IRAN: 2026 Shutdown Technical Analysis

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

14 January 2026

dd

Context

Following the onset of antigovernment 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.

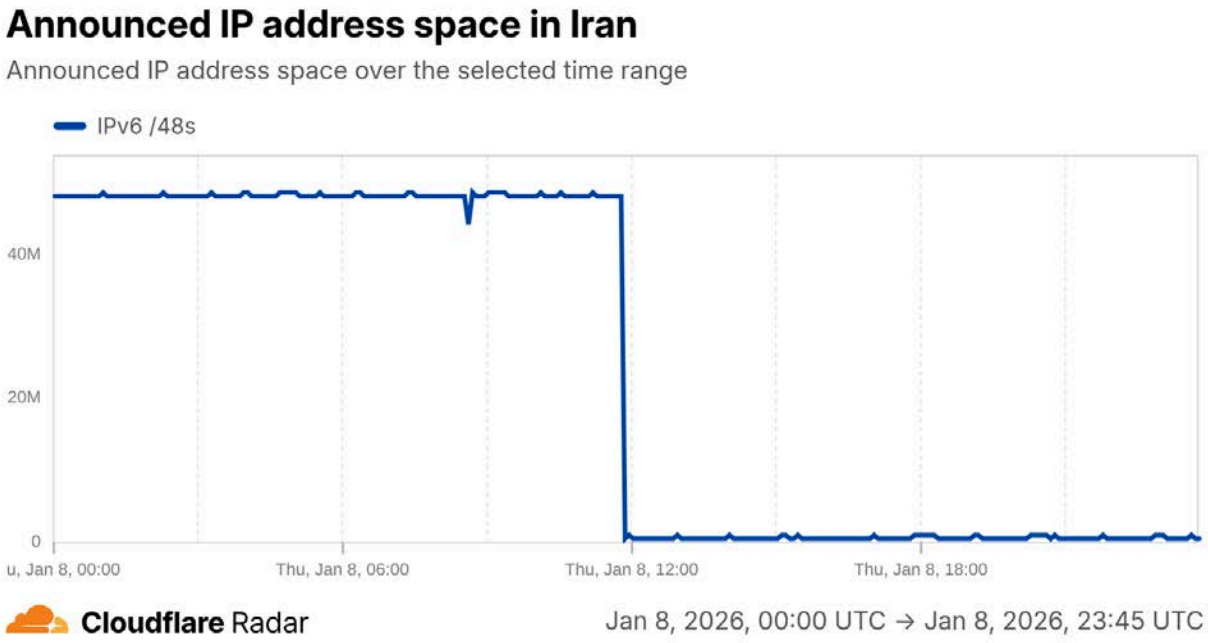
This approach shifted dramatically on January 8, 2026, when protests expanded sharply in size, intensity, and geographic reach. Iranian authorities responded with arguably the most comprehensive and total shutdown of the Internet and other communication tools in history. Beyond shutting down international traffic, authorities also shut down the NIN, privileged (unrestricted) sim cards, mobile phones, and even landline telephones. As of this writing, this blackout is still largely in place, with authorities restoring only some phone connections and whitelisting (i.e. granting specific access) government websites, as well as government approved news outlets, communications tools, entertainment services, financial institutions, retail applications, and some health and educational platforms.

This report provides a technical analysis of network traffic trends based on data from IODA, Kentik, and Cloudflare to map the escalation from partial disruption to a near-total communications blackout.

Chronological Overview of Internet Disruptions

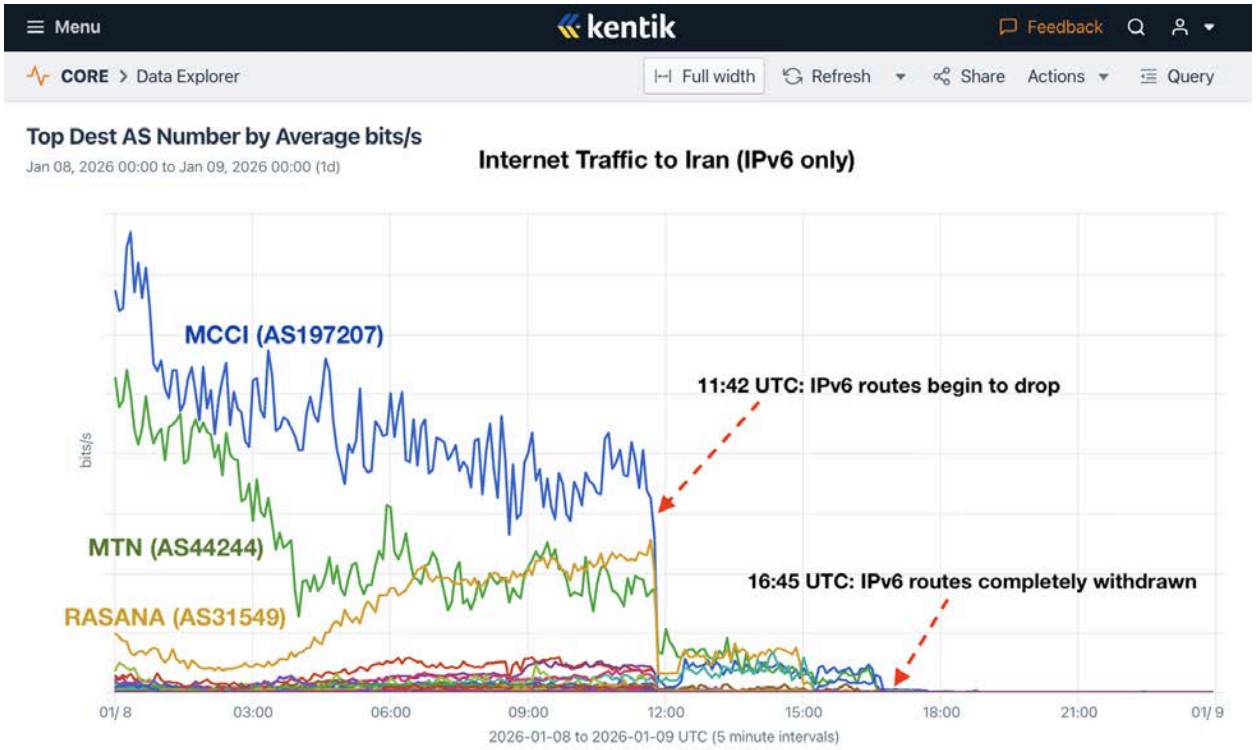
Network Degradation Pre-Shutdown on January 8th

