

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	1140
Land:	Iran
Kilde:	Freedom House
Titel:	Freedom on the Net 2024 – Iran
Udgivet:	16. oktober 2024
Optaget på baggrundsmaterialet:	7. november 2024



FREEDOM ON THE NET 2024

Iran

NOT FREE

12

/100

A. <u>Obstacles to Access</u>	7 / ₂₅
B. <u>Limits on Content</u>	4 / ₃₅
C. <u>Violations of User Rights</u>	1 / ₄₀

LAST YEAR'S SCORE & STATUS

11 /100

Not Free

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.



Key Developments, June 1, 2023 – May 31, 2024

Internet freedom remained highly restricted in Iran during the coverage period. The regime has taken steps to make access to the global internet more cumbersome and expensive, and drive users to a domestic version of the internet where authorities can more effectively control content and monitor users. The regime also employs extensive censorship, surveillance, content manipulation, and extralegal harassment against internet users, making Iran's online environment one of the world's most restrictive.

- Authorities instructed internet service providers (ISPs) to increase their prices between 30 and 40 percent, making access significantly more expensive (see A2).
- While localized internet shutdowns continued throughout 2023, there were fewer reports of deliberate connectivity disruptions in the second half of the coverage period (see A3).
- In February 2024, the Supreme Council for Cyberspace (SCC) prohibited the use of unlicensed virtual private networks (VPNs) and pushed users seeking to access blocked or filtered web content to use domestic circumvention tools (see B1, B7, and C2).
- In September 2023, the Hijab and Chastity Bill was enacted, which introduces a range of punishments for women who appear in public, both online and offline, without a hijab (see B8 and C2).
- Several online users were handed multiyear prison sentences, and several people received death sentences, in connection with their online content (see C3).

Political Overview

The Islamic Republic of Iran holds elections regularly, but they fall short of democratic standards, including due to the influence of the hard-line Guardian Council, an unelected body that disqualifies all candidates it deems insufficiently loyal to the clerical establishment. Ultimate power rests in the hands of the

country’s supreme leader, Ayatollah Ali Khamenei, and the unelected institutions under his control. These institutions, including the security forces and the judiciary, play a major role in the suppression of dissent and other restrictions on civil liberties. Iranian authorities have maintained a protracted crackdown after the antigovernment “Woman, Life, Freedom” protests, which were sparked by the 2022 death of Jina Mahsa Amini at the hands of the morality police. President Ebrahim Raisi was killed in a helicopter crash in May 2024, and Masoud Pezeshkian succeeded him as Iran’s next president after snap elections held in July 2024.

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	5/6
---	------------

Internet penetration, bandwidth, and speeds have slowly improved in recent years due to government investment in information and communication technologies (ICTs). However, the expansion of the National Information Network (NIN)—the country’s domestic internet architecture—has enabled the regime to deliberately restrict internet access (see A3).

Nevertheless, Iranians still face poor broadband and mobile connectivity quality and slow speeds, as well as increasing prices and network disruptions (see A2 and A3). **1** Internet penetration stood at 81.7 percent and there were 73.1 million internet users and 146.5 million mobile connections in Iran as of January 2024. **2** Fixed-line broadband connections remained significantly slower than mobile speeds. As of May 2024, the median mobile and fixed-line broadband download speeds were 37.36 megabits per second (Mbps) and 15.28 Mbps, respectively. **3**

When the late president Ebrahim Raisi came to power in 2021, the ICT Ministry made the development of the NIN a main priority in order to reduce Iran’s dependence on the global internet and limit user access to international content.

4 The ICT ministry has since encouraged Iranians to migrate to the domestic internet infrastructure by decreasing bandwidth and increasing prices for international internet services (see A2 and A3). **5** Following Raisi’s death in May

2024, candidates for his replacement also stressed their commitment to investment in Iran’s domestic internet infrastructure. ⁶

Amid economic difficulties, several NIN-related infrastructure projects and investments have been announced in recent years. ⁷ In early 2024, the Ministry of Communications and Information Technology (ICT Ministry) received a 25 percent budget increase to continue to advance the NIN and specifically to expand the country’s domestic internet while minimizing reliance on the international internet. ⁸ In September 2023, Issa Zarepour, the ICT Minister, said that fiber-optic coverage via the NIN would reach 75 percent of users by early 2024. ⁹ However, statistics related to NIN progress have been disputed by digital rights groups in the past. ¹⁰

The use of satellite internet in the form of very small aperture technology (VSAT) is only used by state-regulated and -licensed ISPs like Pars Online. ¹¹ In June 2023, authorities put out a general call to local companies to apply for satellite internet licenses with the Communication Regulatory Authority (CRA). ¹² In December 2023, the Iranian government signed a contract with Yahsat, a UAE-based company to provide satellite services in Iran. ¹³

Starlink began providing satellite-based services in Iran shortly after the Woman, Life, Freedom protests broke out in September 2022, allowing citizens a degree of internet access independent from Iran’s government-regulated telecommunications infrastructure. ¹⁴ In May 2023, authorities filed a complaint with the International Telecommunication Union (ITU), requesting that Starlink comply with the regime’s regulations and licensing requirements (see A4). ¹⁵ In July 2023, ITU ruled that Starlink lacked a license as required by Iranian law. ¹⁶ In March 2024, the board called for Starlink to dismantle its infrastructure in Iran. ¹⁷

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?

1/3

Inflation and price increases in recent years have resulted in high costs for internet users. In December 2023, authorities instructed ISPs to increase their prices between 30 and 40 percent, reportedly to help keep up with rising inflation.

18 However, some internet service providers (ISPs) increased their prices even more. **19** For example, the cost of packages from Hamrahe Aval, a mobile service provider, increased from 2,000 rials (\$0.05) to 6,000 rials (\$0.14) for one gigabyte (GB) of data. **20**

The urban-rural divide has decreased in recent years as authorities have invested in better connectivity in rural areas, though pricing remains high. For Iranians to access the international internet they must purchase virtual private networks (VPNs), the prices of which have increased significantly as the regime continues to filter and censor online content. **21**

Users continue to rely on cheaper mobile internet packages over fixed-line broadband offerings. **22** As of September 2023, the cost of a monthly fixed-line broadband internet package was approximately \$10.69. Packages with faster speeds or more data cost as much as \$70.29 a month. **23** One GB of mobile data can cost up to \$10.65. **24** For comparison, Iran's gross national income (GNI) per capita was \$18,130 in 2022, according to the World Bank. **25**

Internationally routed traffic—downloads or uploads of global internet content—is priced at a higher rate than domestically hosted websites (through the NIN) and other government-approved content (see B7). **26** This policy also discouraged the use of VPNs by effectively making them more expensive to use. **27** In February 2024, the SCC officially prohibited the use of VPNs without obtaining a license, after criminalizing the sale and distribution of these tools earlier in 2023 (see C2).

