Wartime Digital Isolation: Iran's Strategic Internet Shutdown

Period covered in the report: February 28 – March 6, 2026

Contributions: IODA, Kentik, Cloudflare, Holistic Resilience, DeltaChat, Miaan, and ASL19

Acknowledgement: We acknowledge the solidarity of the internet freedom community working to monitor and respond to the internet shutdowns in Iran. This community has continued to coordinate, collaborate, and share information to date, playing a significant role in countering the impacts of shutdowns in Iran, including contributions and analysis included in this report.

Introduction

Following the joint U.S.-Israeli military strikes on February 28, 2026, Iranian authorities imposed a near-total international internet blackout in two stages. Disruptions to international internet access began in the early hours of February 28, shortly after the military strikes started. Around 10:30 AM Iran time, the country's three main operators experienced a sudden and sharp drop in traffic. Later, around 3:30 PM Iran time, traffic across all three networks, Mobile Communications of Iran, MTN Iran Cell and Telecommunication Company of Iran fell to nearly zero.

In contrast to the shutdown in early January, the transition to the National Information Network was much more seamless and the domestic network and services experienced minimal disruptions. After nearly ten days since the shutdown began, the National Information Network (NIN) remains active to preserve domestic services, and global connectivity continues to be systematically dismantled.

This report analyzes the technical nature of this wartime shutdown and the strategic utility of the state's "digital whitelisting" model —a system now fully activated to monopolize the conflict's narrative and enforce strict, identity-linked control over the remaining points of access.

Policy Analysis

Service-Level Whitelisting

Domestic news agencies, including Tasnim, published a list of essential websites accessible via the national internet. This list included websites in several main categories to meet users' needs through the national network: news agencies, domestic search engines, maps and navigation services, online translators, video and entertainment platforms, practical services (religious times and calendar, road maintenance, the Adl Iran system, etc.), domestic messaging platforms (Bale, Eita, Rubika, Soroush Plus), software downloads (Android and iOS), the national portal and organizations (Smart Government, the website of the Office for the Preservation and Publication of the Works of Ayatollah Khamenei, Civil Registration, Social Security, Cyber Police, etc.).

While these services remained available, there were consistent reports that even whitelisted international platforms faced intermittent disruptions, suggesting a highly restrictive and fluctuating control environment.

User-Level Whitelisting

Select individuals and entities retain unfettered access to the internet during this internet shutdown. Individuals have access through their mobile operators, referred to in Iran as "white-sim cards" while larger institutions and entities have access through physical locations.

Factnameh research confirms the consistency of this "asymmetric information environment" across consecutive shutdowns. During both the January 2026 blackout and the current conflict, data analysis revealed that while independent and reformist outlets were forced into silence, a select group of state-linked and IRGC-affiliated channels—including Tasnim, Fars, and Mehr News among others—maintained regular, uninterrupted online activity.

This infrastructure has remained a central pillar of the state's communication blockade following the February 28 attacks. While independent and reformist outlets remain silenced, Factnameh's analysis of the current conflict shows that select pro-state Telegram channels have been functioning as the sole coordinated voices within a manufactured information vacuum. This orchestration has become critical for the state to manage the narrative surrounding the war as well as the leadership succession following the February 28 death of the Supreme Leader. By ensuring these pro-government voices remain active in both English and Persian, the state continues to counter external reporting and dominate the narrative surrounding the conflict and domestic stability in real-time.

State-Sanctioned Communication and Physical Information Hubs

To support this manufactured information vacuum, authorities have coordinated a shift toward domestic and traditional channels that ensure state narratives reach the public even when digital access is entirely severed. Following the February 28 shutdown, government-affiliated channels—including influential hubs like @sepah_quds—circulated messages urging the public to subscribe to official news on the domestic messaging app Eitaa. These communications explicitly framed the move as a necessary precaution in light of the international internet blackout.

Government-affiliated channel directing users to migrate to the domestic messaging app Eitaa as a precaution against the international internet blackout.

This strategy extends into a fallback plan for total network failure, where digital infrastructure is replaced by traditional physical hubs. Official instructions circulated during the first days of the conflict emphasized that if state television, social media, or even telephone networks were to be disrupted, information would be delivered through local mosques. Citizens were directed to go to their mosques to receive critical updates, signaling a strategic reliance on hyper-local, state-aligned physical sites as a way to disseminate information in times of crisis. Additionally, the state promoted specific radio frequencies, such as 95.5 MHz FM, as alternative broadcast channels for news in the event of television antenna failures. Together, these actions demonstrate a comprehensive management model that seeks to ensure state authority remains the sole source of information, regardless of the level of technological disruption.

Civil defense instructions from the @sepah_quds channel designating local mosques and specific FM radio frequencies as

primary information hubs in the event of total network failure.

Warning Messages Sent to Mobile Users

While the state promotes domestic and physical alternatives for information, it simultaneously employs aggressive enforcement measures against those attempting to maintain global connectivity. In the midst of a rapid military escalation and profound internal instability, Iranian authorities appear to be utilizing direct-to-user SMS alerts as a primary tool for psychological control.

The message shown below, sent from a sender ID labeled 'POLICE' during the first few days of war, warns the recipient that 'repeated connection to the international internet' will lead to their phone line being blocked and potential judicial referral. In an environment characterized by widespread insecurity and a near-total blackout of global communications, this tactic represents a surgical effort to project state authority directly onto personal devices. By framing global connectivity as a criminal act during a national crisis, the state is attempting to enforce digital isolation and suppress the flow of information, leveraging the mobile infrastructure to deliver high-stakes threats to an already vulnerable and isolated population.

Monetizing Access: Subscription Based Connectivity

During the initial days of the military strikes, the mobile operator MCI (Hamrah-e Aval) launched the "Stable Communication Network" project. This initiative allows users to purchase unfiltered internet packages via USSD codes that reportedly remain active even during nationwide blackouts. These access points were initially uncovered and shared by VPN developers and network researchers who discovered the "hidden" codes while monitoring which parts of the network remained functional during the shutdown. The project now operates under official coordination, with similar mechanisms adopted by other operators like Irancell.

Parallel to this, the government introduced the "Pro Internet" plan, marketed as a solution for businesses requiring stable international connectivity. This plan is highly restrictive and expensive, requiring a special SIM card and formal identity verification, including a business license. The pricing is tiered to further monetize access: while standard international traffic is 8,000 tomans (~0.05 USD) per gigabyte, accessing sites that are typically filtered costs a premium of 40,000 tomans (0.25 USD) per gigabyte.

By limiting this service to only 500 initial users and requiring rigorous registration, the state has created a model of "Accountable Access," ensuring that those with global connectivity are fully traceable. Ultimately, these programs demonstrate that the technical infrastructure for global access remains intact during shutdowns; the blackouts are a policy choice designed to monetize censorship and maintain strict state oversight.

The state's strategic shift toward aggressive whitelisting and 'Accountable Access' is not merely a policy directive; it is directly reflected in the granular technical patterns observed across global network monitors. The following technical breakdown of the February 28 shutdown illustrates how authorities have developed a more sophisticated model of network fragmentation. By dismantling global connectivity while maintaining a functional domestic intranet, the state is trying to build a walled digital environment. This allows for the uninterrupted operation of state services and media while simultaneously blinding the population to international reporting and external military developments, effectively turning the national infrastructure into a tool for absolute narrative control.

