IRAN

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	21	21
Limits on Content (0-35)	29	32
Violations of User Rights (0-40)	39	37
Total (0-100)	**89**	**90**

* 0=most free, 100=least free

POPULATION: 79 million
INTERNET PENETRATION 2011: 21 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The Iranian regime has long had an ambivalent relationship with the internet, viewing it alternately as a catalyst for economic development or as an invading force that threatens the Islamic state's strict social, religious, and political values. Over the past three years, the balance has markedly shifted towards the latter, as the leadership has decisively chosen political control over the benefits of a more open society. After the internet played an important role in the opposition movement that followed the disputed presidential election of June 12, 2009, the Iranian authorities waged an active campaign against internet freedom, employing extensive and sophisticated methods of control that went well beyond simple content filtering. The government also reportedly allocated US$500 million in its 2010–11 annual budget for the purpose of combating of what it termed a "Soft War" being waged against the regime by its perceived enemies via media and online activities. The regime's increasing tendency to view the internet as a threat and the importance of countering the "Soft War" were reflected in various official statements in 2011.[1]

These circumstances contributed to an overall deterioration in the internet freedom environment in 2011 and early 2012, although the mass arrests and denial-of-service attacks that characterized the previous two years were less prominent. Instead, the regime turned to more nuanced and sophisticated tactics for subverting free expression online. These included: upgrading the filtering technology and using it to block particular types of traffic,

[1] For instance, Reza Taghipour, the ICT Minister, said that "the Internet has been formed based on liberal and humanistic values, which is dangerous and needs to be changed," http://www.mehrnews.com/fa/NewsDetail.aspx?NewsID=1431708.

hacking two international firms' digital certificates to undermine user privacy, and implementing the first stages towards establishing a National Internet. Together, these measures indicate the regime's intention to increasingly cut off Iranian internet users from websites and others online resources based outside the country. Alongside this enhanced technical sophistication, however, the regime also continued to use low-tech repression to punish and intimidate bloggers, journalists, and ordinary users. Over the past two years, Iranian judicial authorities meted out some of the harshest sentences in the world for online activities, including imposing the death penalty on three bloggers and information technology (IT) professionals.

The government first introduced the internet into Iran in the 1990s to support technological and scientific progress in an economy that had been badly damaged by eight years of war with Iraq. Until 2000, the private sector was the main driver of internet development. This changed under the government of the reformist President Mohammad Khatami (1997–2005), when the authorities invested heavily in expanding the internet infrastructure, but also began to clamp down on free expression online. Meanwhile, Supreme Leader Ali Khamenei first asserted control over the internet through a May 2001 decree that centralized service providers' connection to the international internet.[2]

OBSTACLES TO ACCESS

The Khatami administration worked to connect different cities with fiber-optic cables and otherwise improve infrastructure, resulting in a rapid expansion in internet use in the country. According to the International Telecommunication Union (ITU), there were 625,000 internet users in Iran at the beginning of 2000. By the end of Khatami's presidency in 2005, the number had increased to several million, spurred forward by the country's increasingly youthful demographics.

Present day statistics on the number of internet users in Iran are inconsistent and highly disputed, though most observers agree that usage continues to grow. According to the ITU, which receives statistics from the government on different information and communications technology (ICT) indicators, Iran's internet penetration rate was 21 percent by the end of 2011.[3] Other sources place penetration as low as 15 percent[4] or as high as 39 percent.[5] The

[2] "Country Profile—Iran," OpenNet Initiative, June 16, 2009, http://opennet.net/research/profiles/iran.
[3] International Telecommunication Union Database, "Internet 2010," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2010&RP_intLanguageID=1&RP_bitLiveData=False.
[4] A January 2011 survey conducted by the Iran Statistics Centre found the penetration rate to be almost 15 percent, or 11 million users, an increase of about 4 percent compared to the center's findings in 2010. "21.4 % of families have Internet access," Wimax News, March 11, 2011, http://wimaxnews.ir/NSite/FullStory/News/?Id=3190.

vast majority of these users (an estimated 94 percent) reside in urban centers, particularly Tehran, Shiraz, Mashhad, Esfahan, and Tabriz. Mobile phone use is significantly more widespread. The ITU estimates that there were 56 million users in 2011, for a penetration rate of 75 percent. However, this does not appear to take into consideration subscriptions from all providers, which would amount to approximately 85 million users, a penetration rate of over 100 percent.[6]

The cost of internet access in Iran remains very high and most users connect to the internet from home, meaning they are predominantly urban middle and upper class. Moreover, the speeds of internet connections in Iran are extremely slow. A recent study by the Iran Statistics Centre found that 84 percent of the country's users still use dial-up connections. Even for those subscribed to ADSL services, speeds remain slow. A government survey revealed that some ADSL subscribers (whose connections should be attaining 128 Kbps download speeds, the maximum speed permitted by the government for personal use) were only able to download at a dismal 6.1 Kbps.[7] According to the Director of Iran's Telecommunications Company (TCI), the government of President Mahmoud Ahmadinejad has halted planning for further expansion of the IT infrastructure, exacerbating this problem.[8]