28

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	1/6
--	-----

Score Change: The score improved from 0 to 1 because there were fewer internet shutdowns during the coverage period than in previous years.

Localized internet shutdowns are often used to immobilize protests, to which authorities often respond with excessive force. Furthermore, Iran's internet governance is highly centralized, which allows authorities to easily restrict connectivity. **29**

Beginning in September 2022, authorities implemented multiple localized and widespread internet shutdowns and mobile disruptions, in an effort to quell massive antigovernment protests sparked by the death in custody of Jina Mahsa Amini (see B8). **30** Authorities also blocked access to WhatsApp and Instagram and filtered VPNs and proxy servers (see B1). **31** For nearly all of 2023, authorities restricted internet and mobile service in several provinces every Friday, typically around protests that followed the day's prayers. **32**

Shutdowns occurred at least once a month for the first half of this report's coverage period, often in Zahedan County in Sistan and Baluchestan Province. The shutdowns similarly tended to occur during antigovernment protests following Friday prayers. In November, several more extensive shutdowns impacting both fixed and mobile internet took place across Iran. **33** For example, according to data from the Georgia Institute of Technology's Internet Outage Detection and Analysis (IODA) project, on November 20, shutdowns occurred across 28 Iranian provinces. **34** Weekly disruptions occurred through January 2024 and then seemed to stop in early February. Moderate, localized disruptions took place in April 2024, **35** but the pattern of weekly internet shutdowns tapered off toward the end of the coverage period.

During the previous coverage period, researchers found that the Communication Regulatory Authority (CRA) used SIAM technology to throttle mobile service on individuals' phones. **36** SIAM is a program that allows service providers to remotely manipulate and downgrade cellular connections at the CRA's direction. SIAM has also reportedly been used by authorities to surveil individuals via geolocation data collected by mobile service providers (see C5). **37**

Outside of deliberate connectivity restrictions, users have reported a deterioration of the internet-service quality and bandwidth as authorities continue to build up the NIN and cut Iran off from the global internet. The Telecommunication Infrastructure Company (TIC) retains a monopoly on internet traffic flowing in and out of the country. **38** In October 2021, local news agencies started reporting a shortage in international bandwidth due to the SCC's refusal to grant new licenses to ISPs for international connections via the TIC, while previous licenses expired with no renewals. **39**

Through the NIN, authorities have been taking steps to roll out a “layered” or “tiered” internet structure, where specific groups of people will be able to access the international internet while the rest are left with the domestic network. ⁴⁰ Implementation would expand the government’s censorship and surveillance capabilities as much of the population would be forced to use domestic apps and platforms that offer weak privacy and security features (see C5). ⁴¹

Iran’s Internet User Protection Bill (IUPB), which includes provisions that facilitate government-ordered censorship and surveillance and was partially implemented during the previous coverage period despite having not been approved by the parliament, will further centralize Iran’s internet backbone under the government (see B3). ⁴² Article 3 of the bill gives the Supreme Regulatory Commission (SRC), a body within the SCC, the power to set bandwidth limits and manage access to the international and domestic internet. ⁴³ Rights organizations, such as Article 19, have expressed concern about the disproportionate impact the bill could have on marginalized populations like LGBT+ people, who heavily rely on the international internet to access information and connect with their community.

44

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	0 / 6
---	--------------

The government tightly controls the telecommunications industry. The TCI owns the Data and Communication Company (DCC), the country’s main ISP. The Mobile Telecommunication Company of Iran (MCI), a subsidiary of the TCI, is the largest mobile service provider. ⁴⁵ The second-largest mobile service provider, MTN Irancell, is owned by MTN, a South African telecommunications company, and Iran Electronics Industries, a state-owned subsidiary of the Defense Ministry. ⁴⁶

The CRA, which operates under the ICT Ministry, regulates the telecommunications sector and is responsible for issuing licenses to service providers. Telecommunications companies are required to register with the ICT Ministry and must comply with CRA rules and regulations. For example, all telecommunications providers must provide the CRA with direct access to their

networks and comply with government censorship and surveillance requests (see C6). **47**

ISPs in Iran can face steep financial penalties for not complying with government censorship orders and must install content filters and other censorship software. ISPs have been shut down or stripped of their licenses for failure to install content filters. **48**

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

0 / 4

Iran's telecommunications regulators are beholden to the authorities. The SCC, which sets most internet-related policy, was established through a 2012 decree by the supreme leader; 17 members come from government institutions, while the supreme leader appoints 10. **49** The SCC is meant to provide a centralized point for policymaking and the regulation of Iran's virtual space, effectively minimizing the roles of the executive, legislative, and judicial branches and bringing internet policy under the supreme leader's direct control.

In February 2024, the SCC issued a VPN ban. Some analysts have criticized the move, saying that the body overstepped its authority by criminalizing not only the distribution and sale, but also prohibiting the usage, of VPNs. **50**

The CRA is responsible for regulating the telecommunications sector and its head is appointed by the ICT minister. **51** Its decisions pertaining to website blocking, internet cuts, and surveillance often lack transparency and accountability. **52** In January 2023, the ICT minister made several changes to the Regulatory Commission at the CRA, such as removing a private-sector representative and including new members from the SCC, the Information Technology Organization, and Iran's Post Services. **53**

The decisions to implement internet shutdowns have no clear legal framework and are considered national security decisions directed by the Supreme National Security Council (SNSC). **54** However, there is much ambiguity over where decisions originate within the multiagency SNSC. **55** Connectivity cuts are then

implemented by the ICT Ministry, which oversees ISPs. Requests for copies of the SNSC's shutdown orders Article 19 made in 2020 were refused. **56**

B. Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	0 / 6
--	--------------

Authorities restrict access to thousands of websites, particularly those of international news and information services, **57** the political opposition, and human rights groups, **58** as well as sites that address ethnic and religious minority groups in Iran and LGBT+ rights. **59** Websites are also blocked if they contradict state doctrine regarding Islam or government narratives on domestic or international politics.