Technical Breakdown

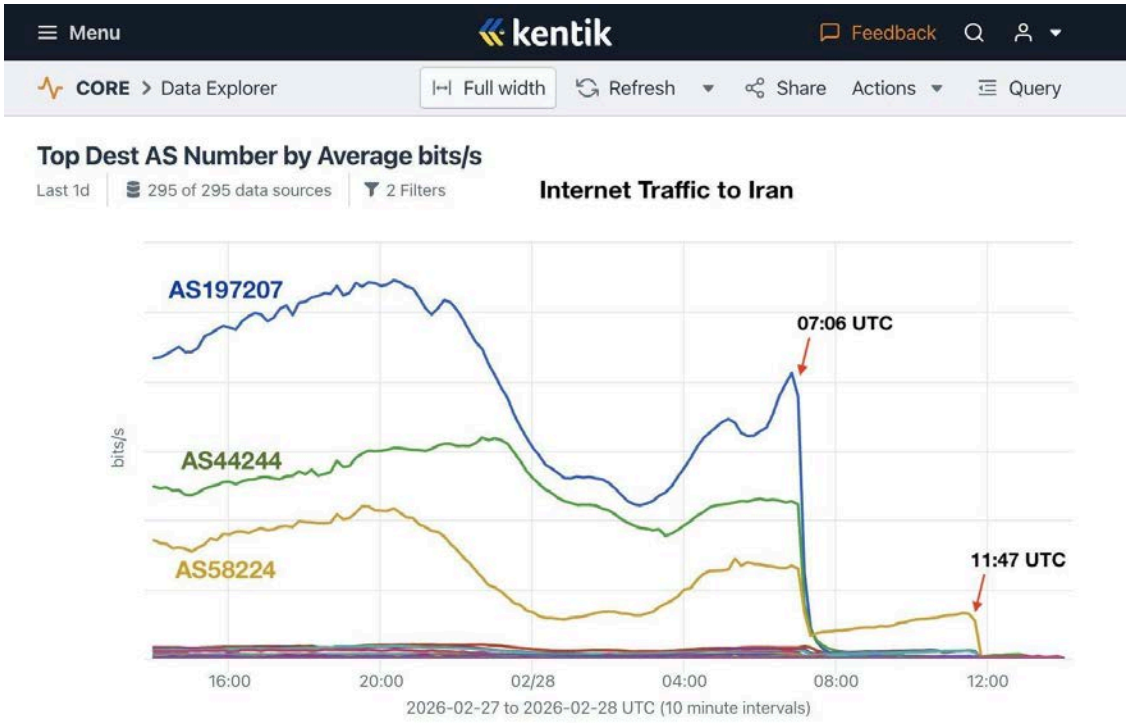
The following technical indicators provided by Kentik, IODA, and Cloudflare collectively document the transition of Iran's network from a standard open architecture to a fragmented, whitelisted environment. While each monitor captures

a different layer of the network, the shared signature across all datasets confirms that global connectivity has been systematically suppressed as a matter of state policy.

Disruptions to international internet access began in the early hours of February 28, shortly after the attacks started. However, unlike the January 2025 shutdown, the National Information Network (NIN) remained active from the outset this time.

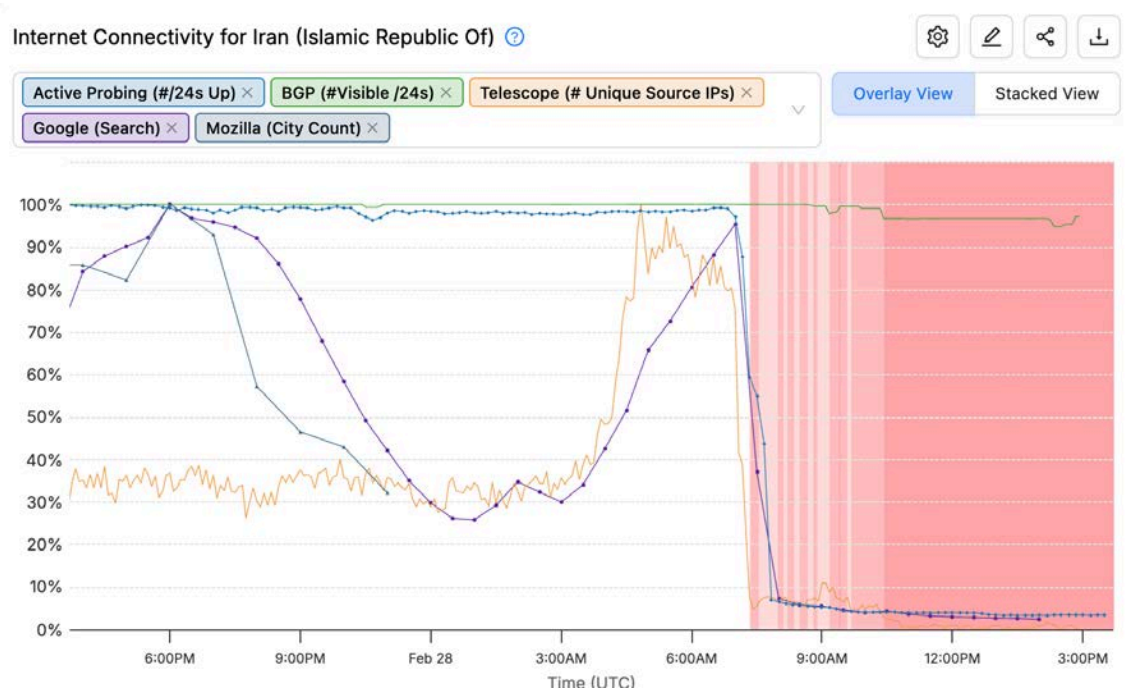
While traditional communication channels were briefly paralyzed in the first hours of the February 28 attacks, they have since somewhat stabilized. Currently, international incoming calls to Iran are being systematically blocked, preventing families and journalists outside the country from reaching Iranians. Conversely, outbound international calling from inside Iran remains functional, primarily through roaming packages provided by domestic operators (MCI and Irancell). SMS services have followed a similar pattern of instability, with domestic messaging restored while international SMS remains largely restricted or delayed.

Data from Kentik below shows that the internet blackout occurred in two stages. First, around 10:30 AM Iran time, the country's three main operators experienced a sudden and sharp drop in traffic. Later, around 3:30 PM Iran time, traffic across all three networks — AS197207 (MCI), AS44244 (Irancell), and AS58224 (Telecommunication Company of Iran – TCI) — fell to nearly zero.



On March 1, the second day of the war, even the limited remaining traffic saw additional simultaneous outages across multiple networks. This raised the possibility of damage or disruption affecting shared infrastructure, such as fiber-optic lines, power supply, or intercity network hubs.

The initial shutdown timeline is systematically corroborated by IODA's telemetry, which shows a near-complete drop in active probing, telescope, and Google product usage at the same 10:30 AM threshold. Crucially, IODA data shows that BGP (Border Gateway Protocol) routes remained active throughout the disruption. This pattern—where the "pipes" to the internet remain visible but traffic is absent—is technically consistent with a whitelist-based control model rather than a physical severance of the lines. While public access to the global internet was cut off, newsroom offices, so-called "whitelisted SIM cards," and a number of government systems continued to have internet access from the very first hours of the international shutdown.