IPv6-related shifts observed on January 8 provided the first indication of changes to come. At 11:50 UTC (15:20 local time), the amount of IPv6 address space announced by Iranian networks dropped by 98.5%, falling from over 48 million /48s (blocks of 2^80 IPv6 addresses) to just over 737,000 /48s. 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.

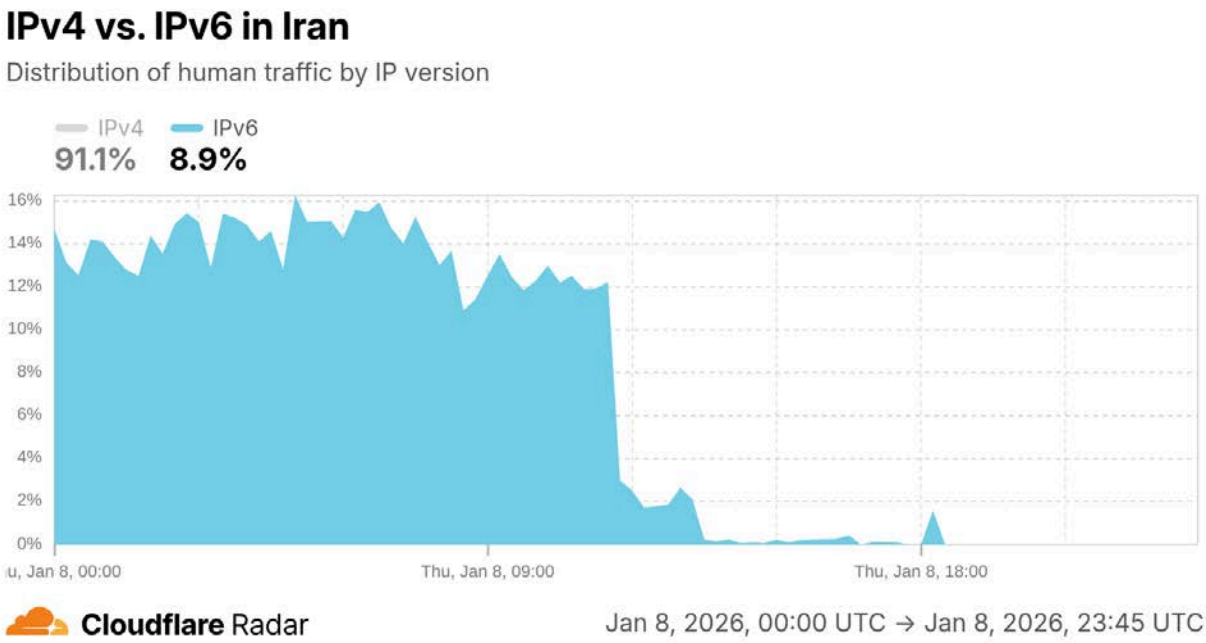


This drop in announced IPv6 address space served to reduce IPv6's share of human-generated traffic from around 12% to around 2%.

On January 8th, authorities withdrew IPv6 routes while leaving the vast majority of IPv4 routes intact. This distinction is significant: by maintaining the IPv4 routing table, the state retains the infrastructure necessary to implement selective whitelisting. Had these routes been withdrawn entirely, authorities would have lost the ability to surgically grant internet access to specific approved individuals and organizations.



IPv6 traffic began to drop at 11:42 UTC on January 8th as the propagation of IPv6 routes dropped precipitously. 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.