The Commission to Determine the Instances of Criminal Content (CDICC) is headed by the prosecutor general and consists of representatives from 12 state institutions. Article 749 of the penal code requires all ISPs to filter content determined by the CDICC to be criminal. Resistance in complying with this article can result in the termination of the ISP or in some cases a financial penalty. **60**

The IUPB, parts of which were implemented during the previous coverage period, requires international technology companies to open offices within Iran and comply with Iranian authorities' censorship requests or risk blocking (see B2 and B3). **61**

Facebook, SnapChat, TikTok, X, and YouTube are all blocked or filtered, as are major blog-hosting platforms, the navigation app Waze, the audio discussion app Clubhouse, and the messaging apps Viber, Telegram., and Signal. **62** Instagram and WhatsApp, the only international platforms that remained accessible in Iran prior to September 2022, were blocked amid the nationwide Woman, Life, Freedom protests. **63**

Other foreign platforms including video gaming software, Skype, and PayPal remained blocked or filtered during the coverage period. **64** The Google Play

store and Apple's app store were filtered in September 2022. After a month of filtering, authorities unfiltered the Apple app store, although users still report issues accessing the site. ⁶⁵ As of June 2024, Google Play remained blocked; ⁶⁶ over 90 percent of mobile phone users in Iran use devices powered by Google's Android operating system, which distributes apps with Google Play. ⁶⁷

Domestic news sites are frequently blocked for hosting material that is critical of the government. In March 2022, the reformist Emtedad news outlet was blocked per a decision by the CDICC. According to some reports, the website did not have a license from the Culture Ministry, ⁶⁸ but the outlet's chief editor claimed they had been given no prior notice about the action. Anar Press and Aban Press were blocked after the chief editor of both sites was arrested in April 2019. ⁶⁹

Authorities employ a centralized filtering system that can effectively block a website across the entire network within a few hours. Private ISPs are forced to either use the bandwidth provided by the government or route traffic through government-issued filtering boxes with blocking capabilities. This method only limits access to content retrieved through unencrypted Hypertext Transfer Protocol (HTTP) connections. Individual pages remain available via encrypted HTTPS connections, which disguise banned text, requiring censors to block the entire site in order to restrict access to specific content. ⁷⁰

Many Iranians rely on VPNs to access international services and content blocked by authorities. However, the regime began blocking various proxy servers and VPNs amid the Woman, Life, Freedom protests. ⁷¹ Circumvention tools such as Nord VPN, Proton VPN, and TunnelBear were all inaccessible during the coverage period. ⁷² During the coverage period, the SCC issued a resolution prohibiting the use of all unlicensed VPNs (see C2). ⁷³ This development is in line with a long-term policy of forcing Iranians onto domestic services and platforms and restricting Iranian's access to blocked or filtered content (see B7). ⁷⁴

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?

0 / 4

Authorities frequently employ administrative measures to force the removal of legitimate online content.

Website owners must register their sites with the Culture Ministry and are then subject to requests to remove posts deemed unacceptable by the government (see B6). **75** The 2009 Computer Crimes Law (CCL) makes content hosts responsible for any content that appears on their sites. **76** This has led to the suspension of blogs and the shuttering of news sites hosted on platforms inside Iran.

Under an August 2019 order, internet hosting companies inside the country are banned from providing services to filtered websites and can face prosecution for doing so. **77** The affected sites include those carrying news and information about human rights or other politically relevant content, which are forced to rely on international hosting companies or shut down entirely.

According to FilterWatch, a website that tracks digital rights abuses in Iran, at least 70 Instagram pages were taken down for publishing content that authorities deemed to be “inciting chaos” between July and September 2023. **78** For example, the Instagram page of Rasoul Khadem, a popular wrestler, was removed after Khadem posted a commemoration of the anniversary of Jina Mahsa Amini’s death. **79** In March 2024, over 40 Instagram accounts were blocked by authorities, including a popular account that shared videos of an elderly man singing and dancing. **80**

The IUPB, parts of which were quietly enacted during the previous coverage period, requires foreign and domestic online platforms to register with a supervisory board and comply with Iranian content-removal laws or face penalties, including blocking or throttling, or be replaced with “domestic alternatives” (see B1 and B6). **81** The law makes companies responsible for removing content deemed inappropriate under Iranian law. **82**

Authorities often coerce detainees, specifically those involved in protests, to remove content from their social media accounts. For example, in September 2022, musician Shervin Hajipour was arrested and authorities forced him to remove his song “Baraye,” which had become an anthem during the Woman, Life, Freedom protests, from his Instagram page. **83** The Islamic Revolutionary Guard

Corps (IRGC) commonly arrests Telegram group administrators and coerces them to remove content or delete their channels (see C3). **84**

Authorities frequently request that outlets or social media platforms take down content, often providing no justification for the decisions.) **85** Separately, according to the British Broadcasting Corporation (BBC), two Persian-language content moderators at Instagram claimed that they were offered bribes to delete the account of Masih Alinejad, a prominent US-based Iranian American activist, in May 2022 (see C7). **86**

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?

0 / 4

The CDICC is responsible for making censorship decisions, which are often arbitrary and lack transparency. Other bodies, such as the judiciary and the SNSC, have also ordered filtering decisions, such as the ban on Telegram (see B1). **87** Such decisions are ostensibly based on the 2009 CCL, which outlines a broad range of banned content, from insulting religious figures and government officials to distributing pornographic content and using illegal circumvention tools. **88**

During the previous coverage period, reports emerged that the SCC had quietly ushered in parts of the IUPB, bypassing the legislative process as the bill had not been approved by the parliament. In September 2022, the SCC announced that a 12-member commission, including members of the IRGC, the Intelligence Ministry, and the judiciary, had been given authority to regulate the online space (see A3). This new commission, known as the SRC, and its responsibilities were key provisions of the IUPB, and this announcement was seen as evidence that some parts of the bill had been enacted. **89**

During the coverage period, Meta removed Instagram and Facebook accounts belonging to Ayatollah Ali Khamenei following criticism of his support for Hamas in the wake of the group's attack on Israel in early October 2023. **90** Meta, based in Menlo Park, California, offered no specifics about its reasoning. However, it said it removed the accounts "for repeatedly violating our Dangerous Organizations and Individuals policy." **91** Previously, in 2022, Khamenei's Twitter account was suspended. **92**