The telecommunications system in Iran is tightly controlled by the government or related entities. In recent years, the role of the Islamic Revolutionary Guards Corps (IRGC)—a politically important branch of the security forces that also controls large sections of the economy—in the ICT sector has notably increased.[9] In September 2009, for example, the IRGC purchased a controlling stake in the TCI, the country's main provider of internet and mobile phone services. The Data and Communication Company (DCC), which operates under the TCI, retains a monopoly on internet traffic flowing in and out of Iran. Other providers must purchase bandwidth from the DCC. In March 2012, the DCC increased the price for private providers of broadband,[10] causing some observers to speculate that it intends to capture their market share and further increase its dominance of the information landscape. Direct access to the internet via satellite is only permitted to certain institutes, and is prohibited for personal use. The mobile phone market is similarly under state

[5] A survey conducted jointly by the U.S.-government funded Broadcasting Board of Governors and Gallup in March 2012, found that among the 2,000 respondents in 31 provinces, 39 percent had accessed the internet during the previous week. BBG Research Series Briefing, *Iran Media Use 2012*, June 12, 2012, http://www.bbg.gov/wp-content/media/2012/06/BBG-Iran-ppt.pdf.
[6] There are two main mobile service providers in Iran. No accumulative number of subscribers have been published, but there are reports of 54 million subscribers of MCI and 31 million for IranCell/MTN. A third mobile operator (Rightel) was also launched recently but had only 10,000 subscribers at the time of writing.
[7] "Average speed of Internet in Iran," ITNA, September 20, 2011, http://itna.ir/vdcj8mev.uqeh8zsffu.html#.
[8] "The 10th Government has ignored ICT," ITNA, May 14, 2011, http://itna.ir/vdcgnz9q.ak97w4prra.html.
[9] "The Revolutionary Guards is entering the IT market," Digarban, December 12, 2011, http://www.digarban.com/node/3715.
[10] "Internet price to increase in 2011," Entekhab, March 26, 2011, http://www.entekhab.ir/fa/news/22391.

influence. The second mobile operator, IranCell, is owned in part by a web of proxy companies controlled by the IRGC (there are a number of high profile IRGC ex-commanders among its management). The third operator, Rightel, was launched in early 2011. It too is a government-owned entity, but as of May 2012 had gained only a few thousand subscribers.

During the 2009 protests, the authorities used their control over the internet infrastructure to curb access by causing a massive drop in the speed of connectivity, making it difficult to conduct basic online activities. Ports used by instant-messaging and chat platforms were also tampered with and mobile phone text messaging was shut down nationwide for 40 days. Similar periodic disruptions continued in 2011 and early 2012 but appeared to be linked to adjustments applied to the content filtering system rather than an effort to thwart protests on sensitive dates.

There is no independent regulatory body for ICTs in Iran. The Communications Regulatory Authority (CRA) is responsible for telecommunications licensing. It is part of the ICT Ministry and its head is appointed by the minister.[11] In March 2012, the broader decision making process related to ICTs underwent a change, when Iran's Supreme Leader Khamenei issued a decree establishing "The Supreme Council on Cyberspace" (SCC). The SCC is intended to provide a centralized focal point for policy making and regulation of Iran's virtual space, effectively removing such authority from the executive, legislative and judiciary branches of the government and bringing it under Khamenei's direct control. Observers believed this reflected Khamenei's dwindling trust of President Ahmadinejad and hesitation to leave such an important area of policy under his authority.

LIMITS ON CONTENT

Internet filtering, which began toward the end of the Khatami presidency in 2005, has become more severe since June 2009. The authorities employ a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private internet service providers (ISPs) are forced to either use the bandwidth provided by the government or route their send traffic (which contains site-visit requests) through government-issued filtering boxes developed by software companies inside Iran. The boxes search for banned text strings—either keywords or domain names—in the URL requests submitted by users, and block access accordingly.

[11] Communications Regulatory Commission of Iran, accessed July 31, 2012, http://www.cra.ir/Portal/Home/.

Throughout 2011 and early 2012, the Iranian authorities continued to restrict access to tens of thousands of websites, particularly those of international news sources, the opposition Green Movement, ethnic and religious minorities, and human rights groups. Some previously accessible websites and blogs also began being blocked, including news sources like Yahoo News and Reuters.[12] Ahead of parliamentary elections in March 2012, the Office of the General Prosecutor threatened to block any website that published calls to boycott, protest, or question the credibility of the polls, a threat that was reportedly acted upon.[13] Websites addressing economic issues were also subject to censorship. In January 2012, shortly after the value of Iran's currency hit a record low against the dollar, the website Mesghal.ir, which provides real time reports on the value of the Rial against other currencies, was blocked.[14] Its manager was arrested and accused of reporting misinformation and causing the fluctuating exchange rates.[15]

The government's filtering also tracked tensions in foreign policy. In December 2011, the authorities blocked access to the website of the British Embassy in Tehran following a diplomatic crisis that led to the closure of the mission.[16] That same month, the United States' Virtual Embassy was blocked the day after being launched. [17]

Even websites operating within the official discourse have not escaped filtering. A number of websites and blogs belonging to Ahmadinejad supporters who publicly criticized some of his government's policies were blocked, reflecting the growing polarization within the regime. In May 2011, the website of Haft-e-Sobh (Seven in the Morning), a group close to Ahmadinejad, was blocked. [18]

As of May 2012, all major international social media tools like the social-networking site Facebook, the video-sharing portal YouTube, the microblogging service Twitter, and the photo-sharing application Flickr were blocked. The periodic disruption of access to services

[12] "Reuters and Yahoo News have been filtered," FardaNews, January 31, 2011, http://www.fardanews.com/fa/news/135558/%D8%B1%D9%88%DB%8C%D8%AA%D8%B1%D8%B2-%D9%88-%DB%8C%D8%A7%D9%87%D9%88-%D9%86%DB%8C%D9%88%D8%B2-%D9%81%DB%8C%D9%84%D8%AA%D8%B1-%D8%B4%D8%AF%D9%86%D8%AF.