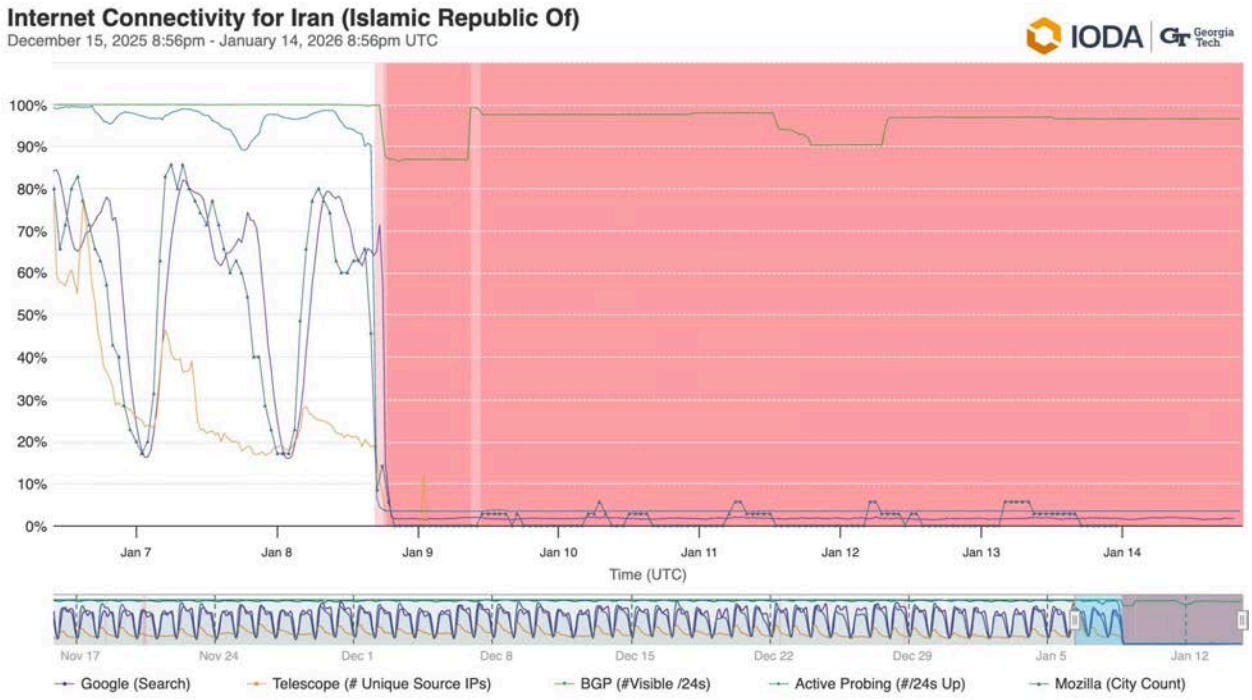
This drop in announced IPv6 address space served to reduce IPv6's share of human-generated traffic from around 12% to around 2%.

Total Shutdown: January 8th → Ongoing

On the evening of January 8th, Internet connectivity measurement data across various sources (IODA, Cloudflare, Kentik) demonstrated a near complete loss in connectivity. Meaning, Iranians lost access to the global Internet.

IODA Data

IODA actively measures the responsiveness of networks through active probing. To create the Active Probing signal, IODA continuously pings devices in tens of thousands of networks around the globe. Most devices are designed to automatically respond to these pings by echoing them back to the sender. IODA collects these responses and labels networks as connected/active. IODA measurements show a nominal amount of responsiveness to active probing (~3%), which could be an artifact of the measurements or lingering connectivity for whitelisted access provisioned to specific users (e.g. Iranian government actors and services). 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.

