Farsi Version

Download PDF .PDF

Accessibility

Text Size − 100% +

Related Articles

Network and Policy Monitor

Under Fire: Tighter Communications, Broader Surveillance

April 7, 2026 Filterwatch

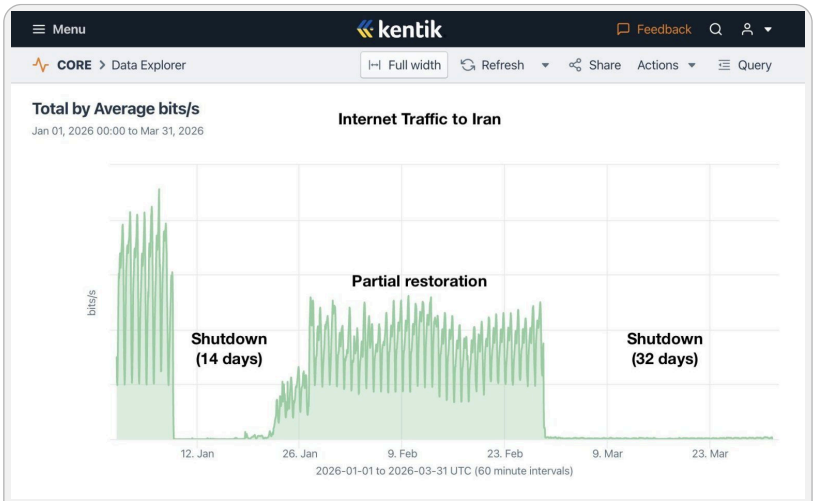
As the shadow of war continues to loom over the country and state control over communications intensifies, this report builds on Filterwatch's previous analysis of the conflict's initial weeks. By examining the escalating internet crisis and heightened security pressures between March 16 and April 1, 2026, we provide a clearer assessment of the government's current trajectory.

During this period, the state's primary focus has shifted toward closing the remaining gaps in global internet access and reviving the "tiered internet" model. These efforts, combined with the visible inefficiency of domestic infrastructure and the deepening socio-economic toll of connectivity restrictions, have further narrowed any remaining prospects for a free and open internet in Iran.

Continued Shutdown and Restriction of Internet Access

More than a month into the conflict, widespread disruptions to international internet access have become a permanent fixture of daily life. When accounting for the earlier shutdowns in January, it is evident that Iran has spent nearly half of 2026 under conditions of either total blackouts or severe, state-imposed restrictions. Data from Kentik highlights the severity of this isolation, showing two distinct periods of total traffic collapse: an initial 14-day shutdown followed by a more prolonged 32-day blackout. Even during periods of "partial restoration," the quality of access remained far

from functional, defined by extreme fluctuations and instability that prevented any reliable connection to the global network.



This chart, based on data from Kentik, shows that international internet traffic to Iran between January and March 2026 experienced two major disruption periods (lasting 14 and 32 days). Recovery between these periods was far from normal, with significant fluctuations and degraded quality of access.

Alongside these targeted restrictions, signs of critical infrastructure vulnerability emerged on the evening of Monday, March 30. Concurrent with reports of power outages at several data centers—including facilities linked to Arvan Cloud—widespread disruptions were reported across data centers operated by HiWeb, Arvan Cloud, Pars Online, Pishgaman, and Asiatech. These failures quickly cascaded into the National Information Network (NIN), leading to complete outages for home internet users on fiber and VDSL connections. The disruption affected the entire online ecosystem, from communication and gaming platforms to specific VPN services and Starlink-based connections that relied on domestic tunneling.

The cause of the outage was initially obscured by conflicting reports. While state media outlets like Fars News Agency first attributed the disruption to shrapnel damage from a Tehran electricity substation, CITNA later reported the origin was domestic and unrelated to enemy attacks. Subsequent internal reports confirmed that power fluctuations at a HiWeb data center led to fires in several server racks, taking all hosted services offline. Despite the severity of the incident, authorities have yet to release an official statement regarding the full extent of the damage or a timeline for restoration, leaving users in a state of prolonged uncertainty.

Infrastructure Breakdown and the Illusion of NIN Resilience

Beyond the physical damage to infrastructure that disrupted the National Information Network (NIN) in late March, field evidence from all three major shutdown periods over the past year reveals that domestic services

consistently buckle under sudden spikes in demand. These failures range from total server overloads to an inability to manage redirected traffic. For instance, just days after international access was severed, platforms like Bale and Eitaa were forced to impose restrictions on file sharing as early as March 3. Simultaneously, basic domestic services—including navigation apps—became largely dysfunctional, suffering from inaccurate location processing, map loading failures, and the total loss of real-time traffic and voice guidance features.