Decisions by social media companies to remove Iranian content at times lack transparency. Amid the Woman, Life, Freedom protests, which continued into the coverage period, Meta continued to remove some protest-related content. **93** Other complaints of the platform censoring dissident content without reason occurred during the coverage period. **94**

In late September 2022, as protests sparked by the death in custody of Jina Mahsa Amini began, the US Treasury Department issued a general license to allow software and communications tools to be exported to Iran outside of sanctions. Several platforms and services, including Google Maps and Google Meets, became accessible within Iran during the previous coverage period. **95** In May 2024, the US officially codified these sanctions exceptions so that Iranians can continue to access certain American internet and communications services. **96**

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	1 / 4
--	--------------

Self-censorship among internet users is extensive, particularly regarding political issues or government criticism. The amount of original content fell significantly after the 2009 crackdown on protests linked to that year's disputed presidential election, with many journalists and bloggers abandoning their online activities. However, the Woman, Life, Freedom protests have ushered in an unprecedented level of critical speech, both online and offline, from activists, human rights defenders, and ordinary citizens. **97**

Beginning in September 2022 when nationwide antigovernment protests began, Iranians—many of whom had long refrained from criticizing the government—took to social media and other online platforms to condemn the death in custody of Jina Mahsa Amini, criticize the government's crackdown on demonstrations, and call for regime change (see C2). **98**

During the coverage period, Iranian internet users continued to speak online about Hamas's attack on Israel in October 2023 and the resulting war in Gaza. This kind of speech continued even after the IRGC issued a directive criminalizing online support for Israel and urging users report such speech. **99**

Iranian women also advocate for their rights online during the coverage period, **100** under the slogan “Woman, Life, Freedom.” **101** Numerous women shared photos or videos of themselves unveiled online, protesting the country’s repressive mandatory hijab legislation (see C2). **102**

While Amini’s death and the resulting demonstrations sparked a wave of critical speech online, the risks facing those who participate in this online dissent remain high. Multiple women were arrested for their antigovernment speech online, or for appearing unveiled in online photos or videos during the coverage period (see C3). **103** In addition to the arrests, harassment, and executions carried out by the regime, Iran’s cyberpolice, known as FATA, have charged internet users with “insults and slander” or “spreading disinformation” for their critical online content. **104**

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?

0 / 4

The Iranian regime frequently partakes in media manipulation and counters online criticism through an extensive digital propaganda apparatus. The media environment is tightly controlled by the state, and the IRIB serves as a vehicle for state-sponsored content manipulation. **105** The X account of state-affiliated *Iran Newspaper*, which has over 153,000 followers, frequently posts false or misleading information that paints the regime in a positive light. **106** Progovernment online media outlets frequently spread hateful disinformation about Iran’s minority communities, including Baha’is, Kurds, and Iranian Arabs. **107**

Ahead of parliamentary elections in March 2024, the Kayhan outlet, which is known for its close ties to conservative politicians, published articles accusing the opposition of attempting to manipulate the results. **108** Ahead of snap presidential elections in June 2024, a high level official argued that the regime should use AI to “influence voters” and “shape public opinion” ahead of the vote. **109**

State-affiliated media accounts and Iranian officials also spread misleading information online in the wake of President Ebrahim Raisi’s death in May 2024. **110** In the wake of the helicopter crash that killed him, one social media analysis

showed that 22 percent of the accounts discussing the accident on X were fake, and that these accounts pushed out misleading narratives. **111**

The regime has a long history of manipulating content, both online and offline, which has increased with the rise of social media. **112** The state has sponsored networks of inauthentic social media accounts to spread propaganda, **113** and has openly boasted about its “cyberbattalions,” which are active in pushing progovernment narratives on X. **114** In the first few weeks after Hamas’s attack on Israel on October 7, 2023, authorities sought to use their extensive disinformation networks to undermine Israel and support Hamas. For example, the Iranian state-affiliated outlet Tasnim News Agency spread deliberate disinformation that the United States was behind several attacks against civilians in Gaza in the early days of the war. **115**

The regime’s “cyberarmy” has also been used to target dissidents or spread false information about government critics through intimidation campaigns (see C7). **116** During the coverage period, reports emerged that a hacking group linked to the IRGC impersonated journalists and human rights activists online to lure government critics into phishing operations (see C8). **117** Similar reports of the Iranian cyberarmy impersonating activists in an effort to influence foreign elections emerged during and after the coverage period. **118**

The regime has allegedly spread disinformation to distract online users from the state’s violent crackdown on nationwide protests which began in September 2022. In January 2023, an anonymous X account impersonating an opposition activist known as Jupyter Rad spread progovernment propaganda to its followers, who numbered over 100,000. **119** The account claimed that Judge Abdolqassem Salavati, a notorious figure known to most Iranians as the “hanging judge” because of the number of death sentences he has handed out, was assassinated. **120** This deliberately false news went viral and quickly overtook Persian-language social media sites, temporarily quelling reporting on the protest crackdowns and executions. Many analysts believe Jupyter Rad is a regime-run troll account that is used to distract the public through its disinformation campaigns. **121**

The regime has backed numerous initiatives to promote blogging among its supporters. **122** For example, a state-affiliated Iranian cultural center has sponsored the annual National Cyber Jihad Festival for bloggers to promote

conservative religious values online. ¹²³ Authorities also actively support the creation of state-sanctioned social networking sites and mobile apps by offering free bandwidth and hosting to local developers. ¹²⁴

During the coverage period, the Iranian regime or its supporters manipulated entries on Wikipedia to deliberately mislead readers and promote government narratives, notably about Iran’s human rights record. ¹²⁵ For example, mentions that senior Iranian officials were involved in the mass executions of thousands of political prisoners in 1988 were removed. ¹²⁶

Government actors and private companies alike spend thousands of dollars on social media manipulation. ¹²⁷ In August 2022, reports revealed that the Mobarakeh Steel Company had spent 4.1 billion rials (\$96,000) on a cohort of X users to reshape the narrative around a pending parliamentary inquiry into a corruption case against it. ¹²⁸

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

0/3

There are several regulatory and economic constraints that affect the ability of users to publish online.