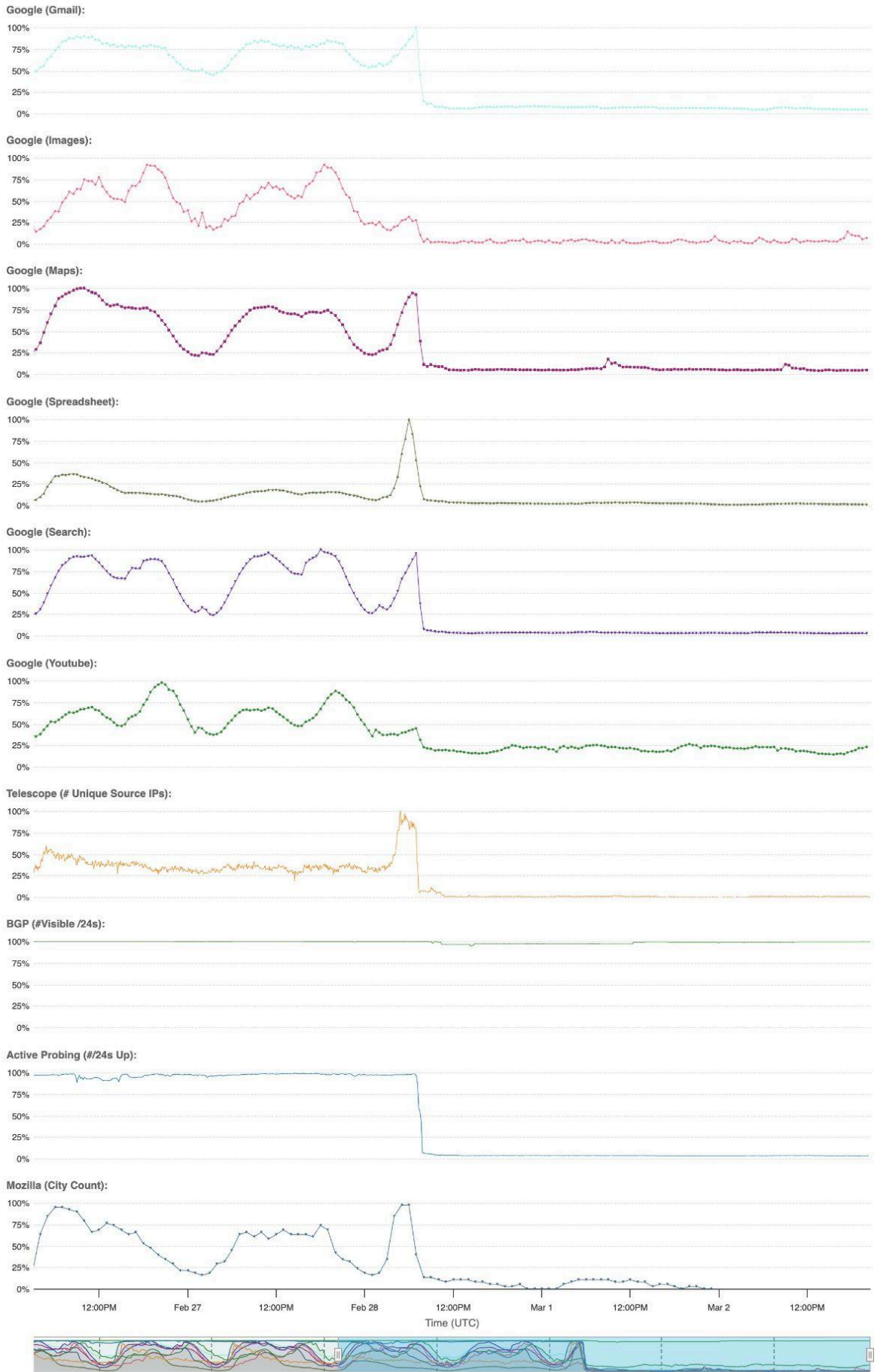


IODA Internet Connectivity Graph for Iran shows BGP routing (green) is not heavily impacted, but Active Probing, Telescope, Google Search usage, and Mozilla Telemetry data all show a significant and simultaneous drop. The red area in the chart represents automated outage alerts.

Internet Connectivity for Iran (Islamic Republic Of)

February 27, 2026 3:30am - March 2, 2026 8:36pm UTC

IODA | Georgia Tech

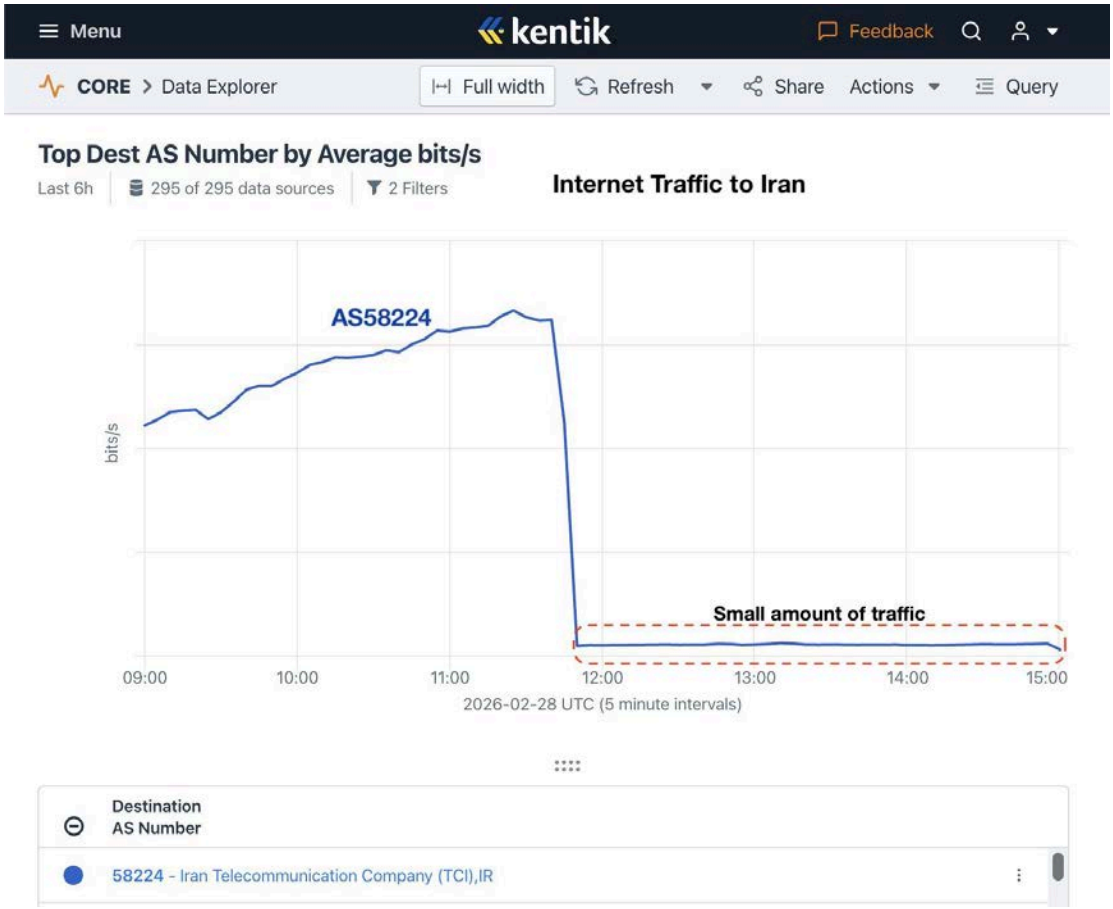


Internet Connectivity for Iran (Islamic Republic Of)