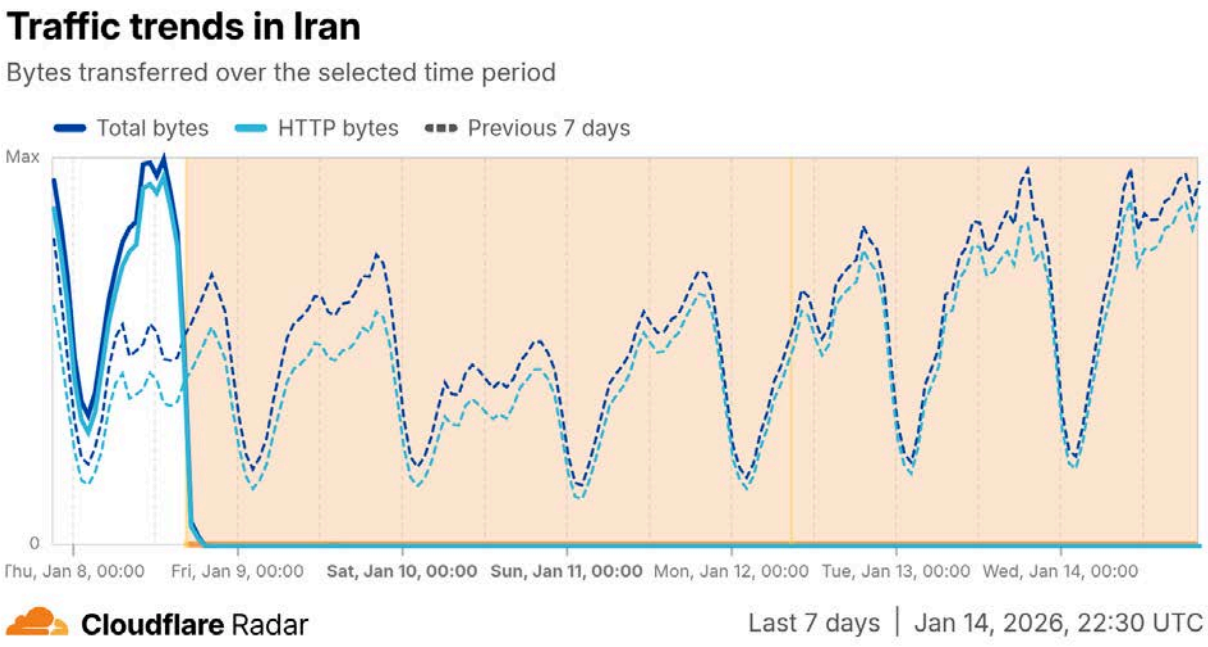


IODA measurements show normal connectivity signals and the Internet shutdown starting

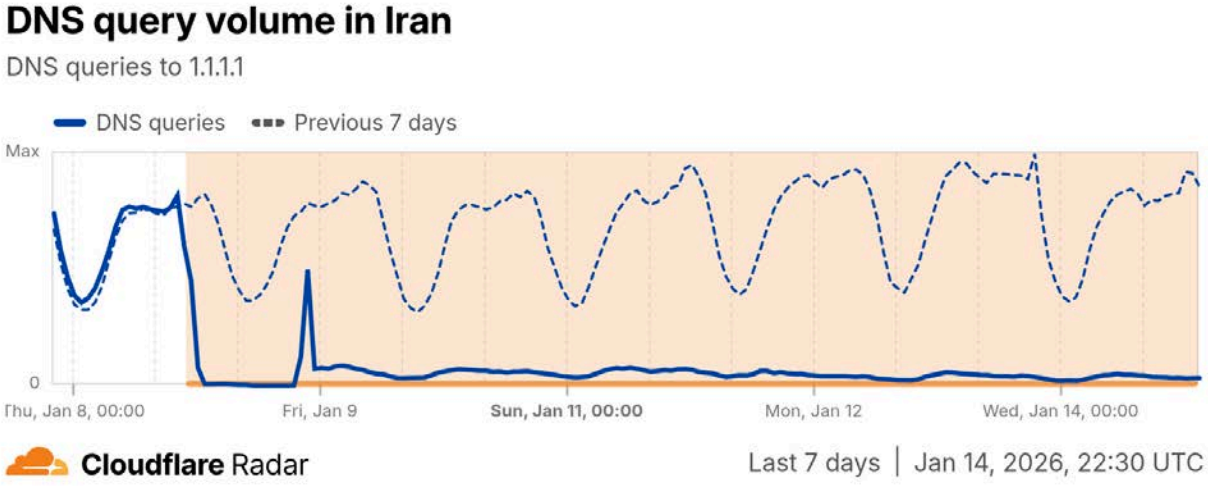
the evening of January 8th.

Cloudflare Radar

Cloudflare provides a public dashboard of traffic data based on its global network and the Internet traffic it handles for millions of customers. Cloudflare Radar data shows traffic volumes from Iran are at a fraction of a percent of previous levels.