[13] "The Iranian State warns the sites: don't joke with the election," BBC Persian, December 31, 2011, http://www.bbc.co.uk/persian/iran/2011/12/111231_l10_election_boycott_warning_majlis9th.shtml.

[14] "The Rial Drops, And Iran Blocks The News," Radio Liberty, January 9, 2012, http://www.rferl.org/content/rial_drops_iran_censors/24446672.html.

[15] "The webmaster of Mesghal has been arrested/The government tries to make excuses for the economic crisis," Saham News, February 5, 2012, http://sahamnews.net/1390/11/165722/.

[16] Saeed Kamali Dehghan, "Iran blocks access to British embassy website," The Guardian, December 22, 2011, http://www.guardian.co.uk/world/2011/dec/22/iran-blocks-access-british-embassy-website.

[17] "US Condemns Iran's Blockage of 'Virtual Embassy Tehran'," Payvand Iran News, August 12, 2011, http://www.payvand.com/news/11/dec/1077.html?utm_source=Payvand.com+List&utm_campaign=b6064ec252-RSS_EMAIL_CAMPAIGN&utm_medium=email.

[18] "Haft-e-Sobh, a website close to Ahmadinejad's team has been filtered," Digarban, June 2, 2011, http://digarban.com/node/1230.

based overseas—such as Google's fairly well-encrypted email and blogging platforms, Gmail and Blogger, or its new social network Google+—appear designed to frustrate users and eventually force them to seek more easily monitored alternatives based in Iran. Although many Iranians have been able to access the blocked platforms using various circumvention techniques, the authorities have actively worked to disrupt such efforts, forcing users to constantly search for new solutions.

The regime has also employed administrative measures to remove unwanted content from the web. The Computer Crime Law (CCL) makes service providers, such as blogging platforms, responsible for any content that appears on their sites. This has led to the suspension of blogs or shuttering of news websites hosted on platforms inside Iran, under orders from government officials. Blogfa, one of the main blogging platforms inside Iran, reportedly receives orders to shut down an average of 50 blogs each week, though on some occasions this has reached 10,000 blogs per week.[19] In other cases, website owners have been forced to register their sites with the Ministry of Culture and have then received requests to remove particular posts deemed unacceptable by the government. According to Alireza Shirazi, the founder and manager of Blogfa, such massive censorship has damaged the Iranian blogosphere by discouraging users from blogging.[20]

Many people have instead shifted to posting on social-networking platforms like Facebook, accessing the blocked site with the use of circumvention tools. Facebook is perceived to offer a safer environment for expressing views among a limited audience of contacts. Some individuals associated with the regime have sought to discourage this practice. In July 2011, the deputy director of the ministry in charge of IT development declared that linking to filtered websites in an online post could be considered "against the spirit of the law" and therefore punishable by a fine or imprisonment.[21] The Iranian Cyber Police seconded this warning in November 2011, stating that exchanging information on foreign social-networking sites could constitute a criminal act and lead to prosecution.[22] Speaking from a different perspective, in January 2012, an Iranian cleric declared Facebook to be un-Islamic and that membership constituted a sin.[23]

[19] Fanavaran, Alireza Shirazi, interviewed by Shabnam Kohanchi, "Filtering killed the indicators of blogosphere," December 17, 2011, http://www.itmen.ir/index.aspx?pid=10324&articleid=3954.
[20] Ibid.
[21] "The internet manager of Ministry of Culture: Iranian users should use Iranian social networks," Gerdab, July 27, 2011, http://www.gerdab.ir/fa/news/6652/%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86%DB%8C-%D8%A7%D8%B2-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%DB%8C-%D8%AF%D8%A7%D8%AE%D9%84%DB%8C-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%DA%A9%D9%86%D9%86%D8%AF.
[22] "Is being a member of social networks a crime?" Jahan News, November 17, 2011, http://www.jahannews.com/vdcdkk0fxyt0no6.2a2y.html.
[23] Amrutha Gayathri, "Muslim Cleric Says Facebook is Un-Islamic, Membership Sin," International Business Times, January 11, 2012, http://www.ibtimes.com/articles/280026/20120111/muslim-cleric-facebook-un-islamic-membership-sin.htm.

As with blocking, the targets of such censorship have included websites and blogs associated with high-ranking officials. In May 2011, the website of Kashan's Friday Prayer leader was taken offline after he revealed details about the conflict between Khamenei and Ahmadinejad.[24] The following month, the news website *MojmelNews* had its Iran-based servers shut down after it reported that Ahmadinejad was not cooperating with the reinstated Minister of Intelligence.[25] In December 2011, the website of influential cleric and ex-President Akbar Hashemi Rafsanjani was blocked and temporarily shut down;[26] Rafsanjani heads an advisory body to Supreme Leader Khamenei but has been openly critical of Ahmadinejad.