January 3, 2026 3:36pm - February 2, 2026 3:36pm UTC

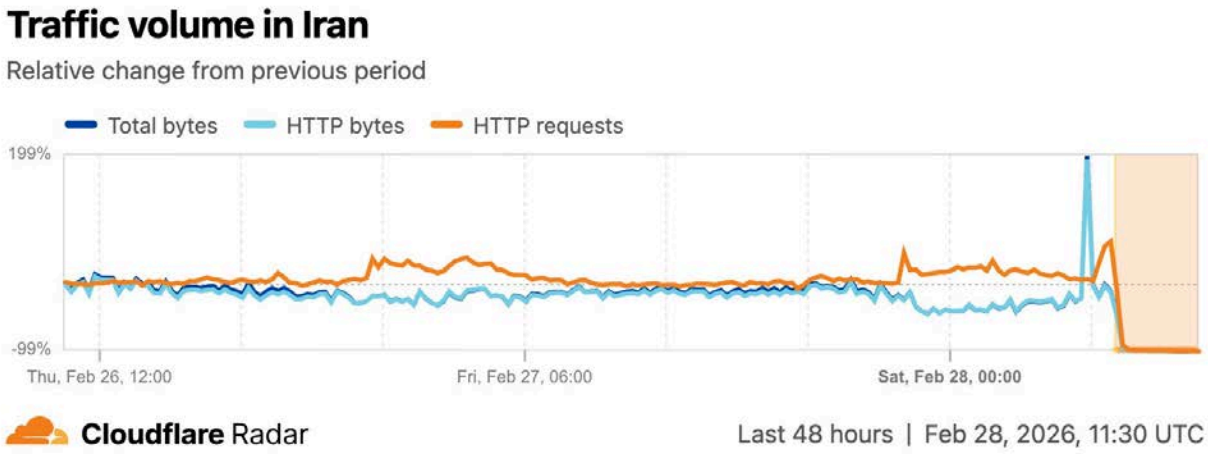
IODA | Georgia Tech

Examining IODA Internet connectivity data in addition to Google product usage data and Mozilla Telemetry data shows that in addition to a near-complete shutdown of access to the global Internet, there is tight control to applications via whitelisting. In the previous shutdowns in January 2026 and June 2025, domestic access to products like Google Search were restored domestically before access to the global Internet was restored. Currently, we see no evidence of a fully restored access to google products or Mozilla's Firefox.

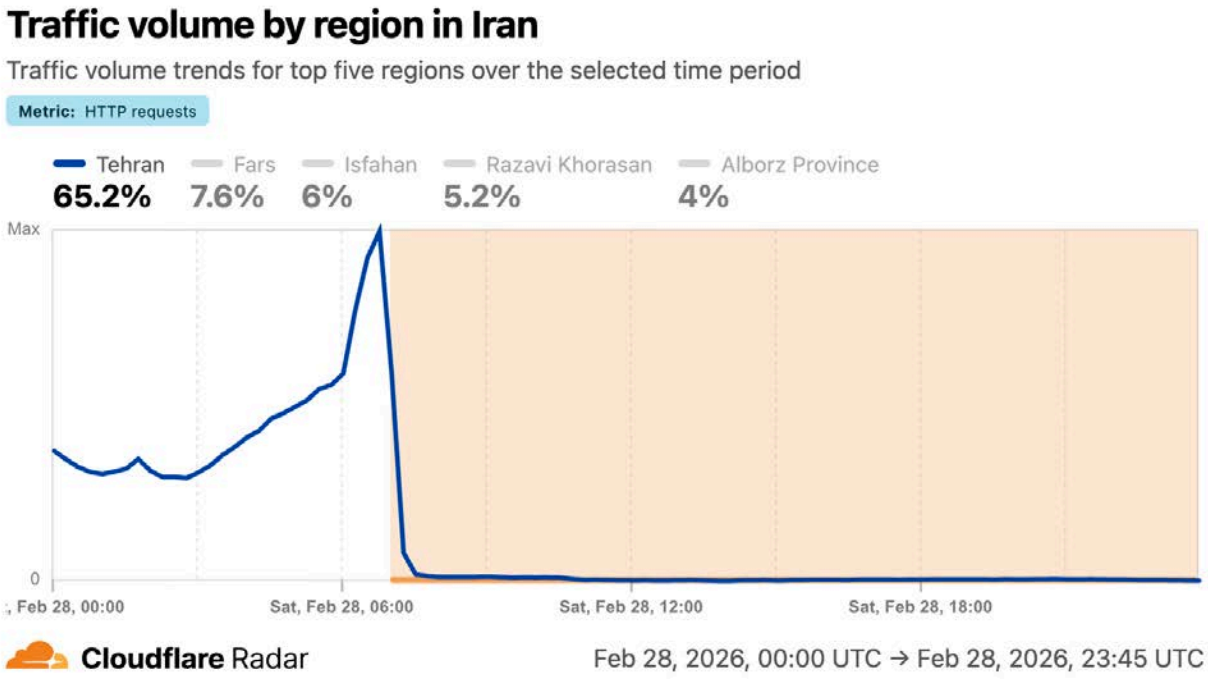


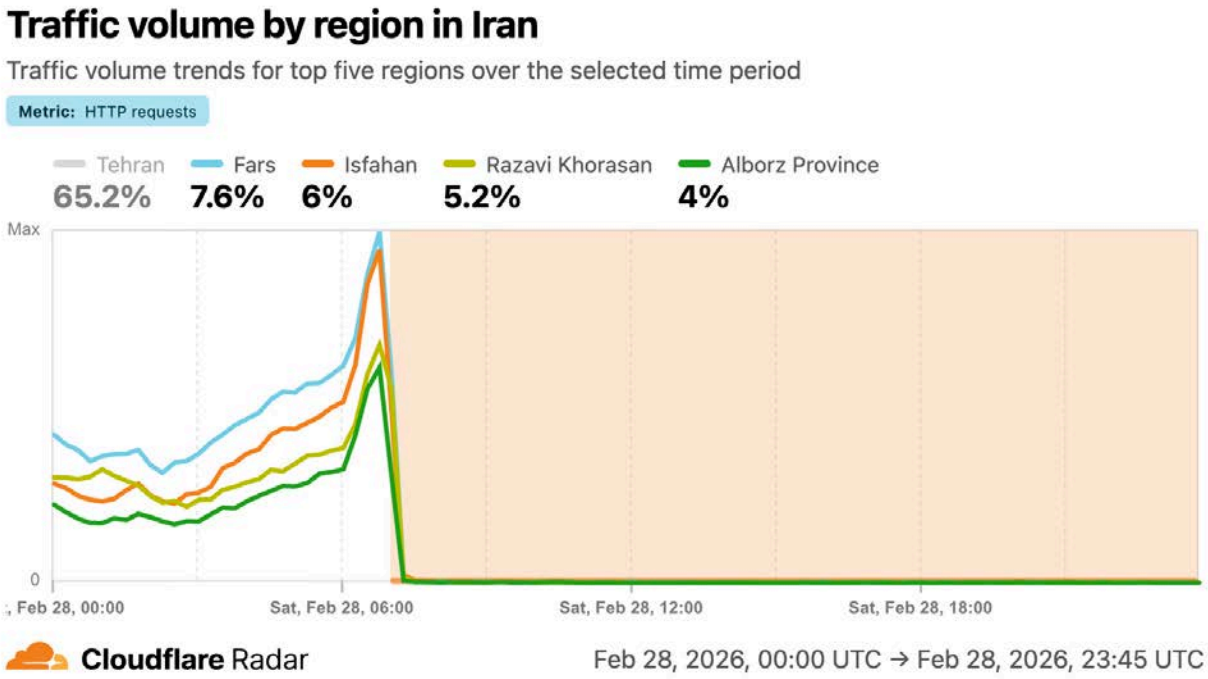
Data from Kentik and others show that while the vast majority of Iranians lack internet service, there is a small amount of traffic that continues to flow in and out of the country (pictured above). The understanding among Iranian digital rights experts is that this traffic is from individuals and services that have been whitelisted by the Iranian authorities, either due to their connection to the government or by technical necessity.