This evidence suggests that the "resilience" of the NIN is less an operational reality and more a state-sponsored narrative built on inflated user statistics. While the government points to massive growth—such as Bale's 159% increase to 28.7 million users, Eitaa's growth to 40.4 million users (a 30.4% increase), and Rubika's 55.5 million monthly active users—this migration is a forced result of international blackouts rather than a genuine preference for domestic tools. Even with the National Smart Government Services Portal reaching 79.4 million users (over 54% increase in users) and the domestic search engine iran.ir seeing 8.7 million visits in March, these platforms remain unable to provide a stable or reliable communication environment during a national crisis.

The Collapse of the Digital Economy and Online Livelihoods

The financial consequences of these prolonged shutdowns have reached catastrophic levels, threatening the very survival of Iran's digital economy. Industry analysts and economic experts estimate daily losses ranging between 400 to 600 billion tomans ($6.7 to $10 million). By the end of January 2026 alone, the cumulative losses were estimated at over 90 trillion tomans ($1.5 billion). This financial hemorrhage is not merely a matter of lost revenue for large firms; it represents a systematic destruction of livelihoods for millions of Iranians who rely on the global internet for their daily work.

The crisis has triggered a massive wave of layoffs across the technology sector, hitting startups, advertising agencies, and game development studios with particular severity. Many businesses that managed to survive previous rounds of filtering now find it impossible to operate under the current conditions of total or near-total isolation. According to the head of the National Union of Virtual Businesses, sales for many online enterprises have plummeted by as much as 80% under these conditions.

Beyond the formal tech sector, the most acute impact is felt in "social commerce." Platforms like Instagram, though heavily filtered, remain the primary marketplace for hundreds of thousands of small, home-based businesses, many of which are managed by women. For these entrepreneurs, the loss of global connectivity is not a temporary inconvenience but a total loss of their only source of income.

The government's refusal to restore stable access, coupled with the proven instability of domestic alternatives, is effectively pushing an entire segment

of the workforce into poverty. Taken together, these factors indicate that the current internet policy is not only a tool of political control but a primary driver of a deepening national economic crisis.

The Return of the Selective and Tiered Internet

As the general public remains largely cut off from the global network, the Iranian government has revived its "tiered internet" model, transforming a fundamental right into a privilege granted only to specific, state-vetted groups. This discriminatory system allows authorities to maintain essential economic and academic functions while keeping the broader population in a state of digital isolation. By centralizing control over who can access the global web, the state effectively uses connectivity as a tool for both surveillance and social management.

Prioritizing Trade over Public Access

During this reporting period, the Tehran Chamber of Commerce announced a new mechanism for its members to regain limited connectivity. Under this arrangement, traders can register for in-person internet access at designated facilities specifically to manage the import and export of essential goods. The process is strictly controlled: all preliminary coordination and registration for this access must be conducted exclusively through the domestic messaging app Bale. This requirement serves a dual purpose, ensuring that even the most vital economic actors are forced into the state-monitored ecosystem while their international communications remain confined to state-controlled physical hubs.

During previous shutdowns in January and February, similar arrangements were implemented in provinces such as Tehran, Bushehr, and Isfahan. However, at that time, due to the absence of a pre-registration system, traders were required to appear in person and wait in long queues to access internet-connected systems on a rotational basis.

Restricted Access for the Academic Sector

A similar model of "geofenced" access has been applied to the academic community, though it has faced significant political and security-related resistance. For instance, when international internet access was briefly and limitedly restored for some universities on March 19, it triggered a sharp backlash from officials. Kamran Ghazanfari, a Member of Parliament, described the restoration as “suspicious” and publicly called for intervention by security agencies.

Despite this opposition, the IT director of Sharif University of Technology announcedon March 27 that limited, controlled international access would be reactivated for faculty members at designated campus locations. However, this access is subject to an incredibly high level of centralized oversight. Faculty requests must be registered through the Ministry of

Science, Research, and Technology's system, and lists of specific IP addresses are then submitted by the Ministry for final approval by higher-level security authorities.

At present, this connectivity is only available in person at specific locations under the university's research office and is strictly reserved for essential tasks. Students with urgent academic needs have no independent access and must coordinate through their professors and the research office to utilize these restricted lines. What underscores the deeply securitized nature of this tiered model are the admissions made by university officials themselves. They have explicitly acknowledged that the implementation phases—and the ultimate decision over when access is enabled or severed—are entirely beyond the control of both the university administration and the Ministry of Science. Instead, connectivity is treated as a tactical resource, dictated by higher-level authorities and subject to fluctuating wartime conditions.