There have also been periodic reports that mobile phone text messages with banned keywords were being filtered, typically around politically sensitive events. Prior to parliamentary elections in March 2012, Iranian Member of Parliament Aliakbar Olya reported that mobile phone operators were blocking text messages containing the keywords "parliament," "provincial governors," "date," or "meeting."[27] In January 2012, around the time of the currency plunge, users reported that text messages containing the word "dollar" or "foreign currency" were also blocked.[28]

In an effort to show that content filtering is based on a legal framework and not arbitrary, institutions to oversee internet filtering have been created. The CCL enacted in 2009 upgraded the mandate of the Committee in Charge of Determining Unauthorized Websites, initially created in 2002. The committee is empowered to identify sites that carry forbidden content and report that information to the TCI and other major ISPs for blocking. The committee is headed by the prosecutor general and other members are representatives from 12 governmental bodies. The law also identifies the violations that might result in a website being marked for filtering. These are defined very broadly and range from insulting religious figures and government officials to distributing pornographic content and illegal circumvention tools.[29]

In practice, little information is available about the inner workings of the committee, and censorship decisions are often arbitrary and nontransparent. According to the law, the committee should meet biweekly to decide on any website bans, but a TCI vice president

[24] "Kashan's Friday prayer leader's website has disappeared," Aftabnews, June 1, 2011, http://aftabnews.ir/vdccx4qs42bqie8.ala2.html.
[25] "Majmal News website has become out of rich," Digarban, June 29, 2011, http://www.digarban.com/node/1499.
[26] "Iran ex-President Rafsanjani's website blocked," BBC News, December 30, 2011, http://www.bbc.co.uk/news/world-middle-east-16368472.
[27] "SMS services are going to be filtered?!," ITNA, October 30, 2011, http://itna.ir/vdcdnf0x.yt0zx6a22y.html.
[28] "UPDATE 1-Iran rial slides, 'dollar' text messages appear blocked," Reuters, January 10, 2012, http://www.reuters.com/article/2012/01/10/iran-currency-idUSL6E8CA2MQ20120110.
[29] "12 memebers of Committee in Charge of Determining Unauthorized Sites," Weblognews, December 16, 2009, http://weblognews.ir/1388/09/mediablog/5740/.

said in 2010 that the rate of filtering was 200 to 300 websites per day, meaning the bulk of filtering decisions are likely made upon discovery of objectionable content, or by a small technical team. This would leave the committee to decide on only the most controversial blocking decisions. In addition, owners of websites registered with the Ministry of Culture have complained that they received no explanation when their websites were filtered.[30] Among them was Zahra-hb, a well-known conservative blogger, whose blog was blocked in March 2012 without notification.[31] The authorities claim there is a procedure for disputing filtering decisions. However, the process is highly inefficient, and even conservative bloggers have failed to have their webpages unblocked by lodging complaints.[32] Moreover, the dispute process requires the website owner to disclose his or her personal information and accept responsibility for any misconduct in the future, a commitment that few are willing to make given the risk of severe punishment.

Alongside the expansion of existing controls, in July 2011, the Iranian authorities began referring to the creation of a National Internet. Iran's fifth development plan from June 2010, which the government is obliged to implement, provides for the establishment of a "National Information Network," although the plan does not specify the objectives of creating it. According to the Minister of ICT, the objectives include protecting the exchange of data within the country from security breaches, monitoring emails, and creating a "safe internet."[33] The particular technical specifications of the plan remain unclear and officials have used various names to describe the initiative, including a "Halal" or "Clean" internet, while others have issued conflicting statements about the project's end result. Media coverage and public discussions have often described the National Internet as a national intranet that, upon its launch, would cut off users inside Iran from the global internet. However, according to some experts, the cut off may not be absolute. Dr. Siavash Shahshahani, known as the founder of the internet in Iran, was quoted as comparing the initiative's outcome to China's censorship model, saying: "What is … referred to as the National Internet means that we will have good and expansive local connections but all our foreign connections are to pass through a controllable channel."[34]

[30] "The News stie's reporter will be insured," Hamshahri Online, November 1, 2011, http://www.hamshahrionline.ir/news-150108.aspx.
[31] Zahra HB, "When the filtering purposes are being violated," 30Mail (blog), April 7, 2012, http://30mail.net/weblog/2012/apr/07/sat/16886.
[32] "On filtering of Ahestan," Ahestan (blog), January 15, 2010, http://ahestan.wordpress.com/2010/01/15/ahestan.
[33] "Iran to launch national data network," Press TV, August 10, 2011, http://www.presstv.ir/detail/193306.html; "The ICT Minister: email management is one of the aims of launching national internet," Radio Farda, July 27, 2011, http://www.radiofarda.com/content/f10_iran_information_minister_managing_emails_collecting_information_national_internet/24278324.html.
[34] "The controversial comment of the founder of Internet in Iran about national internet," Jam News, March 5, 2012, http://www.jamnews.ir/NSite/FullStory/News/?Id=65655.