This timeline is further validated by Cloudflare Radar, which recorded a precipitous decline in traffic volume that fell more than 98% below the previous week's levels. Cloudflare's regional data further highlights the granularity of the shutdown: while traffic in Tehran initially stayed slightly above zero, it ultimately collapsed by 2:00 PM local time, trailing the near-total blackouts already observed in other provinces.



Both the aggregate view and the regional views below (with and without Tehran included) show that HTTP request traffic increased in the hour ahead of the outage, before plummeting at around 07:00 UTC (10:30 local time) and remaining flat in the hours that followed. In Tehran, traffic tumbled sharply but stayed slightly above the near-zero levels seen in other regions, before also dropping to nearly zero at 10:30 UTC (14:00 local time).





While traffic from most networks (ASNs) dropped off at 07:00 UTC (10:30 local time), it took a little longer on other networks. As seen in the graphs below, traffic from AS43754 (Asiatech), AS49100 (Pishgaman Toseeh Ertebatat Company), and AS58224 (TCI) initially started to decline around 07:15 UTC (10:45 local time), remained steady, albeit lower, for approximately two hours, and then fell to near zero at around 09:20 UTC (12:50 local time).

HTTP traffic from AS43754

ASIATECH

HTTP requests over the selected time period

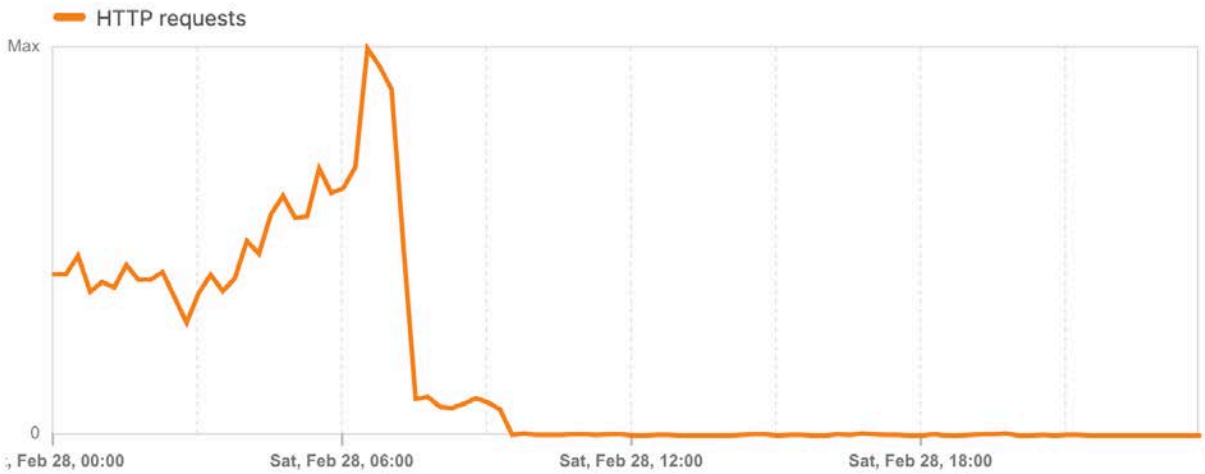
Cloudflare Radar