Domestic internet traffic is priced at a lower rate compared to international traffic, making it more costly for users to access international platforms. ¹²⁹ Efforts towards implementing a “tiered” internet could allow authorities to determine who gets access to the global internet and who will be forced to rely on the highly censored domestic web (see A3). For example, in January 2023, the ICT minister announced that “preferential access” to international content may be provided to freelancers, developers, and academics. ¹³⁰ To obtain this access, the organization or individual would need to submit an application to a government entity and be approved to get access to “select restricted websites.” ¹³¹

The IUPB requires foreign and domestic online platforms to register with a supervisory board and comply with Iranian laws or face penalties (see B3). ¹³² It also requires that foreign companies open offices within Iran. Meanwhile, Iranian versions of popular social media apps, such as Bale, Rubika, and Soroush, receive

significant financial support from the government as it continues to push users away from the international internet. **133**

The IRIB is responsible for issuing licenses and regulations relating to audio and video content online. **134** As of January 2023, all online platforms that publish audio or visual content must receive a license from the Audio Visual Regulatory Authority. **135** Platforms without a license will not be permitted to publish content. **136** In February 2024, authorities mandated that social media influencers with over 5,000 followers must obtain an advertising license. **137**

US sanctions have historically prohibited US technology companies from operating in Iran, though these sanctions were loosened during the previous period (see B3). **138**

According to a survey released in October 2022 by the Tehran Computer Trade Union Organization, responding online businesses lost more than 50 percent of their income during the first month of the Woman, Life, Freedom protests due to online restrictions and connectivity disruptions. **139**

B7 0-4 pts

Does the online information landscape lack diversity and reliability?

1 / 4

The media landscape is tightly controlled by the regime and there are very few independent or critical media outlets. **140** Nearly all international news websites and websites that host content about LGBT+ rights and religious minorities are blocked (see B1). **141** Before its blocking in 2022, Instagram was often used as a news source, a platform for activism, or to discuss politics (see B1). **142** Independent journalists and bloggers are frequently jailed for their reporting, further hindering the diversity of content available online.

VPNs are commonly used to protect online privacy and to circumvent the government's filtering. **143** However, the government regularly seeks to disrupt access to VPNs and has made efforts to criminalize the distribution and use of these tools (see B1 and C2). **144** In February 2024, the SCC announced that the use of unauthorized VPNs would be banned, and that individuals will need to apply to purchase licensed VPNs and secure approval from the government to gain

access to the global internet (see C4). **145** It is unclear how much it will cost users to obtain a government-approved VPN or license.

Aparat, an Iranian website similar to YouTube that enjoys less expensive tariff rates, is one of the most visited websites in Iran. **146** Content on Aparat is governed in accordance with Iranian law, making it difficult for users to share or access socially or politically sensitive views. Internet hosting companies inside Iran are banned from providing services to filtered websites under threat of prosecution (see B2). **147**

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?

2 / 6

Despite formal blocks on major international platforms, social media plays an important role in allowing dissidents to pursue online campaigns and share information. While Instagram and WhatsApp were blocked in 2022 (see B1), they remained central to the Woman, Life, Freedom protests. **148** Social media platforms have been integral to organizing protests and documenting violent crackdown on protesters by security forces. **149** Authorities frequently take action to curb social movements online, including to prevent the organization of offline dissent.

During the coverage period, social media was used to campaign against the executions of protesters under the hashtag “do not execute.” In April 2024, the hashtag #FreeToomaj was used to protest a death sentence handed out to an Iranian rapper who used social media to share his music and activism around the Woman, Life, Freedom protests (see C3). **150** Political activists used social media platforms to call for boycotts of the March 2024 parliamentary elections. **151**

Bandwidth throttling and internet cuts are common during politically sensitive times and used to discourage protests and disrupt the documentation of human rights violations. **152** Localized internet shutdowns and mobile restrictions began in September 2022 amid nationwide protests and continued through the end of 2023 (see A3). Localized internet shutdowns also occurred around the one-year anniversary of Jina Mahsa Amini’s death. **153**

During the coverage period, authorities arrested social media users or removed their social media accounts because of their participation in online mobilization initiatives (see C3). ¹⁵⁴ In September 2023, the Hijab and Chastity Bill (HCB) was passed, which includes criminal penalties for women who appear in public without properly wearing the hijab. The HCB has been used to stifle both online and offline feminist activism (see C2). ¹⁵⁵

During the previous coverage period, authorities began requiring that “virtual groups” at universities that count more than 100 members obtain authorization. Penalties for noncompliance with the law include suspension or expulsion. ¹⁵⁶

C. Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?

0/6

The 1979 constitution and legal framework do not protect freedom of expression and press freedom online. The head of the judiciary is appointed by the supreme leader, and the courts in general lack independence.

Broad, vague restrictions on expression exist in the constitutional framework and in the Islamic penal code, neither of which comply with international human rights law (see C2). ¹⁵⁷ Article 24 of the constitution guarantees the right to freedom of expression, but language providing for the restriction of expression deemed to infringe upon “the basic tenets of Islam or public rights” can be applied broadly. ¹⁵⁸ It is one of numerous constitutional provisions that can be invoked to restrict speech. ¹⁵⁹

Media freedom, while technically protected under Article 40 of the constitution, is subject to restrictions. ¹⁶⁰ The media is further regulated through the 2002 Press Law, which contains provisions used to deny access to independent, pluralistic, and diverse sources of information. ¹⁶¹

In response to the nationwide protests following the death in custody of Jina Mahsa Amini in September 2022, authorities adopted a range of repressive legislative and policy measures that further violated freedom of expression in Iran (see C2). **162**

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?

0 / 4

Numerous laws tightly restrict online speech and allow harsh punishments for those who deliberately flout the constraints or inadvertently draw the ire of authorities. The Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly defined. **163** The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize offline and online criticism of the regime.

The 2009 CCL outlines punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage “public morality” or result in the “dissemination of lies.” **164** Punishments are severe and include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines, and other penalties, including for service providers that fail to enforce government content restrictions. **165**

The repressive penal code also applies to online activities. **166** Article 286, which relates to the crime of *efsad-e fel arz* (“sowing corruption on earth”), is punishable by death. Efsad-e fel arz includes a set of vaguely defined acts, such as “spreading lies,” the “disruption of the economic system,” and actions that cause “severe disruption in the public order of the state and insecurity.” **167**

In September 2023, lawmakers passed the Hijab and Chastity Bill, **168** which introduces a range of punishments, including monetary fines, restrictions on accessing bank accounts, travel limitations, bans on online activity, and imprisonment for violations. The law aims to further restrict the online activities of influencers and celebrities who appear unveiled by labelling their activities as “crimes of national security.” **169**

Ongoing efforts to curb the use of VPNs include criminal penalties for those found to sell or use illegal circumvention tools. In October 2022, the ICT Ministry announced that anyone selling or using illegal VPNs could be charged under Article 753 of the penal code and could face fines or imprisonment (see B1). ¹⁷⁰ In February 2024, the SCC announced that the use of unauthorized VPNs would be banned (see B1, B7, and C4). ¹⁷¹

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?