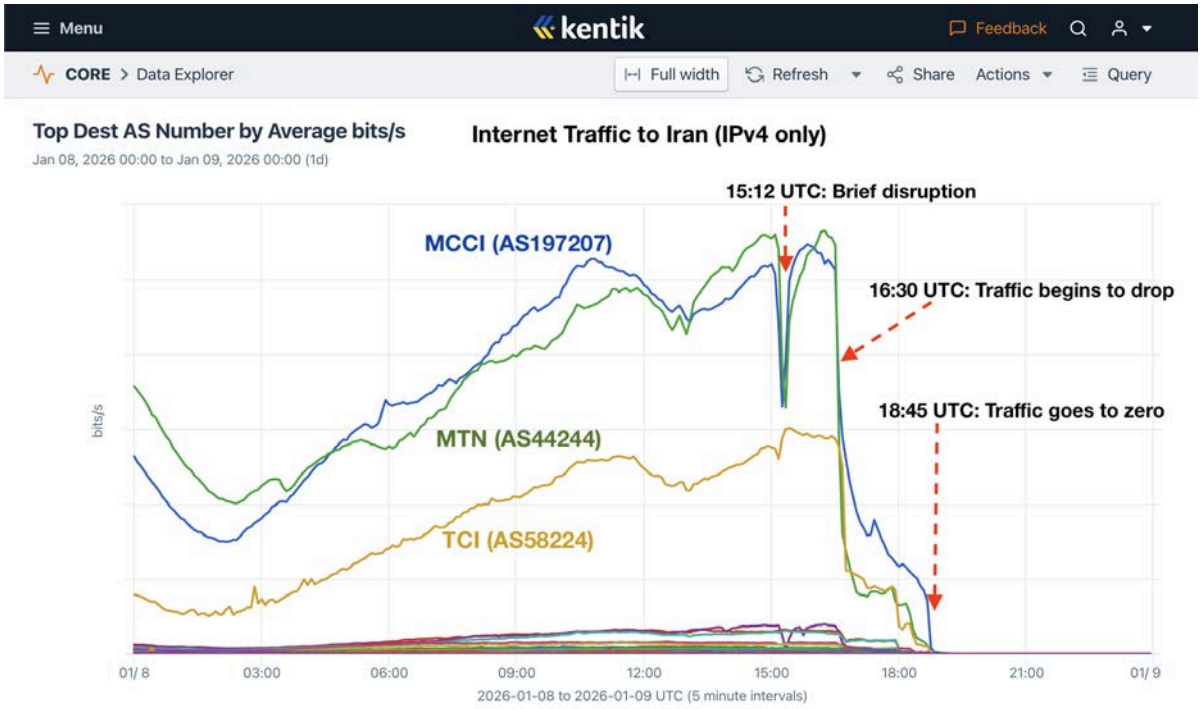


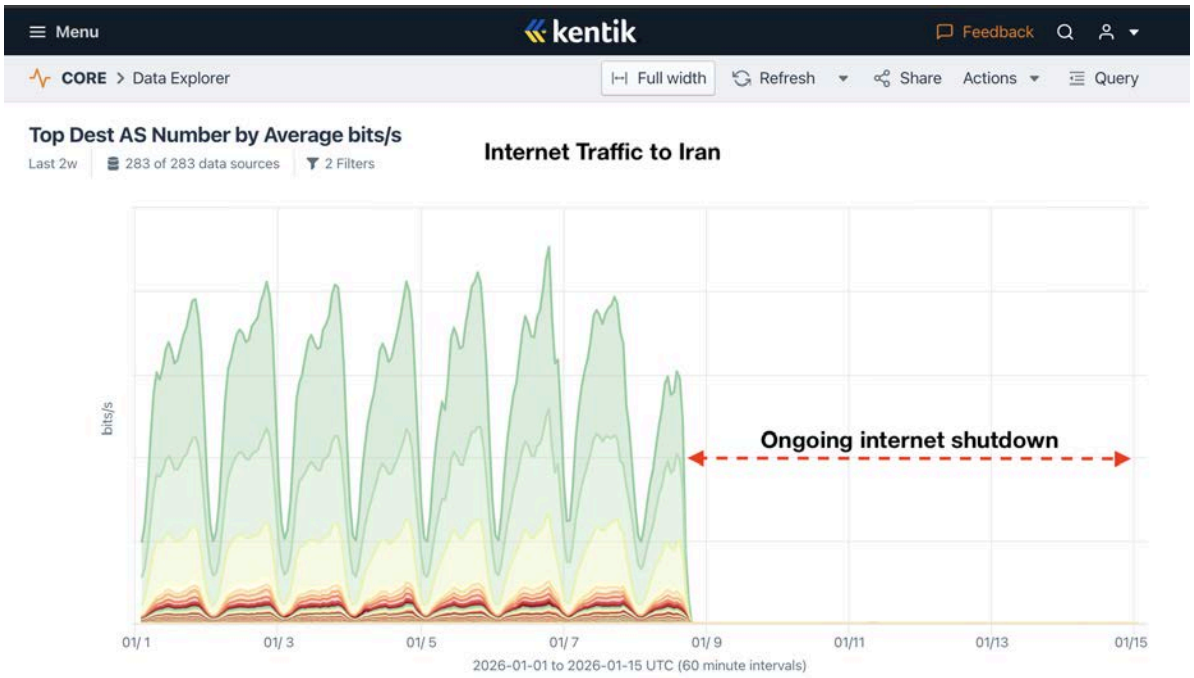
Traffic to 1.1.1.1, Cloudflare's public DNS resolver, from Iran also disappeared as the shutdown began, but a small amount of traffic has remained visible since January 9.



Kentik

Kentik is a popular cloud-based NetFlow analytics platform. On January 8th, Kentik data shows traffic to Iran stopped and the country completely severed itself from the global Internet.



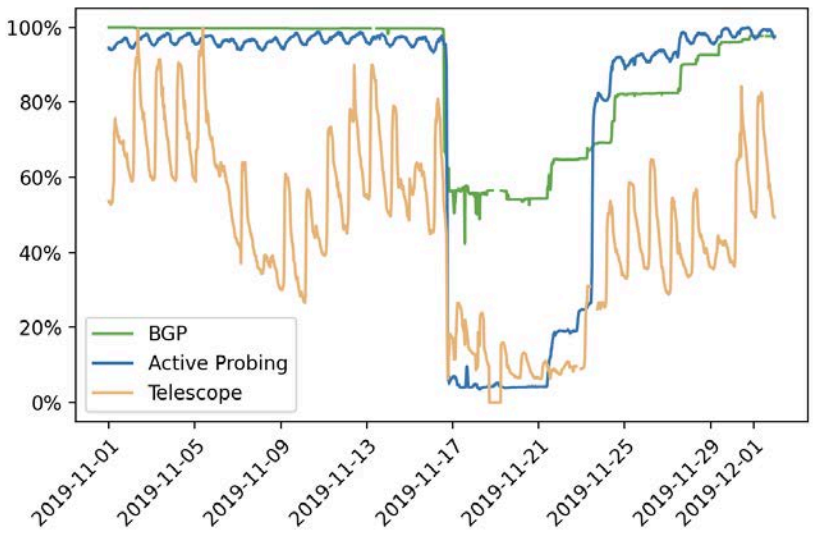


Comparison with past shutdowns

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 four-day 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.