Feb 28, 2026, 00:00 UTC → Feb 28, 2026, 23:45 UTC

HTTP traffic from AS49100

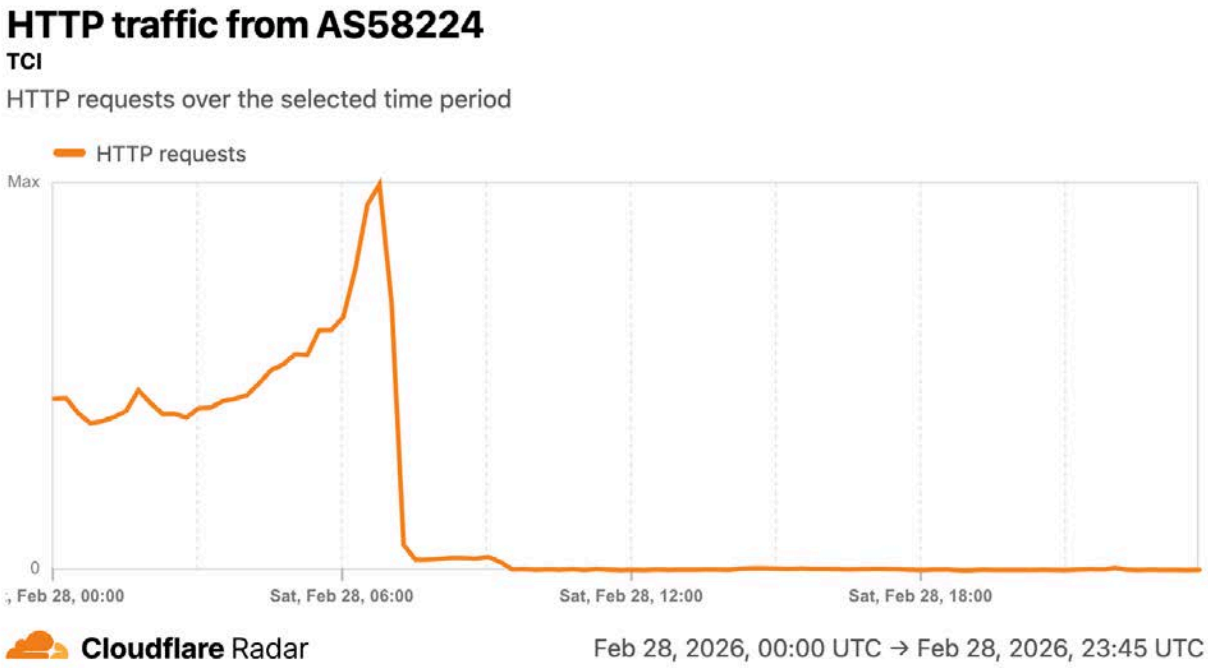
IR-THR-PTE

HTTP requests over the selected time period

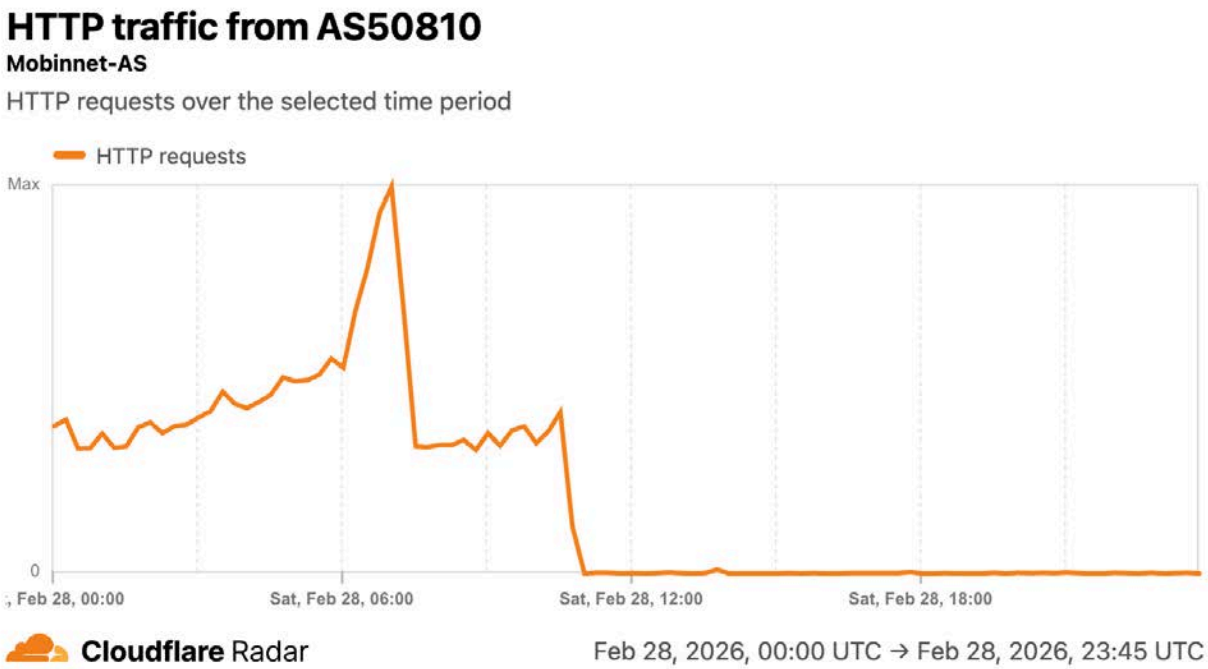


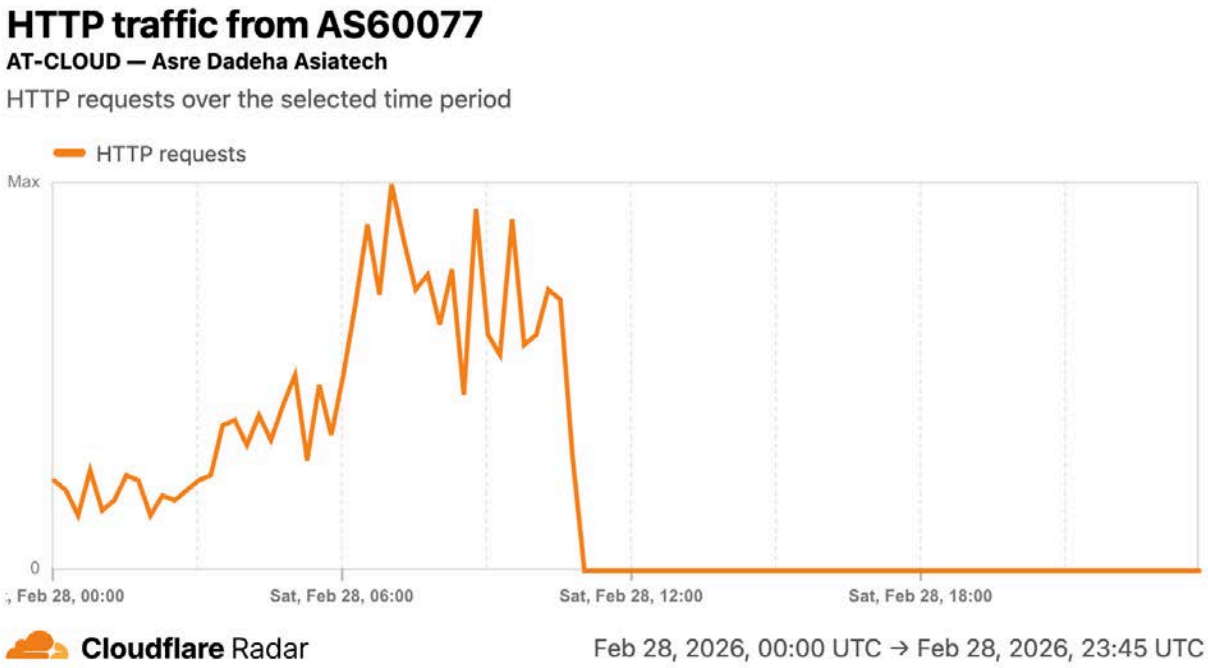
Cloudflare Radar

Feb 28, 2026, 00:00 UTC → Feb 28, 2026, 23:45 UTC

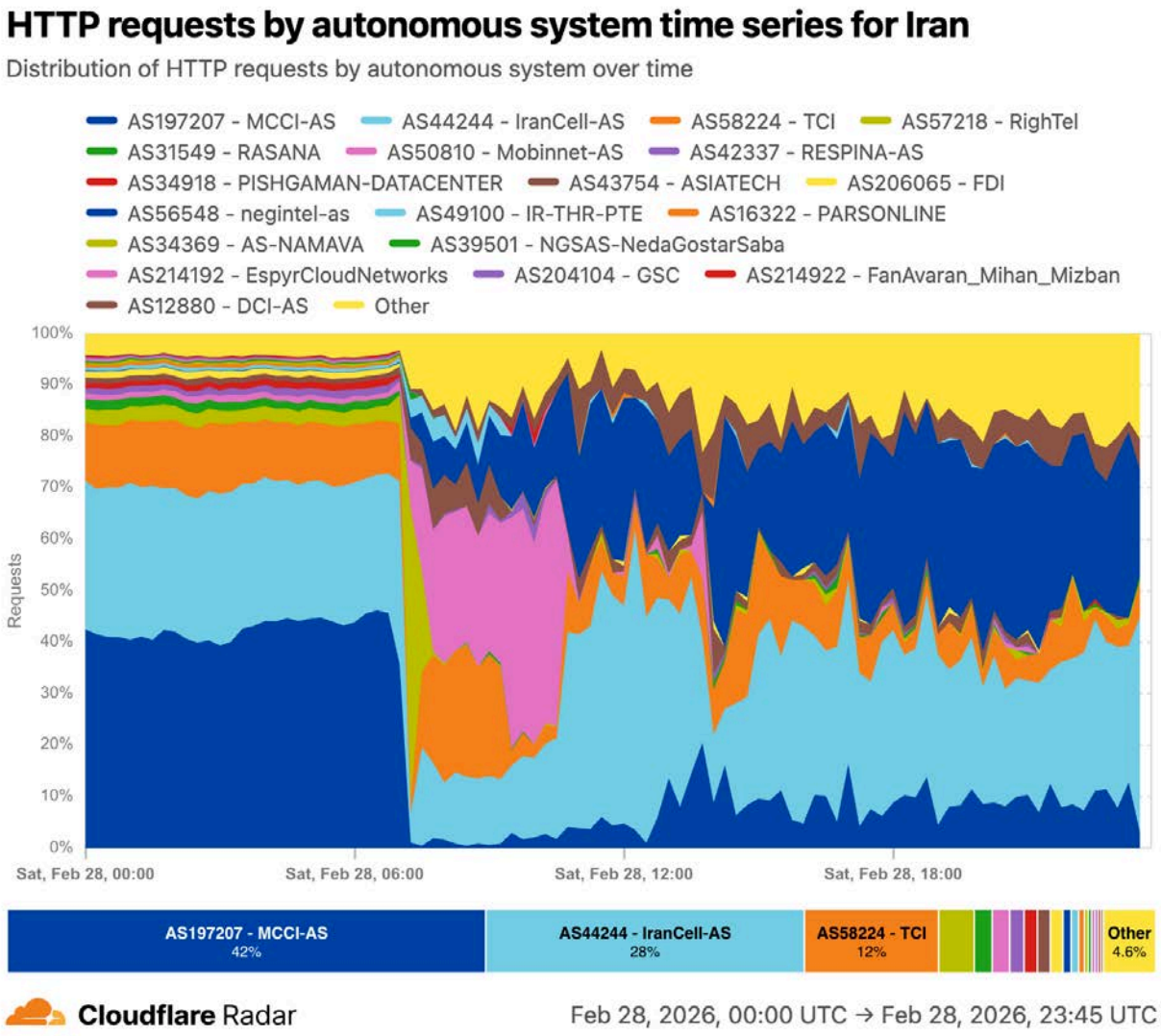


Other networks, including AS50810 (Mobinnet) and AS60077 (Asre Dadeha Asiatech), saw traffic initially drop between 07:00-07:15 UTC (10:30-10:45 local time), and then dropped further towards zero around 10:45 UTC (14:15 local time). It isn't clear why these networks appeared to maintain connectivity for several hours longer than other network providers within the country.





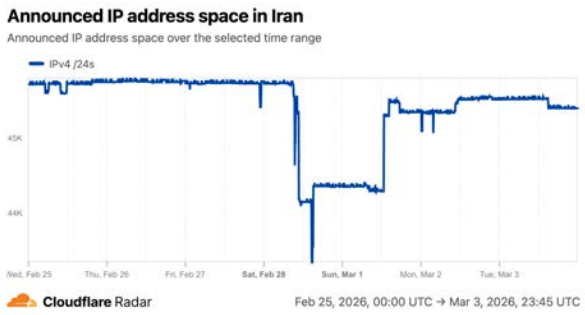
Once the Internet outage started, the distribution of the remaining traffic (a small fraction of previous levels) across ASNs shifted radically. Initially, three providers (MCI, IranCell, and TCI) accounted for over 80% of requests, with nearly half of that from MCI. After connectivity was cut off at 07:00 UTC (10:30 local time), IranCell still generated approximately 30% of requests, but MCI's share had dropped to around 10%. Mobinnet's traffic share grew from nearly 1% to as much as 45%, until it too fell offline around 10:45 UTC (14:15 local time) as discussed above. Negintel surprisingly emerged as a major source of remaining traffic, previously contributing under 1%, but reached peaks