0/6

The Iranian regime routinely arrests journalists and social media users for their online activities. Those affected in recent years have included prominent activists, Instagram celebrities, editors at independent news outlets, and citizen journalists associated with persecuted religious groups. ¹⁷²

Prominent musician Toomaj Salehi was sentenced to death in April 2024 by the Revolutionary Court in Isfahan on charges of “spreading corruption on the earth.” The court added that he was eligible for a sentence reduction. ¹⁷³ Toomaj had previously been arrested and sentenced to six years in prison in November 2023 after he posted a video to social media speaking about antigovernment protests and torture in prisons (see C7). ¹⁷⁴ After domestic and international pressure, the Supreme Court overturned the death sentence and called for a retrial in June 2024, after the coverage period. ¹⁷⁵

In July 2023, Ali Akbar Zaz was arrested in Tehran and after posting comments to an online forum that were critical of the government. Zaz has been accused of “corruption on earth,” “propaganda,” and committing blasphemy against the Supreme Leader. If charged, Zaz could face the death penalty. ¹⁷⁶ As of the end of the coverage period, Zaz remained in Evin prison awaiting trial. In October, he reported to have suffered torture while in custody (see C7). ¹⁷⁷

In October 2022, Saman Yassin, a Kurdish musician, was sentenced to death for “waging war against god” after sharing songs online that supported the protest movement. ¹⁷⁸ He was held in pretrial detention in Rajai Shahr prison for 18 months, where he has reportedly suffered physical and psychological torture (see

C7). **179** In April 2024, the death sentence was overturned and Yassin was sentenced to five years in exile. **180**

Several bloggers and social media users were arrested and received prison sentences for their online content during the coverage period. Two sisters received prison sentences of 20 years and 15 years for social media posts of women dancing in Iran. **181** In March 2024, Saba Azarpik, a social media activist, received a three-year prison sentence and a two-year social media ban after being charged with defamation for her online activism. **182**

In December 2023, an Iranian court handed Donya Hosseini, a blogger first arrested in 2022 over her activism during the Woman, Life, Freedom protests, a five-year suspended sentence on charges of “inciting others to commit violent acts.” Hosseini also received a nearly \$2,000 fine and was “banned from using smartphones.” **183** In August 2023, authorities arrested Elaheh Asgari, a travel blogger, Elaheh Asgari, reportedly in retaliation for her blog activities. **184**

A number of journalists arrested for their coverage of Amini’s death remained in detention during part or all of the coverage period. They include journalist Niloofar Hamed **185** and journalist Elaheh Mohammadi, who stood trial in relation to their work in May 2023. Mohammadi was handed a three-year suspended sentence in September 2023 for reporting on the protests. **186** Both women were held in detention for 17 months before being released in January 2024. **187** In July 2023, the editor in chief of Etemad was arrested for covering the protests. **188** Independent investigative journalists Saba Azarpeik and Yashar Soltani were sentenced to 2 years and 13 months in prison respectively, in June 2024, after the coverage period. They were charged with spreading “false information” and “propaganda against the state” in their online reporting. **189**

Following the implementation of the new Hijab and Chastity Bill (see B8 and C2), several women were arrested for posting photos or videos of themselves unveiled online. Sadiqeh Vasmaghi, an academic and activist, was sentenced to a year in prison in March 2024 after she posted a video on social media where she appeared without a hijab, reportedly in protest of the HCB. **190**

People have also been criminally charged or arrested for sharing videos to social media of women being violently arrested by Iran’s morality police for improperly

wearing the hijab. In March 2024, four social media users were arrested after they posted a video to X, which garnered over 100,000 views, depicting a woman being harassed by a cleric because of how her hijab was worn. ¹⁹¹

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?

1 / 4

The legal status of encryption in Iran is ambiguous. Authorities have additionally pursued regulations that discourage the unfettered use of VPNs and require internet users to verify their identity in order to gain access to the internet. Together, these factors make anonymous internet use extremely difficult.

The CCL prohibits “concealing data, changing passwords, and/or encoding data that could deny access of authorized individuals to data, computer, and telecommunication systems.” ¹⁹² While this could be understood to prohibit encryption, enforcement of the provision is uncommon. Nonetheless, authorities have periodically blocked encrypted traffic from entering the country through international gateways, particularly during contentious events such as elections. ¹⁹³ Several encrypted messaging applications including Signal and WhatsApp are blocked in Iran (see B1).

In February 2024, the SCC announced that individuals seeking to obtain VPNs will have to apply to purchase government-licensed VPNs and secure approval from the government (see B7 and C2). ¹⁹⁴ The IUPB includes provisions that would threaten online anonymity by banning unauthorized encrypted communication tools and VPNs (see B3), ¹⁹⁵ and requiring users to provide official identification to authorities to access online services. ¹⁹⁶ The bill, which has been partially enacted, could force users onto domestic platforms that lack encryption, essentially making anonymous communication impossible.

Iran’s National Mobile Registry Plan, which was implemented in 2017, requires user to register mobile devices with government agencies. ¹⁹⁷ Purchasing a SIM card requires real-name registration, and users must present their passport or identifying documents. ¹⁹⁸

According to FilterWatch, the Iranian User Verification System, which was launched in February 2024, “records Iranians’ identity information from birth.” According to Article 3 of the SCC’s Guidelines for Data Privacy Protection, the National Organization for Civil Registration is responsible for the collection of personal and identifying information (see C5). Section 1 of Article 3 states that “every cyberspace interaction must be accompanied by a valid identity, and everyone on the national information network or networks connected to it must verify their identity.” **199**

In February 2024, the Supreme Cyberspace Regulatory Commission (a subsidiary of the NCC) passed the Data Hosting Service Organization Guidelines, which, according to FilterWatch, state that anyone who “offer[s] data, cloud, or hosting centers” must verify their identity. **200**

C5 0-6 pts

Does state surveillance of internet activities infringe on users’ right to privacy?