Although the final goal of the National Internet project remains unclear, available evidence indicates that the ICT Ministry has been tasked with implementing it in several phases, the initial of which appear to have already been put in place.[35] The first phase involves an upgrade in filtering capacity to enable more nuanced management, blockage, monitoring, and redirecting of traffic. On numerous occasions throughout 2011, users across Iran reported the slowing of internet speeds and heightened blockage of circumvention tools. Although no official explanations were offered, a number of news websites suggested the disruptions were related to an upgrade of the internet infrastructure.[36] Some observers noted that a growing percentage of domestic internet traffic was being routed only through Iranian servers rather than external ones, as would normally be the case. Then, in the run-up to the 2012 parliamentary elections, the authorities blocked all encrypted international traffic for several days. This confirmed that the government had developed a new capability, using sophisticated deep-packet inspection technologies to recognize different types of traffic and throttle them as deemed necessary. For instance, during the pre-election disruptions, traffic to services using the Secure Sockets Layer (SSL) protocol and based outside Iran was effectively blocked, restricting users' ability to access applications like Gmail. At the same time, however, users encountered no problems accessing online banking services within Iran that also run on SSL (displaying addresses beginning with "https"). Users also complained of trouble using virtual private networks (VPNs) to circumvent censorship. This new technical capacity will allow the Iranian authorities to control access to particular international communication flows during periods of political unrest without the need to shut down all domestic services or the entire network.

The next stage of the National Internet project is the mandatory registration of internet protocol (IP) addresses assigned to users (see "Violations of User Rights"). The final stage for implementing the National Internet is to move the hosting of government-approved websites to servers based inside the country and to launch Iranian equivalents of major online services like email, social-networking sites, and search engines. According to Iran's Deputy Minister of ICT, the government has already moved more than 90 percent of its websites to providers based inside the country and is now pressuring privately owned websites to follow suit.[37] Compliance has been limited, however, primarily because hosting services offered by Iranian companies are significantly more expensive than those of their overseas competitors.

[35] "Internet for all, internet for some," ITNA, July 16, 2011, http://www.itna.ir/vdcbfwb8.rhbw5piuur.html.
[36] "Continued disruption in the Internet," Kaleme, December 8, 2011, http://www.kaleme.com/1390/09/17/klm-82762/.
[37] "The ministry promises 20 Mbps internet again," Mashregh News, July 23, 2011, http://www.mashreghnews.ir/fa/news/59736/%D9%88%D8%B9%D8%AF%D9%87-%D9%85%D8%AC%D8%AF%D8%AF-%D9%88%D8%B2%DB%8C%D8%B1-%D8%AF%D8%B1%D9%85%D9%88%D8%B1%D8%AF-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-20%D9%85%DA%AF%D8%A7%D8%A8%DB%8C%D8%AA%DB%8C.

Launching viable national equivalents of major online services, as has happened in China, is considered to be the most critical stage of rolling out the National Internet. Iranian users will then be effectively cut off from the global internet and transnational conversations. However, successfully implementing this stage will be challenging for various reasons. First, several equivalents of major online services have been launched since 2010 but have subsequently gone out of business after failing to attract large numbers of users due to poor design. Second, international sanctions on Iran over its nuclear program have limited the government's ability to purchase the equipment required to run data centers on the scale needed to host a national email service, for example.[38] Existing data centers are incapable of servicing a large number of users. The Iranian authorities have been trying to entice the private sector to get involved, but due to a lack of experience and expertise in running large-scale web services, private firms have also not managed to get many popular platforms off the ground.

In addition to censorship, the state counters critical content and online organizing efforts by extending regime propaganda into the digital sphere. There are at least 400 news websites either directly or indirectly supported by the state. They seek to set the agenda by providing pro-government commentary or publishing rumors. In April 2011, an official from the Ministry of Culture and Islamic Guidance stated that 40 firms had received over US$56 million from the ministry to produce digital content.[39] There have also been a large number of government-backed initiatives to promote blogging among its supporters and members of the Basij paramilitary group. In July 2011, the head of the Basij said there were three million members active online and praised their activities.[40] Despite this large contingent, the content produced is limited in quality and quantity, constraining its practical influence over online discourse. In response, paramilitary commanders have called for the allocation of more resources, recruitment of another ten million Basiji bloggers, and the creation of a cyber army of loyalist content producers to fight the "Soft War."[41]

Self-censorship is extensive, particularly on political matters. The widespread arrests and harsh sentences meted out to reporters and activists after the 2009 elections, as well as

[38] "Persian email service, Chaapaar will be launched in December," IRNA, September 27, 2011, http://www.irna.ir/NewsShow.aspx?NID=30583255.
[39] "Reuters has Iran accreditation revoked for offensive headline; Cyber Council: 'use cyberspace to further the regime'; Cyber-defense curriculum to be introduced in some graduate level programs; OFAC lifts some IT sanctions-what does it mean for Iranians?" Iran Media Programme, April 2, 2012, http://www.iranmediaresearch.org/en/newsletter/12/04/02/901.
[40] "Basij have had large and effective measures in cyberspace," Fars News, October 11, 2011, http://www.farsnews.com/newstext.php?nn=13900719001180.
[41] "Basij should be equipped to deal with the soft war," Fars News, November 16, 2011, http://www.farsnews.com/newstext.php?nn=13900825001411.;
"10 million Basij should have 10 million blogs," Fars News, July 9, 2012, http://www.farsnews.com/newstext.php?nn=13900624000195; "The first Iranian cyber army to be launched," IT Analyze, February 21, 2012, http://itanalyze.com/news/2012/02/21/16506.php.

perceptions of pervasive surveillance, have increased fear among online journalists and bloggers. Many of them either abandoned their online activities or use pseudonyms. The result has been a palpable drop in the amount of original content being produced by users based inside the country.

