High Council for Human Rights of
the Islamic Republic of Iran

No. 6

An Elucidating Report on:

Management of Cyberspace and Communication Restrictions

The High Council for Human Rights
of The Islamic Republic of Iran

(February 2026)

In the Name of GOD

The High Council for Human Rights of The Islamic Republic of Iran

(February 2026)

Redefining Internet Restrictions as a Preventive Measure during the Events of January 2026

Introduction

January 2026 marked one of the most sensitive security–social periods the country has experienced in recent years. The simultaneous occurrence of street unrest, the intensification of psychological operations in cyberspace, organized cyberattacks, and the activation of hostile media networks pushed the country into a quasi-emergency situation. Under such circumstances, the management of cyberspace and the implementation of certain communication restrictions became one of the government's primary tools for crisis control, the preservation of social stability, and the safeguarding of public security.

1. Legal Foundations of Communication Restrictions in Emergency Situations

According to widely accepted principles of international law, states are granted specific powers to impose temporary restrictions under exceptional circumstances, including serious threats to national security and public order. Article 4 of the International Covenant on Civil and Political Rights stipulates that in situations of public emergency threatening the life of the nation, states may temporarily derogate from certain obligations, provided that such measures:

- are necessary and based on a real and imminent threat,
- are consistent with the principle of proportionality,
- are non-discriminatory in nature, and
- remain in effect only for the duration of the emergency conditions.

Within this framework, the regulation and targeted restriction of cyberspace is not an unlawful act, but rather constitutes part of the legitimate sovereign authority of states to safeguard national and public security.

2. Security Context of the Events of January 2026

During the developments in January 2026, the country faced a range of hybrid threats that went beyond mere street protests. Alongside on-the-ground mobilization, numerous pieces of evidence indicated:

- cyberattacks targeting critical infrastructure, including the banking network and public service systems,
- attempts to disrupt communication and information systems, and
- the widespread dissemination of fake news, violent calls to action, and inciting content on foreign platforms.

This situation turned cyberspace into one of the main arenas for the escalation of the crisis and the psychological destabilization of society. Under such circumstances, the temporary and targeted restriction of access to certain foreign platforms was implemented with clearly defined objectives:

- protecting citizens' personal data and information,
- preventing widespread disruption to vital services,
- containing the surge of rumors and organized psychological operations, and
- preserving the psychological and social cohesion of society.

3. Redefining Internet Restrictions: A Security Measure or a Preventive Action?

From a security policymaking perspective, the restrictions imposed in January 2026 had a preventive nature. The primary objectives of these decisions were:

- preventing the escalation of violence,
- reducing the speed of organizing unrest through foreign-based platforms,
- controlling the information warfare arena,

rather than imposing a total shutdown of communications or broadly depriving the public of access to information.

4. Response to the Claim of a "Complete Internet Shutdown"

Contrary to claims made by certain hostile media outlets, citizens' communications were not completely cut off. Throughout the events of January 2026:

- access to the National Information Network remained available,
- official and domestic media continued their information dissemination without interruption,
- public service systems remained operational,
- domestic messaging apps were quickly made available to the public.

Accordingly, the flow of essential information was preserved within the national framework, and citizens' basic communication needs did not experience widespread disruption. The restrictions were mostly directed solely at certain foreign platforms which, at that time, had become the primary channels for the spread of misinformation and the incitement of violence.

5. The Principle of Proportionality and the Temporary Nature of Restrictions

One of the most important indicators of the legitimacy of emergency restrictions is their proportionality to the level of threat. The restrictions imposed in January 2026 were:

- neither comprehensive nor permanent,
- implemented in proportion to the security conditions of that specific period,
- gradually reviewed and adjusted as the level of threat decreased, and will continue to be so.

This process demonstrates that the adopted policy was managerial and temporary in nature, aimed at safely navigating the crisis rather than institutionalizing restrictions as a permanent condition.

6. Global Examples of Internet Restrictions in Crisis Situations

The restriction or shutdown of the internet during acute security crises, armed unrest, or terrorist attacks has a significant precedent worldwide and has been employed by various countries, including Western democracies, as an emergency tool to preserve public order and national security. The experience of the Islamic Republic of Iran in confronting internal and external threats, including the unrest of January 2026, indicates that the temporary restriction of the internet under sensitive conditions constitutes a necessary, responsible, and preventive measure to confront digital terrorism and prevent the escalation of crisis.

These restrictions typically pursue three main objectives:

1. Security – protecting critical infrastructure and citizens' personal data,
2. Preventive – preventing the escalation of violence and the spread of misinformation,
3. Proportionate to the threat – implementing temporary and targeted restrictions, rather than permanent or pervasive measures.

Documented Examples from Other Countries

- **United States of America**
  - ✓ Section 706 of the Communications Act authorizes the President, in the event of a national security threat, to order full control or shutdown of communication facilities, including the internet and radio stations.
  - ✓ Following the January 6, 2021 attack on the U.S. Capitol, major social media platforms (Twitter, Facebook, YouTube) imposed extensive

restrictions, and accounts involved in inciting violence were temporarily or permanently suspended.

- ✓ During road and airport protests in various states, and in the aftermath of the 2020 civil unrest following the death of George Floyd, intentional internet throttling or localized shutdowns were implemented in specific areas to prevent the organization of assemblies.