Bloody November: 2019



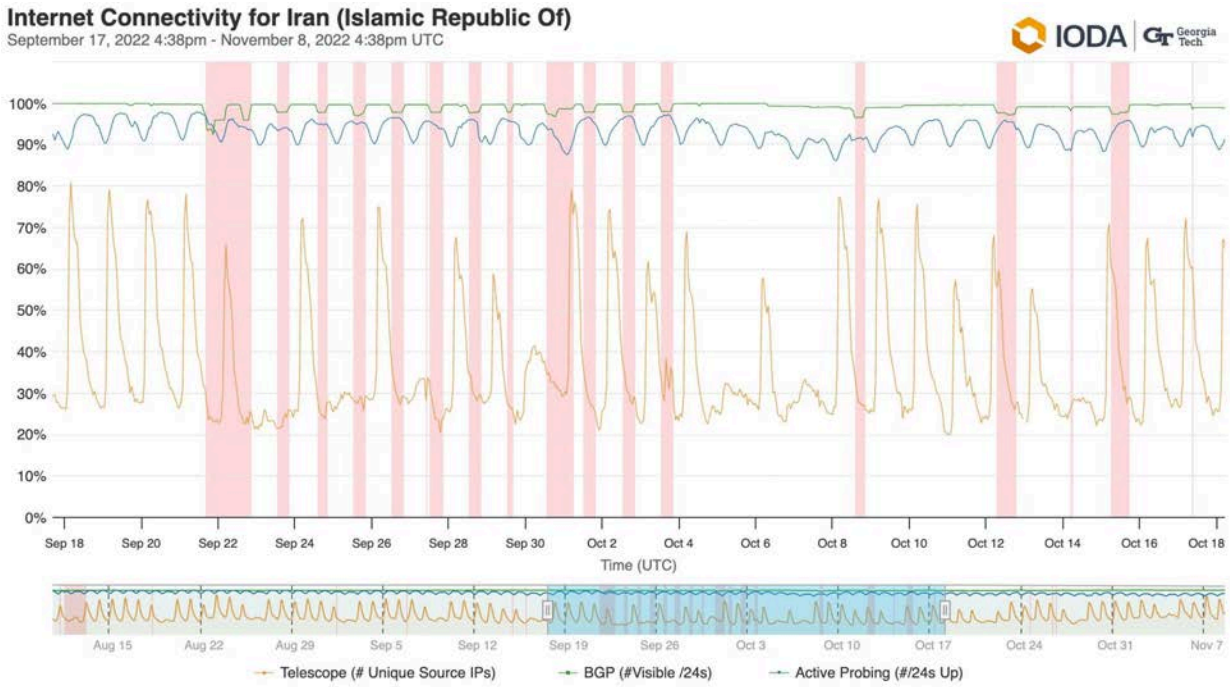
IODA data shows the ~7-day shutdown with all signals impacted

From the evening of November 16, 2019 to the morning of the 21st, Iranians experienced a near complete Internet shutdown. Differences in signal-drop-patterns among the three IODA data sources demonstrate the regime's adoption of diverse disconnection mechanisms and large differences in the timing of their execution by various Iranian Internet Service Providers (ISPs).

A central observation to the 2019 shutdown measurement data is that the primary method of implementation was through the withdrawal of routing announcements. This method is considered "blunt force" because it does not allow for more sophisticated information controls through methods like whitelisting. Censorship measurement groups reported that during the 2019 blackout, most Iranians still had access to the NIN. OONI measurements (which require Internet connectivity) were collected from multiple networks inside Iran between November 16-23, 2019, indicating that the Internet blackout was not total.

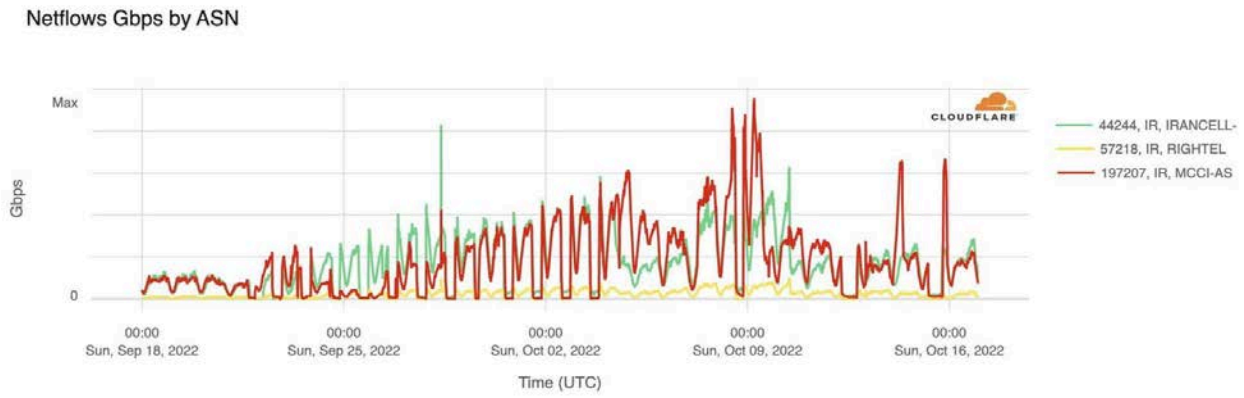
Women, Life, Freedom: September - October 2022