of 35% or more later in the day. An aggregation of "other" networks within the country also grew from about 4% to around 15% on average. Extending the timeframe past February 28, we find that IranCell is still the most significant source of traffic, followed by the aggregated "other" networks and MCI.



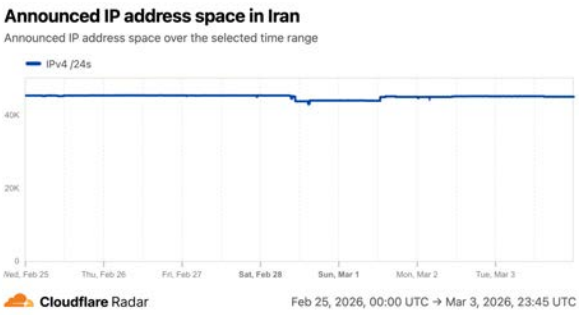
The coordinated nature of the shutdown is evidenced by a 26-hour sustained drop in announced IPv4 address space starting at 2:00 PM local time on February 28. Analysis shows a simultaneous prefix withdrawal across over 20 smaller Iranian ASNs. Respina Networks (AS42337) was identified as the common upstream provider responsible for taking these networks offline during this period. However, according to IODA data, this drop made up only around 3% of Iran's announced address space.

Announcements from major ASNs remained stable during the period. Recovery occurred as a single sharp step at 12:30 UTC the next day. A "precursor event" is also visible in the graph at 09:15 UTC (12:45 local time) when AS42337 (Respina Networks) briefly withdrew prefixes before recovering.

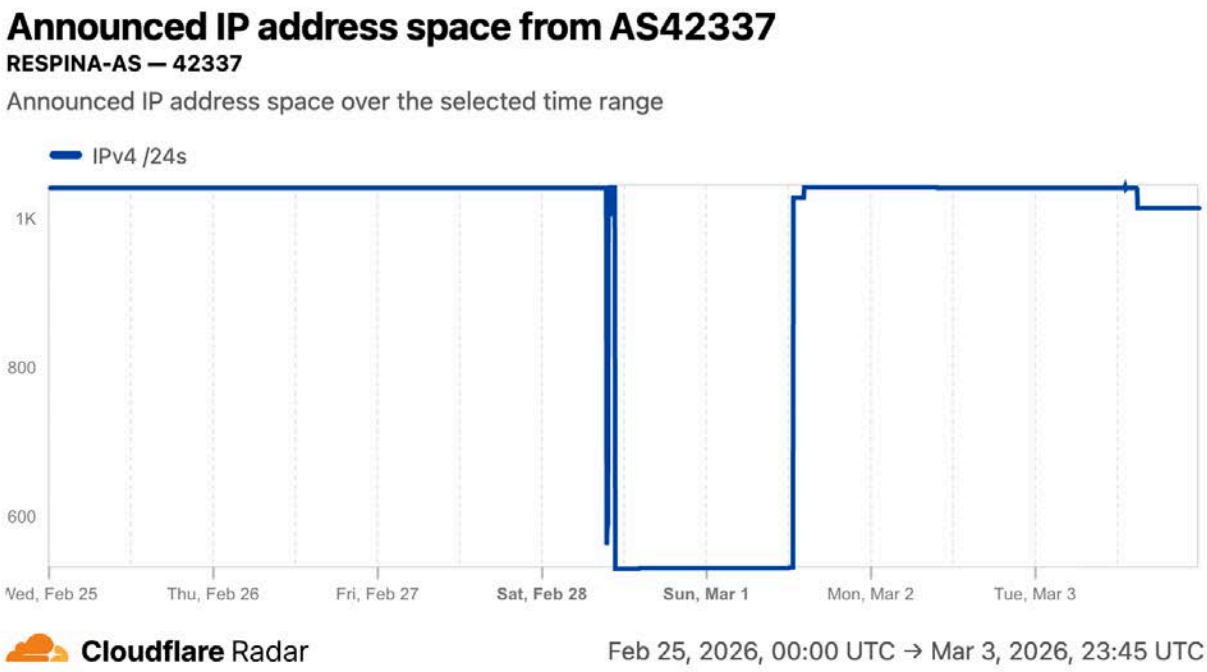
Respina Networks also experienced a [significant drop in announced IP address space] during that 26 hour period, and was likely responsible for taking these 20 networks partially or completely offline for more than a day, as path analysis identified AS42337 as a common upstream provider across all of them.