Digital Repression, Intimidation, and Security Campaigns

Alongside the disruption of communication networks, the state has intensified its digital crackdown. ro-government media outlets have published lists labeling circumvention tools such as Psiphon as "malicious applications," urging citizens to delete them. Meanwhile, mass-messaging campaigns have been used to mobilize participation in state-backed campaigns—such as "Janfada" (Devoted to the Homeland). Furthermore, the state has promoted platforms like "Hafeze Ma" (hafezehma.ir), designed to crowdsource the identification of individuals labeled as "enemies" or "traitors."In addition, SMS campaigns have circulated calls to join initiatives such as the so-called "Trump assassination campaign."

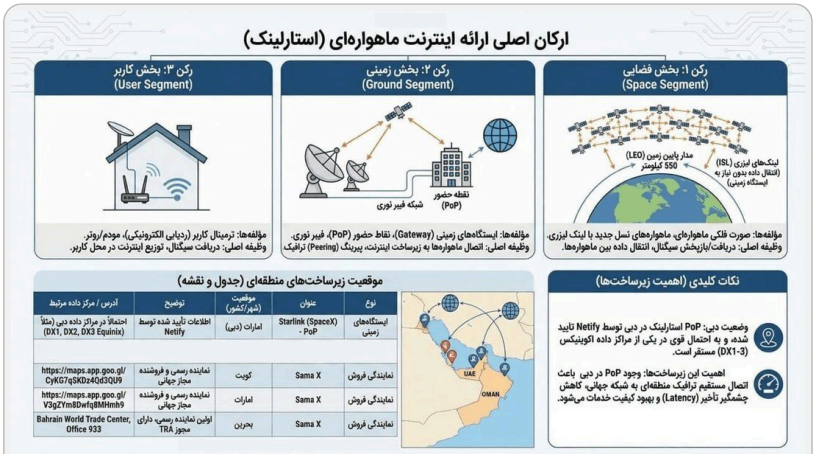
Arrests, Criminalization, and Escalating Enforcement

On the ground, a wave of arrests and judicial actions has accompanied systematic efforts to restrict global internet access. Reports indicate that on March 28, a teacher in Khuzestan was detained solely for using a VPN. As Starlink satellite internet has become one of the few stable connectivity options under wartime conditions, the state has launched an aggressive enforcement campaign against its users and distributors.

The scale of this crackdown is visible in recent provincial reports. On March 26, reports emerged that in Yazd province, 61 bank accounts linked to Starlink users were blocked and six Starlink devices were confiscated. In a separate case, on March 30, Iran's police chief Ahmad-Reza Radan announced that 46 individuals involved in the distribution network of Starlink equipment across 19 provinces had been identified and arrested, with 139 Starlink devices and routers seized. He also stated that, alongside the arrest of 77 individuals described as "pro-monarchy traitors" active online, another 197 individuals

accused of collaborating with “terrorist media” by sharing images of missile strike locations had been detained.

The rhetoric regarding satellite internet has now reached a military level. In a recent move, Fars News Agency published an infographic titled “Key Components of Starlink Satellite Internet Delivery,” which provided a technical breakdown of the system’s user, ground, and space segments. Most alarmingly, the report explicitly labeled Starlink’s regional infrastructure —specifically citing presence in countries such as Bahrain, Kuwait, and the United Arab Emirates —as “legitimate targets” for Iranian intervention. By framing civilian communication tools as part of an enemy's tactical infrastructure, the state is attempting to justify extreme measures of interference and military-grade censorship.



An image published by Fars News Agency outlining the main components of Starlink satellite internet, including the user segment, ground segment, and space segment, along with regional infrastructure locations and key operational notes.

Final Assessment:

The findings and evidence presented in this report paint a clear picture of a multi-layered crisis. Under the shadow of ongoing military conflict, the Iranian government has moved beyond simple content filtering to consolidate a structured, high-tech system of digital repression. Through the expansion of the tiered internet model, the intensification of surveillance, and the active criminalization of alternative connectivity tools like Starlink and VPNs, authorities are reinforcing absolute control over the digital space. This consolidation of power comes at a devastating cost, threatening not only the survival of the digital economy but also the fundamental rights and safety of Iranian citizens.

Tags Digital blackout in Iran | Digital Repression in Iran | Selective Connectivity in Iran | Surveillance and Censorship