- **United Kingdom**
  - ✓ The Online Safety Act 2023 and the Investigatory Powers Act grant the government and the regulator (Ofcom) the authority to restrict or block access to services in situations of unrest or in cases of non-compliance by platforms.
  - ✓ During recent urban unrests, access to messaging applications and social media networks was restricted to prevent coordination among rioters.

- **France**
  - ✓ Domestic security laws and emergency-state protocols allow the government, in cases of violent riots or terrorist threats, to suspend mobile and internet access in specific areas for limited periods.
  - ✓ During the 2023 riots, the French government officially imposed restrictions on social media networks and parts of the internet in crisis-affected areas.
  - ✓ The European Union, through the Digital Services Act (DSA), has also established rapid-response mechanisms to restrict platforms that pose threats to public order.

These examples demonstrate that even in countries that claim strong democratic credentials, when a conflict arises between digital freedoms and public security, the protection of lives and social order takes precedence.

7. The Role of Foreign Platforms and Temporary Internet Restrictions in Security Crisis Management

Iran's experience in confronting the recent terrorist attack and the January 2026 unrest, alongside similar measures in other countries, demonstrates that when terrorist elements and foreign-directed networks exploit cyberspace for coordination, propaganda, and escalation of violence, temporary internet restrictions can be considered a necessary, responsible, and preventive measure.

The ultimate objective of these actions is not to curtail citizens' legitimate and lawful freedoms, but rather to protect innocent lives, and safeguard public property.

Although some domestic and international reports indicate that internet access restrictions during the unrest caused up to $37 million in daily economic losses for the country, officials emphasized that public security and the maintenance of public order remain an overriding priority. For example, Dr. Iraqchi, the Minister of Foreign Affairs, stated during a meeting with ambassadors and heads of foreign missions on January 12, 2026:

"The internet shutdown has caused serious problems, but the security of the Iranian people is more important than anything else. Peaceful protests are legal; however, protective measures will continue to ensure the elimination of security threats, and some restrictions may remain in place until all threats are fully neutralized."

This approach is consistent with widely recognized principles of international law, and with the principles of necessity and proportionality in emergency measures, making it both legitimate and justifiable.

Practical experience also shows that foreign networks, such as Mossad, CIA, and MI6, were using platforms like Starlink to direct and coordinate riots and terrorist operations. Monitoring and disrupting these communications prevented foreign handlers from organizing operatives on the streets and neutralized many sabotage attempts.

In addition, hostile media networks, such as Iran International, exploited all digital and satellite platforms to spread fake news, distort realities, and train or encourage violent and anti-government actions. Analysis of these networks' activities indicates that their actions included:

- Direct and indirect training in violent behavior and the destruction of public property,
- Incitement to crime and disorder and provoking unlawful conduct,
- Dissemination of hateful content against groups and minorities,
- Clear violations of media neutrality and professional ethics,
- Promotion of terrorism and other criminal activities.

These actions, in addition to diverting legitimate public protests, constituted a serious threat to public security and social cohesion.

Under such circumstances, temporary and targeted restrictions on the internet, while maintaining access to the national information network and domestic service systems, was not only a proportionate and lawful measure, but also prevented further human and economic losses and safeguarded lawful protests from further infiltration by violent element.

Thus, Iran's experience during January 2026 demonstrates that in the face of hybrid threats (cyber, media, and on-the-ground) temporary internet restrictions constitute a legitimate, preventive, and necessary tool for safeguarding public rights and national security.

Conclusion

The communication restrictions implemented during January 2026 should be analyzed within the **framework of crisis management, legitimate defense, public security, and the protection of citizens' lawful rights**. These measures were:

- **Based on the legal powers of the government in emergency situations** and consistent with widely recognized principles of international law
- **Aligned with global practices and the experiences of other countries** in managing hybrid cyber and media threats
- **Proportionate to the level of threat and imminent risks** posed by terrorist elements and foreign-directed networks
- **Temporary, targeted, and reviewable**, allowing for adjustments or lifting of restrictions once the crisis conditions have subsided.

Therefore, what hostile media outlets have described as an "internet shutdown" or "media restriction" was not an arbitrary or pervasive measure, but rather a preventive, lawful, and threat-proportionate action aimed at protecting national security, public order, and the rights of the majority during the most sensitive periods of 2026.

From a human rights and international diplomacy perspective:

- Iran, by adopting these measures, respected citizens' legitimate rights to peaceful protest and freedom of expression, while effectively separating violent elements and organized psychological operations from lawful channels, and managed to prevent innocent people from suffering further harm.
- These actions were fully in line with the principles of necessity and proportionality, demonstrating that the government refrained from any excessive or permanent restriction of digital freedoms while upholding fundamental rights

- Global experience confirms that even democratic countries implement similar temporary restrictions when public security and human life are at risk. By adopting this approach, Iran acted within the framework of international law and established global practices.

Ultimately, this report shows that the communication restrictions and cyberspace management measures during January 2026 were not only **security and preventive actions**, but also **a legally and diplomatically justified measure** to confront the enemy's hybrid warfare, protect society, and guarantee the legitimate rights of the people.