-speed network for the elite was further evidenced by the activity of high-profile regime defenders and relatives of state officials. During the peak of the blackout, professor and government advisor Mohammad Marandi was notably able to conduct high-quality video interviews with international news outlets, a feat that requires high-bandwidth connectivity technically unavailable to the rest of the country. Similarly, social media activity from members of the political elite—such as the grandson of Ayatollah Khomeini—continued despite the general population being severed from global platforms. However, research by Factnameh identified a notable correlation between account reactivation and political compliance; for instance, the Jamaran channel (associated with Hassan Khomeini's office) resumed activity on January 13, the same day Hassan Khomeini issued a public statement condemning the protests.

These cases provide visible proof of a "digital aristocracy" that remains connected to the global web to preserve the state's international image and social standing, even as millions are denied the same access for their basic livelihoods. The institutionalization of this tiered internet extends beyond the elite to influential professional groups, such as university professors and select commercial actors, who are granted access to minimize institutional pushback. According to a Filterwatch report, procedural shifts at the Tehran Chamber of Commerce further illustrate this: merchants must now undergo physical verification, IP registration, and sign conduct pledges to receive "authorized" connectivity.

Ultimately, this system ensures that digital access is no longer a platform for independent communication, but a potent instrument of statecraft and social engineering. By maintaining high-bandwidth connections for its own functions while keeping the broader population in a state of managed digital isolation, the state has effectively weaponized the infrastructure of the internet to create a new, permanent hierarchy of digital citizenship. This shift is also fundamentally altering the circumvention landscape; the traditional "Filter-shekan" (VPN) is evolving into the "Melli-shekan" (National Network Breaker)—tools required not just to bypass specific blocks, but to escape the confines of a hermetically sealed domestic intranet.

Institutional Actors and the "War Room" Model

The Iranian state has formalized a shift from bureaucratic interference to a direct "war room" model of command. This transition reflects a broader consolidation of authority within the security apparatus, where the IRGC has effectively become the

executive arm responsible for implementing internet policies approved by the Supreme Council of Cyberspace (SCC) under the direct supervision of Ali Khamenei.

The January shutdown was managed by a centralized "Cyber War Room" involving several key governmental bodies. The Supreme National Security Council (SNSC) provided the legal mandate for the blackout, with numerous reports indicating that the IRGC's Khatam al-Anbia Headquarters functioned as the executive arm for these policies. The National Cyberspace Center (NCC), led by Mohammad-Amin Aghamiri, acted as the technical coordinator between security forces and private ISPs.

This institutional takeover is part of the practical application of the "Cyberspace Regulatory System"—the latest iteration of the User Protection Bill, which was re-submitted to Parliament in November 2025. This framework explicitly delegates the determination of access protocols at the "International Internet Gateway" to the SNSC, making their directives legally binding for all executive bodies. By embedding the power to disconnect or whitelist access within this formal, pre-defined mechanism, the state has effectively shifted de-facto control of internet gateways from civilian oversight to the security and military apparatus.

Under this framework, the militarization of the network is visible at the highest managerial levels. The ICT Ministry has been relegated to a purely executive role, functioning as the technical arm for higher-tier security agencies. This shift in command was starkly illustrated by the forced removal of Irancell's CEO, Alireza Rafiei. While public reports suggested he resisted the shutdown, industry insiders clarified that his dismissal resulted from a strategic disagreement over the technical methods used to execute the blackout. His replacement, Mohammad Hossein Soleimanian—a figure with deep ties to the Ministry of Defense and military hubs like SAIRAN and SAGA—confirms that mobile operators are no longer viewed as civilian utilities, but as strategic assets managed with a "battlefield" mandate.

The current agenda for this military-led oversight was articulated by Brigadier General Majid Khademi, head of the IRGC Intelligence Organization. Khademi outlined a strategy to "strengthen immunity" against external influence through the completion of the National Information Network (NIN) and the active monitoring of domestic communication infrastructures. Under the "Cyberspace Regulatory System," the NIN is now defined as the default, stable state of the nation, while the global internet is treated as a conditional and manageable exception. This ensures that future shutdowns are executed as disciplined military operations, bypassing the need for public legislative debate or civilian accountability.

7. Conclusion

The January 2026 internet shutdown represents a permanent shift in Iran’s approach to information control, moving from reactive "kill switches" to a structural "blocked-by-default" architecture. This multi-phase operation has transformed global internet access from a public utility into a state-granted privilege, creating a tiered digital society where connectivity is tied to identity and professional status. The state’s technical successes—specifically its selective restoration of whitelisted services and the herding of traffic onto older, more easily monitored infrastructure—confirm that Iranian authorities have successfully engineered a sustainable model of digital isolation.

However, the unprecedented scope of this blackout was met with an equally unprecedented domestic response. The emergence of the "Helper Community" demonstrated that years of capacity building have yielded a resilient, decentralized counter-force. Successes with in-country Starlink terminals and peer-to-peer messaging apps proved that local volunteers can maintain critical lifelines even during total blackouts.

To counter this new digital reality, the international community must pivot its strategy. While we must continue to sustain the global rapid response ecosystem—including the researchers, technologists, and developers who build vital circumvention tools—we must also scale our investment and prioritize domestic resilience. This means not only providing tools from the outside but directly empowering the local helper communities with the resources and training to sustain their own connectivity independently of state-controlled gateways. Supporting these grassroots enablers is the most vital path forward for preserving internet freedom in Iran.