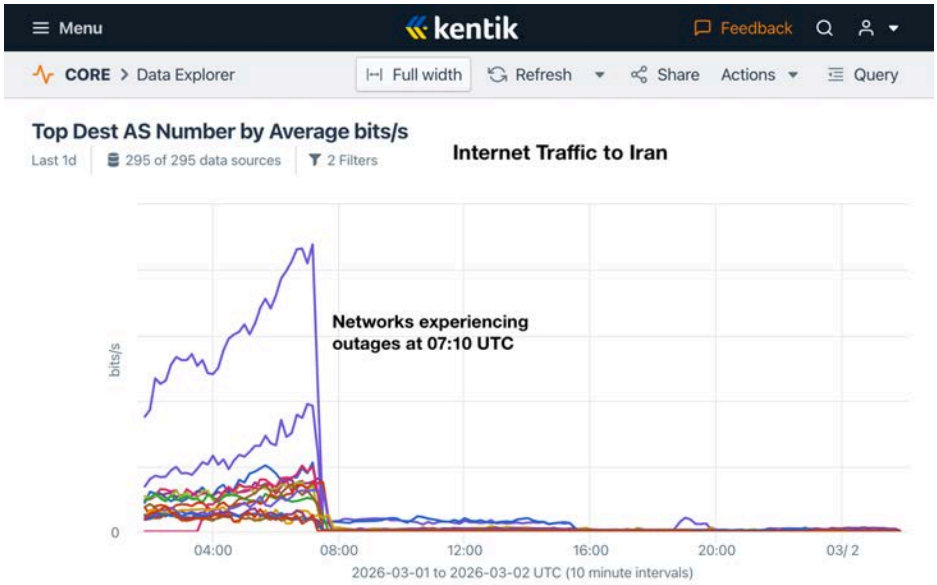


Simultaneous prefix withdrawal across over 20 smaller Iranian ASNs visible in Announced IPv4 address space

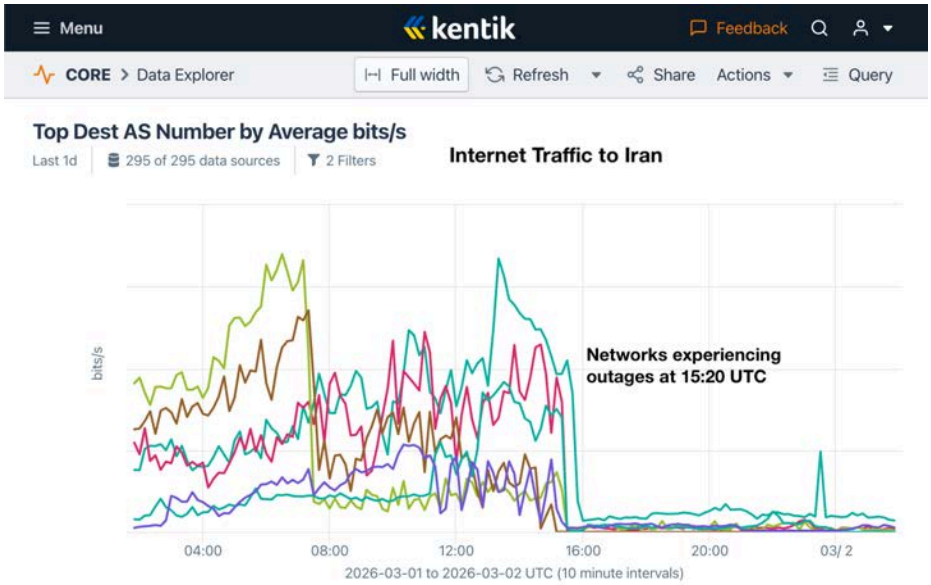


Overall, the drop announced IPv4 address space represents a small fraction of Iranian IP addresses.





Another group of outages occurred a little before 7:00 PM Iran time (15:20 UTC), as shown in the chart below.



On March 1, the limited remaining traffic saw additional simultaneous outages across multiple networks. While the initial February 28 shutdown followed a clear policy-driven pattern, these subsequent disruptions across disparate providers suggest the possibility of physical damage to shared infrastructure, such as intercity

fiber-optic lines, power supplies, or network hubs, resulting from the ongoing conflict.

This shift from a uniform, state-ordered blackout to a more chaotic environment highlights the increasing pressure on Iran's network. While authorities continue to enforce strict domestic controls, the physical infrastructure of the internet is now also being degraded by the ongoing physical conflict. This creates a fragmented network where the state is struggling to manage a functioning domestic intranet at a time when technical indicators suggest that physical infrastructure may be disrupted by the conflict.

Social Digital Resilience

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.

Decentralized messaging apps

DeltaChat remains one of the main functional communication tools in Iran during this time. We are unable to verify the size of the DeltaChat network at this point, but

based on reports from communities managing the local infrastructure, we estimate there are around a million active DeltaChat accounts. The servers inside the country remained active since the beginning of the shutdown, allowing users to securely communicate within Iran, but not abroad.

DeltaChat's infrastructure was partly affected by the NIN disruptions, likely as part of a broader outage impacting numerous servers nationwide. In the past months, DeltaChat has launched multiple features such as hosting channels and launching mini-apps on the platform. These allow the users not only to communicate with one another, but share media files, videos, polls and subscribe to media channels, host blogs and share content with a broader audience using the platform.

Starlink terminals and Starlink VPNs

There are ongoing community-wide initiatives organized by Iranian internet freedom organizations to deliver Starlink terminals to communities on the ground. These initiatives started after the internet shutdowns following the Women, Life, Freedom movement, and have continued since, providing thousands of Starlink terminals to thousands of people in Iran. These terminals have proven to be a lifeline for internet connectivity and communications during the past two months of internet shutdowns and network degradations.

In response to the internet shutdown of early January , Starlink made its service completely free for users inside Iran. Users are not required to pay the usual monthly subscription fees, and even accounts that were previously suspended or had outstanding balances have been reactivated.

Devices simply need to be powered on to regain connectivity. This has significantly helped with deploying new terminals and bringing older devices back online.

Rise in Home-Made Starlink VPN

We're seeing a really interesting rise in people using tools to share their Starlink internet connection by setting up homemade personal VPN servers. Basically, users create a VPN server at home and use it to share their Starlink connection with friends and family over the domestic network (what we used to call "domestic internet").

This is great to see and it can significantly expand the impact of each Starlink terminal, potentially multiplying its reach by up to 20 times.

As shown in the image below, more than 600 Starlink users downloaded NasNet Connect in the past 30 days alone. NasNet Connect is one of the tools designed to

help Starlink users securely share their internet connection remotely with their trusted network.

Jamming Status

Over the past two days, we have not observed any direct Starlink signal jamming anywhere in Iran. However, GPS spoofing and broader jamming activities remain active nationwide. That said, the current GPS interference appears to have minimal or close to no serious impact on Starlink users at this time.

Market Availability

As expected, bringing terminals into the country has become more challenging. The number of devices entering Iran has decreased compared to previous weeks. This reduced supply has driven prices significantly higher, with some terminals reportedly reaching up to $4,000 (approximately 2x the price earlier this month).

Road Ahead: Recommendations

Both the June 2025 shutdown and the recent blackouts 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.