Furthermore, the majority of independent content producers lack the financial resources to operate in such a hostile environment. The online advertising market in Iran is exclusively limited to apolitical and pro-government websites. Even businesses based outside Iran avoid political websites to maintain trading relationships with the country. Although the United States adjusted its sanctions against Iran to enable American internet companies to provide services to Iranian users, Google Advertising does not recognize Persian as one of the languages in its system, disadvantaging Persian content producers.[42]

Despite all of these limitations, the internet remains the only means available for Iranian citizens and dissenters to obtain news and organize themselves. Traditional media outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy jamming. Paralleling the rise in censorship, the use of VPNs, proxies, and other circumvention tools has also grown dramatically since 2009. Data from AnchorFree, a popular VPN distributor, shows that usage of its services in Iran increased ten-fold between July 2010 and July 2011, reaching over 360,000 users by that time.[43] This increase occurred despite repeated statements by the Minister of ICT that the use of circumvention tools and VPNs is a punishable crime.[44] Nevertheless, compared to the high level of online organization and mobilization in 2009 and 2010, one of the most notable changes since January 2011 has been the sharp drop in offline activities sparked by online communications.

VIOLATIONS OF USER RIGHTS

Iranian internet users suffer from routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those critical of the authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or

[42] Jamal Abdi, "Obama Norooz promise a good step, more needed to ensure U.S. not part of 'Electronic Curtain,'" NIAC InSight, March 21, 2012, http://www.niacinsight.com/2012/03/21/obama-promises-to-ease-internet-restrictions-in-norooz-message/.

[43] Elizabeth Flock, "Iranians using proxy servers 10 times more than they were last year," Washington Post, April 15, 2012, http://www.washingtonpost.com/blogs/blogpost/post/iranians-using-proxy-servers-10-times-more-than-they-were-last-year/2012/02/15/gIQA4LFMGR_blog.html.

[44] "Are Millions Of Iranians Criminals?" Radio Liberty, October 25, 2011, http://www.rferl.org/content/iran_internet_antifiltering_tools_censorship/24370376.html.

detrimental to public rights, none of which are clearly defined. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions. The 2009 Computer Crime Law (CCL) identifies punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage "public morality" or to be a "dissemination of lies."[45] Punishments mandated in the CCL are severe. They include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines, and penalties for service providers who fail to enforce government content restrictions.

Since June 2009, the authorities have cracked down on online activism through various forms of judicial and extralegal intimidation. An increasing number of bloggers have been threatened, arrested, tortured, kept in solitary confinement, and denied medical care, while others have been formally tried and convicted. At least 50 bloggers and online activists were arrested in 2009 and 2010. Although the number of new arrests decreased in 2011, many individuals detained during the previous two years were sentenced, often harshly. Three bloggers and IT professionals—Saeed Malekpour, Vahid Asghari and Ahmad Reza Hasempour—were sentenced to death between October 2011 and January 2012 on various questionable charges. Malekpour, for example, was prosecuted because a software program he had designed was used to upload pornography, although it was done without his knowledge.[46] The Committee to Protect Journalists speculated that the three were targeted because of their technical knowledge and ability to assist in the building and hosting of independent websites.[47] Other bloggers have been sentenced to prison terms of up to 20 years. Blogger Hossein Ronaghi-Maleki continues to serve a 15-year sentence imposed in December 2009 for "spreading propaganda against the regime" and insulting the Supreme Leader.[48] In June 2011, Hossein Derakhsan, considered the father of the Iranian blogosphere, lost his appeal against a 19-year sentence imposed on charges of cooperating with hostile countries, spreading propaganda against the regime, and insulting Islamic thought and religious figures. [49]

[45] *Islamic Republic of Iran: Computer Crimes Law Article 19*, January 30, 2012, www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf.

[46] Saeed Malekpour, interviewed by Olivia Ward, "Saeed Malekpour: A Canadian on Iran's death row," The Star, February 18, 2012, http://www.thestar.com/news/world/article/1132483--a-canadian-on-iran-s-death-row; Amnesty International, "Iran must halt execution of web programmer," January 19, 2012, http://www.amnesty.org/en/news/iran-must-halt-execution-web-programmer-2012-01-19.

[47] Danny O'Brien, "Online publishers, developers sentenced to death in Iran," Committee to Protect Journalists, January 20, 2012, http://cpj.org/internet/2012/01/online-publishers-and-developers-sentenced-to-deat.php.

[48] "Iranian blogger on hunger strike close to death, warn fellow prisoners," The Guardian, June 6, 2012, http://www.guardian.co.uk/world/iran-blog/2012/jun/06/iran-blogger-hossein-ronaghi-maleki-hunger-strike.

[49] "Iranian blogger loses appeal against 19-year sentence," The Guardian, June 9, 2011, http://www.guardian.co.uk/world/2011/jun/09/jailed-iran-blogger-loses-appeal.