In the wake of the death of Jhina (Mahsa) Amini on September 16, 2022, protests erupted in Iran. With this mobilization came daily shutdowns to Iran's top 3 mobile network providers: Irancell, Rightel, and MCCI. For 13 consecutive days, from September 21 to October 3, 2022, the Iranian government enacted a "digital curfew" by shutting down access to mobile networks from 4:00 PM local time until around midnight. Over the 13 day period, Iranians experienced ~100 hours without access to mobile networks. Mobile networks were again shut down on the 8th, 12th and 15th of October 2022. The drop in connectivity is visible across all IODA signals (Routing Announcements (BGP), Active Probing, Telescope).



IODA data shows nightly curfews affecting mobile connectivity

The Cloudflare Radar graph shows both that traffic on these network providers was disrupted for several hours each day and that traffic was significantly higher than pre-shutdown levels each day once connectivity returned.



Graph showing Cloudflare traffic volumes for Irancell (green), Rightel (yellow), and MCCI (red) between 18th September 2022 and 16th October 2022 (source: Cloudflare Radar).

Additionally, Kentik's data showed increases in traffic on fixed-line services in Iran during the outages of mobile networks (Figure 6), suggesting that a small portion of the Internet traffic lost due to mobile blockages was rerouted over fixed-line services.

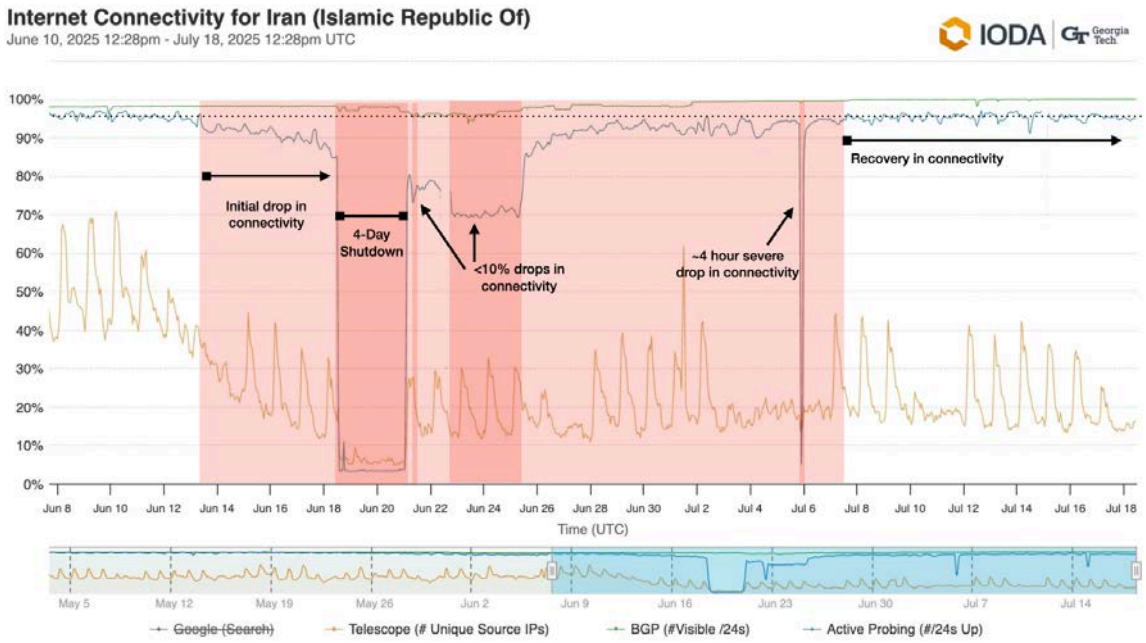
Graph showing Kentik traffic volumes for the Iranian three mobile carriers Irancell (dark green), Rightel (yellow), and MCI (light green) between 18th September 2022 and 5th October 2022 (source: Kentik).

Graph showing Kentik traffic volumes for Iran's largest wireline carrier (TCI, in blue) surging during shutdowns of Iran's largest mobile carrier (Irancell, in green) between 22nd September 2022 and 28th September 2022 (source: Kentik).