0/6

The online sphere is heavily monitored by the state despite Article 37 of the nonbinding Citizens’ Rights Charter, which states that online privacy should be respected. **201** In April 2018, the supreme leader issued a fatwa related to users’ privacy on social media and online messaging, saying the invasion of privacy is against Islamic law. **202** However, the fatwa is not law and is not respected in practice.

Investigations published during the previous coverage period from the Intercept and Citizen Lab found that government agencies, namely the CRA, have the ability to intercept, store, and analyze mobile user data for the purposes of surveillance. **203** According to the reports, authorities can intercept mass mobile data—including geolocation data, voice and text messages, and data usage records—without a court ruling or warrant.

Citizen Lab and the Intercept also found that SIAM software installed on Iranian ISP networks has allowed the CRA to monitor mobile users’ online activity. Specifically, SIAM can throttle individual’s mobile service (see A3), analyze telecommunications metadata, access the content of encrypted communications (see C4), and use geolocation tracking to identify individuals. **204**

State surveillance of online activity is in part facilitated by the NIN, which includes several National Data Centers that not only house telecommunications data within Iran but allow authorities to have unfettered access to the servers where this data is collected and stored (see C4 and C6). **205**

The state monitors social media for activity it deems illegal. FATA is tasked with monitoring and tracking social media under the auspices of combatting cybercrime. **206** DPI tools allow authorities to filter online content while also analyzing browser history and communications. **207**

Authorities have promoted domestic social media and communications applications that rights groups say are linked to Iran's intelligence services, and offer avenues for surveillance. **208** In March 2022, the ICT minister announced that security forces may be permitted to access user data from these apps with a warrant. **209** According to New Lines magazine, managers of Rubika, one of Iran's domestic messaging apps, have claimed that they use artificial intelligence (AI) to identify and remove content that is deemed "immoral" from the app, although these comments have not been verified. **210**

Amid the Woman, Life, Freedom protests, reports emerged that Iranian authorities were using AI-powered technology, including facial recognition, to identify and target protesters, specifically women violating the country's hijab laws. **211** In May 2020, FATA had announced that not wearing the hijab online would be considered a crime, and that offenders would be prosecuted (see C3). **212** According to reports, authorities plan to increase the use of facial-recognition technology for those appearing unveiled online to enforce the HCB (see C2). **213**

Tehran has purchased surveillance technology from other authoritarian governments, including those of China and Russia. Several investigations have found that the IRGC has purchased facial-recognition technology from Tiandy, a Chinese technology firm. **214** In March 2023, the *Wall Street Journal* reported that the Russian government had sold Tehran technology that included "communication-surveillance" software. **215**

State agencies such as the IRGC have pressured or coerced detained activists into handing over log-in details for their social media accounts, which the authorities have then used for surveillance and phishing attacks (see C8). **216** During the

Mahsa Amini protests, the Committee to Protect Journalists (CPJ) documented 48 cases of journalists who had their devices seized and illegally searched while in detention. It was also discovered that authorities used consumer disk-recovery software known as Disk Drill to recover deleted files and content from detainees' devices. **217**

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	0 / 6
---	--------------

All service providers and platforms hosted in Iran are subject to arbitrary requests by various authorities to provide more information on their users.

Iran lacks a comprehensive data-protection law. In May 2023, a committee within the ICT Ministry announced that a draft bill on data protection and privacy would be sent to the cabinet. **218** Previous data-protection bills lacked an independent implementing body **219** and adequate remedies for users whose rights were violated, and ultimately never became law. **220**

During the coverage period, the government announced the country's seventh National Development Plan, whose "Lifestyle Assessment System" data-collection component would collect and store personal and identifying data from various government entities including the IRIB and the Ministry of Culture. **221**

The CRA, which sits under the ICT Ministry and is heavily controlled by Iran's intelligence forces, enforces the use of surveillance and censorship equipment at the ISP level, and has the ability to access user data collected by ISPs (see A4). **222** In October 2022, reporting from the Intercept found that the CRA was using SIAM, a web program for remotely manipulating cellular connections and conducting surveillance operations, to track users through data collected from their registered SIM cards (see A3 and C5). **223**

Long-term government policies and financial incentives aim to force Iranian users to migrate from international platforms to less secure domestic platforms and services, which do not guarantee the kind of user protection offered by some of their international counterparts. **224** Since Telegram was banned in 2018, the

government has promoted domestic, state-linked messaging apps such as Soroush and Bale. **225**

Iranian social media users have reported having their personal and user profile information taken from Instagram (prior to its blocking in September 2022) and transferred and replicated onto Rubino—a domestic version of Instagram and part of the state-affiliated app Rubika—without their consent or awareness. **226**

In 2017, the SCC released a new resolution outlining a legal framework for messaging apps operating in Iran and formalizing previous demands that foreign messaging apps work with Iranian authorities to obtain licenses and move their data centers inside Iran. The rules also tasked the ICT Ministry with forming a committee to suggest a licensing process for domestic and foreign messaging apps (see B6). **227**

Locally operated platforms for taxis or food-delivery services have been used to collect and share user data with authorities, who then used geolocation data to identify and, in some cases, arrest protesters and activists. **228**

The partially enacted IUPB has concerning provisions around data protection and online privacy. The bill requires foreign and domestic online services to register with a supervisory board, and foreign social media and messaging companies would have to “designate an Iranian company as their legal representative” and would be forced to comply with “rules set by the regulator” which could include complying with government requests for user data (see B2 and B6). **229**

A 2009 law requires ISPs to retain user data for at least three months. **230** There are several national data centers in Iran, where domestic and local internet traffic and user data is stored (see C5). **231** Authorities have unfettered access to these data storage centers, such as the Shahkar System, a data warehouse that stores mobile user data; and Shamsa, an interface that allows the collection of bulk text and voice message records as well as internet protocol (IP) data. **232**

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?

O/5

Iranian authorities commonly engage in extralegal intimidation and violence. Journalists, bloggers, and activists who are serving prison sentences due to their online activities frequently experience maltreatment and torture while in detention.