Despite the relative decrease in new arrests, several bloggers and online activists were detained in 2011 and subsequently sentenced to prison. In February 2011, the Ministry of Intelligence arrested eight bloggers who had been critically discussing Islamic doctrine over the internet. In January 2012, they were all sentenced to prison terms ranging from five to nine years.[50] In another round of arrests in early 2012, security forces detained at least six journalists and bloggers in what appeared to be a preemptive measure to thwart protests surrounding the March parliamentary elections.[51]

Members of ethnic and religious minorities have also faced harsh punishment for expressing their views online or using websites to disseminate information. In May 2011, at least 30 Baha'is were arrested in coordinated raids in Tehran, Karaj, Isfahan, and Shiraz. The detained individuals were involved in an online university initiative to provide higher education to Baha'i students.[52] In September 2011, the administrators of a website related to the Daraawiish Sufi Muslim group were arrested.[53] In December, a user in Kurdistan province was reportedly arrested by police on charges of insulting officials and promoting an opposition group on social-networking sites.[54] In June 2011, Sakhi Reigi, a blogger from the Baluch ethnic minority was sentenced to 20 years in prison for acting against national security, a charge commonly used to jail members of ethnic minorities advocating for more rights.[55]

In other instances, ordinary users were detained for engaging in apolitical online activities deemed socially inappropriate by the regime. In March 2012, the authorities arrested the administrators of a soccer betting website, as betting is prohibited under Islam.[56] In September 2011, a handful of people who tried to organize a water fight at a Tehran park

[50] "8 people imprisoned in Iran for holding discussion on Islam in internet," APA, January 21, 2012, http://en.apa.az/news.php?id=164113.; "Iran sentences 8 people to prison for expressing religious beliefs in internet social network," HARDIP, January 20, 2012, http://hrdip.com/iran-sentences-8-people-to-prison-for-expressing-religious-beliefs-in-internet-social-network/.

[51] Rick Gladstone and Artin Afkhami, "Pattern of Intimidation Is Seen in Arrests of Iranian Journalists and Bloggers," The New York Times, January 25, 2012, http://www.nytimes.com/2012/01/26/world/middleeast/iran-steps-up-arrests-of-journalists-and-bloggers.html?_r=1&scp=1&sq=afkhami&st=cse.

[52] "Government Attacks Baha'i Online University, Detains 30 Instructors," International Campaign for Human Rights in Iran, May 23, 2011, http://www.iranhumanrights.org/2011/05/bahai-university-attacked/.

[53] "The managers of Majzoobanoor website have been arrested," 30Mail (blog), September 5, 2011, http://www.30mail.net/news/2011/sep/05/mon/11602.

[54] "The publisher of offensive materials to national authorities has been arrested," ISNA, November 27, 2011, http://www.isna.ir/isna/NewsView.aspx?ID=News-1899523.

[55] "Sakhi Rigi, Baluch blogger, was sentenced to 20 years imprisonment," Green Waves News, June 8, 2012, http://www.greenwavenews.com/1390/03/18/%D9%85%D8%AD%DA%A9%D9%88%D9%85%D9%8A%D8%AA-%D8%B3%D8%AE%DB%8C-%D8%B1%D9%8A%DA%AF%DB%8C%D8%8C-%D9%88%D8%A8%D9%84%D8%A7%DA%AF%E2%80%8C%D9%86%D9%88%D9%8A%D8%B3-%D8%A8%D9%84%D9%88%DA%86-%D8%A8%D9%87/.

[56] "Feta police will react to disturbing the public opinion," IT Analyze, March 26, 2012, http://itanalyze.com/news/2012/03/26/16968.php.

over Facebook were detained.[57] In another Facebook-related case, Iranian authorities arrested two men and two women in January 2012 on charges of "promoting vulgarity and corruption." The four had maintained a page on the social-networking site that acted as an online beauty contest, to which thousands of young people posted glamorous photos of themselves. [58]

The scale and arbitrariness of such arrests, as well as the harsh punishments meted out, have created a climate of fear among Iranian internet users. As a result, a large number of bloggers, journalists, and activists have gone underground or fled the country to seek political asylum in neighboring countries, mainly Turkey.[59] Meanwhile, ordinary users tread carefully when communicating online, unclear of what kinds of activities might inadvertently put them at risk.

Since early 2011, the authorities have increased technical measures to curb anonymous communications. On several occasions, around politically sensitive dates, ISPs blocked the SSL protocol, denying millions of Iranians secure access to their email addresses. In a similar move that also affected internet users outside of Iran, two international companies responsible for issuing digital certificates for popular online services like Gmail, Yahoo, Hotmail and Skype were hacked during 2011.[60] The precise number of users whose privacy was compromised remains unclear, but the forged certificates could have been used to potentially spy on some 300,000 users in Iran.[61] In September 2011, Google issued a warning to its users from Iran urging them to change their passwords as a precaution.[62]

Such blocks have generated criticism from within the government. In March 2012, Rasool Jaafarian, an influential cleric and director of the parliamentary library criticized the obstacles imposed on accessing informational websites, arguing that this has caused frustration among researchers because there is no domestic replacement for such services.[63] Iranian Member of Parliament (MP) Ahmad Tavakoli seconded this assessment, warning that