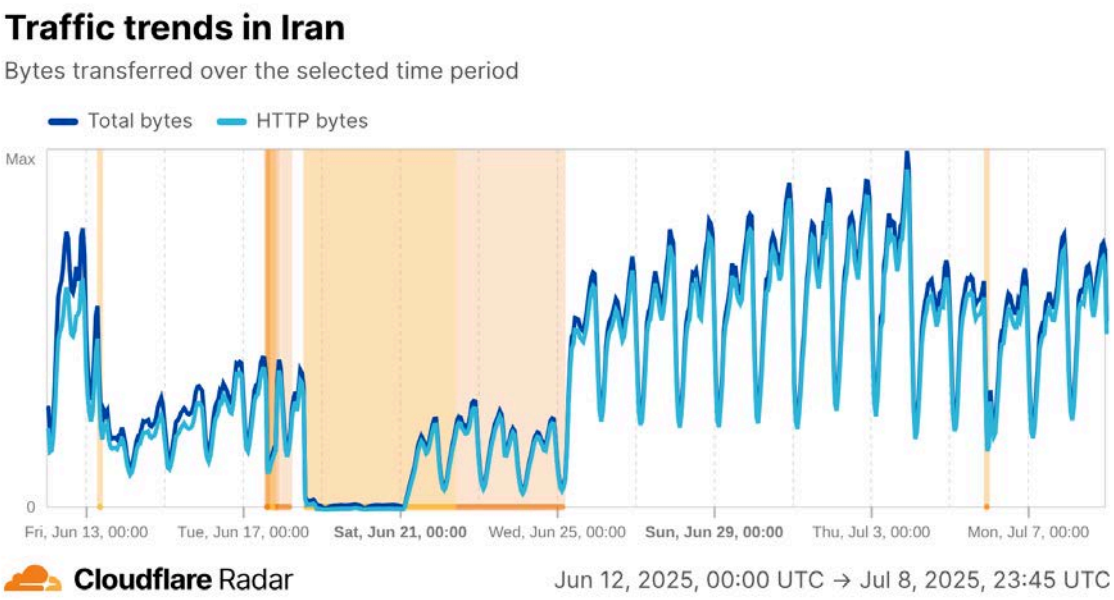
In addition to the above network shutdowns with country-wide scale, IODA data, corroborated by Cloudflare data, demonstrated signs of Internet disruption impacting the provinces of Kurdistan and Khuzestan.

Israel-Iran War: June 2025

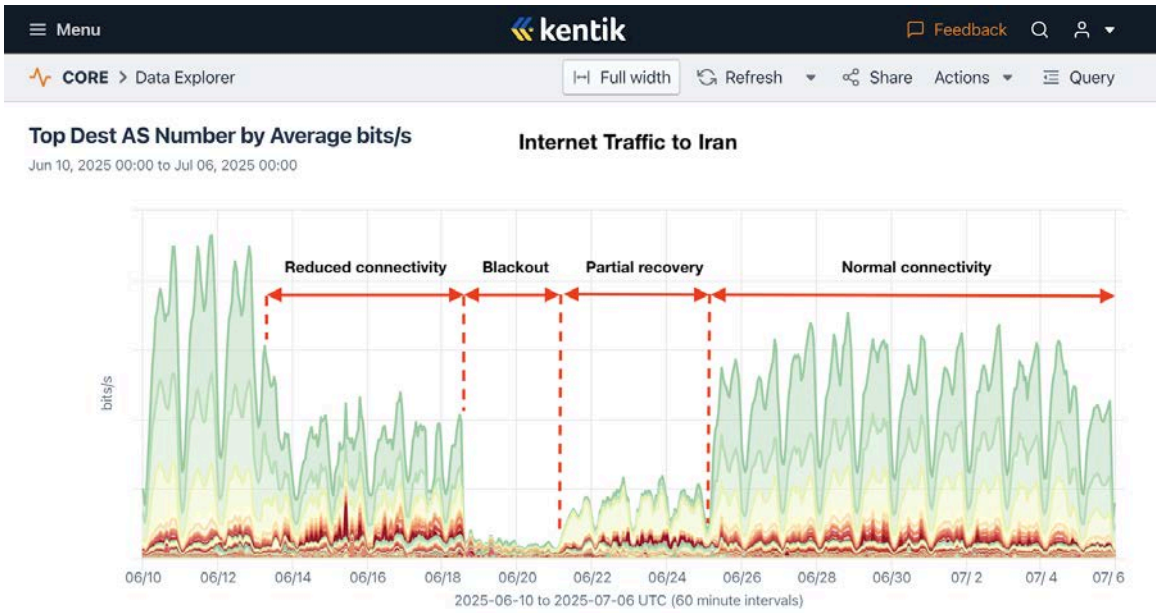
In June 2025, the Israel-Iran War began and IODA observed initial degradation in Internet connectivity that is often present during times of conflict when Internet and power infrastructure is impacted by missile attacks. Beginning on June 18, connectivity across the country plummeted, with Internet traffic dropping by as much as 97%. The Iranian regime shut down the Internet over 4 days and cited national security as the motivation. Unlike the 2019 Bloody November shutdown, Border Gateway Patrol (BGP) or Routing Announcements were not used to implement the shutdown.



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