Hundreds of people have been killed at the hands of Iran's security forces while participating in the Woman, Life, Freedom protests, including several prominent social media influencers. Hadis Najafi, a prominent TikTokker who used social media to promote women's rights, in Iran was shot and killed at a protest, reportedly by security forces, in September 2022. ²³³ Also in September 2022, 16-year-old video blogger Sarina Esmailzadeh was beaten to death by security forces while participating in protests. ²³⁴ Naim Arbabi, a prominent social media activist, was killed by four armed assailants in March 2024, with some reports suggesting that his death was a result of his continued political activism. ²³⁵

Numerous reports of torture in detention emerged during the coverage period. Saman Yassin, a Kurdish musician and artist, faced physical and psychological torture while in detention following his arrest in October 2022 (see C3). ²³⁶ According to a July 2023 report, Yassin has been subjected to unknown injections, forced unconsciousness, and forced hospitalization. ²³⁷ In January 2024, Roya Heshmati was flogged 74 times by security agents reportedly because of a social media post from April 2023 that depicted her without a hijab. ²³⁸

In March 2023, the Office of the UN High Commissioner for Human Rights (OHCHR) expressed concern over the mass poisonings of over 1,200 schoolgirls across Iran. Iranian schoolgirls, including those who were poisoned, have been instrumental online activists during the protests, sharing images and videos on social media—some of which have gone viral—to protest the regime and the mandatory hijab law. ²³⁹ The poisonings started in November 2022; UN experts believe the poisonings were deliberate attempts to silence those demanding accountability for human rights crimes or for supporting the ongoing protests.

240

The families of protesters condemned to death over their protest activity have also received threats and harassment for using social media to call attention to these sentences. ²⁴¹ This is consistent with the authorities' long-standing practice of intimidating, harassing, and persecuting those who speak out about human

rights violations. The father of an executed prisoner said that security forces violently entered their home and confiscated their laptops and phones. **242** Gohar Eshghi, the mother of Sattar Beheshti, a blogger who died in prison in 2012, apparently under torture, has made public claims that she and her family have been threatened by government agents. **243**

The LGBT+ community has been a primary target of persecution both offline and online. **244** According to ongoing research by Article 19 and the researcher Afsaneh Rigot, LGBT+ individuals are frequently targeted and entrapped on dating apps and social media platforms by state and nonstate actors. **245**

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	0/3
--	------------

State hackers often launch cyberattacks against activists and campaigners, including those in the diaspora. Charming Kitten, a cyberwarfare group affiliated with Tehran, has launched spear-phishing campaigns against activists and dissidents in recent years.

Independent media have been targeted by distributed denial-of-service (DDoS) attacks. **246** In March 2024, during the Nowruz holidays, a DDoS attack disrupted internet access, leading to widespread disturbances. **247**

During the coverage period, reports emerged that a hacking group linked to the IRGC had created fake social media accounts that impersonated journalists and human rights activists as part of a sophisticated phishing campaign. **248** In June 2023, the social media accounts of several members of an independent artists organization were hacked, likely because of the organization’s support of the Woman Life Freedom movement. **249**

Iran’s sophisticated cyberwarfare tactics have also been used to target dissidents abroad. In August 2023, Article 19 documented a series of leaks from the IRGC-affiliated Aadl Ali Telegram account, which revealed that the account operators had hacked into the devices and emails of several prominent members of the

Iranian diaspora over several years, with the intention to embarrass and discredit them by publicly posting intimate and private recordings. **250**

During the previous coverage period, Human Rights Watch (HRW) and Amnesty International revealed that Charming Kitten had targeted two HRW staff members and at least 18 other high-profile activists, journalists, researchers, and politicians working on regional issues with ongoing credential phishing campaigns. These attacks were conducted through WhatsApp links sent between September and November 2022. **251**

Several cyberattacks on state infrastructure and media took place during the coverage period. In January 2024, an Israel-affiliated hacking group Gonjeshke Darande (Persian for Predatory Sparrow) launched a cyberattack that disabled petrol stations across Iran. **252** In August 2024, after the coverage period, an Israeli hacking group called WeRedEvils claimed credit for cyberattack against Iran that disabled internet access for several hours in various regions, including Tehran. **253**

In October 2022, the Iranian hacking group Black Reward claimed credit for hacking into the email account of the country's atomic energy organization and stealing information related to the country's nuclear program. The group said it had carried out the attack in solidarity with Woman, Life, Freedom protests. **254** (State media confirmed the attack but said a foreign government was responsible.) In October 2022, another group hacked into an email account affiliated with Iranian mobile service provider Ariantel and leaked documents connecting the regime to censorship and surveillance activities at the company (see A3 and C5). **255**

Several "hacktivist" groups also targeted state-media with cyberattacks in solidarity with Woman, Life, Freedom protesters. For example, in May 2023, hackers struck the Foreign Ministry's website. The website's home page was defaced with crossed-out images of Supreme Leader Khamenei and then president Raisi. **256**

The *New York Times* identified malware spread via malicious emails beginning in February 2018, initially targeting the Gonabadi dervishes. **257** The goal of these tools is to steal information from opposition groups and spy on Iranians who use mobile apps to organize protests." **258** A separate report published by the Center

for Human Rights in Iran in May 2019 found that the Gonabadi dervish website Majzooban had suffered state-sponsored DDoS attacks that rendered it inaccessible for hours. **259**

Footnotes

- 1** Mahmoud Hamidi, “Iran’s Internet Quality Declines Despite Price Hike,” Iran News Update, June 27, 2024, <https://irannewsupdate.com/news/economy/irans-internet-quality-declines...>
- 2** Simon Kemp, “Digital 2024: Iran,” Data Reportal, February 23, 2024, <https://datareportal.com/reports/digital-2024-iran>
- 3** “Iran’s Mobile and Fixed Broadband Internet Speeds,” Speed Test Global, May 2024, <https://www.speedtest.net/global-index/iran>
- 4** “A look at the process of completing the national information network,” ISNA, March 26, 2023, isna.ir/xdNygL
- 5** FilterWatch, “Blocking Access to the Global Internet Through Economic Pressure,” February 26, 2024, <https://filter.watch/english/2024/02/26/policy-monitor-jan-2024/>

More footnotes



On Iran

See all data, scores & information on this country or territory.

See More [➤](#)

Country Facts

Population

88,550,000

Global Freedom Score

11/100 **Not Free**

Internet Freedom Score

12/100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2024

Other Years

2023

**Be the first to know
what's happening.**

Join the Freedom House weekly
newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

(202) 296-5101

press@freedomhouse.org

@2024 FreedomHouse