[57] "Iran makes arrests over new water fight attempt," Iran Focus, September 5, 2011, http://www.iranfocus.com/en/index.php?option=com_content&view=article&id=23670:iran-makes-arrests-over-new-water-fight-attempt-&catid=4:iran-general&Itemid=26.
[58] J. David Goodman, "Iranian Authorities Arrest Four Over Facebook Beauty Contest," The New York Times, January 31, 2012, http://thelede.blogs.nytimes.com/2012/01/31/iranian-authorities-arrest-four-over-facebook-beauty-contest/.
[59] "Iran and Cuba have the most exiled journalists," BBC Persian, June 20, 2012, http://www.bbc.co.uk/persian/iran/2011/06/110620_l39_cpj_iran_cuba_journalists_exile.shtml.
[60] The first hacking incident was of Comodo which took place in March 2011 and the second incident was the hacking of DigiNator which was made public in August 2011.
[61] Byron Acohido, "Authenticity of Web pages comes under attack," USA Today, September 29, 2011, http://www.usatoday.com/tech/news/story/2011-09-27/webpage-hackers/50575024/1.
[62] "Google issues warning to Iranian Gmail users," The Hindu, September 13, 2011, http://www.thehindu.com/sci-tech/article2449951.ece.
[63] "Internet disconnection and playing with the passion and talent of youth," Khabar Online, February 20, 2012, http://www.khabaronline.ir/detail/199918/weblog/jafarian.

the blockage of online services using the SSL protocol was creating widespread discontent that could be very costly for the regime, as more users seek out how to circumvent censorship and render the blocking of other sites ineffective.[64]

The Iranian authorities have taken a range of measures to monitor online communications and use them as a basis for criminal punishment. A number of protesters put on trial after the 2009 election were indicted for their activities on Facebook and Balatarin, a Persian content-sharing site. Many arrested activists reported that interrogators had confronted them with copies of their emails, asked them to provide the passwords to their Facebook accounts, and questioned them extensively on their relationships with individuals on their "friends" list. The authorities actively exploited the fear created by these reports, claiming that they had access to all the email and text messages exchanged in Iran.

The CCL obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to process all this data. When purchasing a mobile phone subscription or prepaid SIM card, users must present identification, facilitating the authorities' ability to track down the authors and recipients of specific messages. Despite international legal restrictions placed on the selling of surveillance equipment to the Iranian government, in 2011 there were numerous media reports that Chinese and some Western companies have been providing the Iranian authorities with technology to monitor citizens' digital activities. Specifically, investigative reports by Reuters and the *Wall Street Journal* found that Huawei Technologies[65] and ZTE Corporation,[66] both Chinese firms, were key providers of surveillance technology to Iran's government, allegations both companies have denied.

As noted above, the second stage of the National Internet plan involves the mandatory registration of IP addresses. Bill 106 issued by the Communications Regulatory Authority in March 2012 requires the registration of all of the IP addresses in use inside Iran, in order to organize and systematize them beyond the data already collected. Implementing such registration will allow the authorities to more to track users' online activities even more thoroughly.

[64] "Iranian MP denounces internet service disruptions," Payvand, April 13, 2012, http://www.payvand.com/news/12/feb/1135.html?utm_source=Payvand.com+List&utm_campaign=128035d177-RSS_EMAIL_CAMPAIGN&utm_medium=email.

[65] Steve Stecklow, Farnaz Fassihi, and Loretta Chao, "Chinese Tech Giant Aids Iran," The Wall Street Journal, October 27, 2011, http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html.

[66] "UANI Calls on Chinese Telecom Giant ZTE to Withdraw from Iran," Market Watch, press release, March 26, 2012, http://www.telecomyou.com/newscenter/news/uani-calls-on-chinese-telecom-giant-zte-to-withdraw-from-iran-marketwatch-press-release.

In January 2011, the government announced new regulations that require customers of cybercafes to provide personal information (such as their name, father's name, national ID number, and telephone number) before using a computer. Cafe owners are required to keep such information, as well as customers' browsing history, for six months. They are also required to install closed-circuit surveillance cameras and retain the video recordings for six months.[67] The regulations came into effect in March 2012.

Filtering and physical intimidation are supplemented by hacking and distributed denial-of-service (DDoS) attacks on the websites of government critics, including leading opposition figures. In the days after the disputed 2009 presidential election, many of the news websites set up by supporters of opposition candidates were taken offline through intense DDoS attacks. Technical evidence confirmed that government-owned IP addresses were used to launch the attacks.[68] Other websites were rendered either permanently or temporarily unavailable by means of hacking, primarily by a group calling itself the Iranian Cyber Army. This phenomenon continued in 2011 and early 2012 but on a smaller scale. In March 2012, for instance, the Iran Cyber Army hacked the website of the Association of Combatant Clerics, a reformist organization under the leadership of former president Mohammad Khatami, and the Baran Foundation, another organization linked to Khatami.[69]

A number of non-Iranian sites were targeted by more sophisticated attacks. The domain of the U.S. government-funded Persian service of Voice of America was hijacked by the Iranian Cyber Army in February 2011. Similarly, the British Broadcasting Corporation (BBC) reported a "sophisticated cyber-attack" in March 2012. It was believed to be linked to other Iranian efforts during that time to disrupt the BBC Persian Service.[70]

Initially, there was some speculation about the connection between the Iranian Cyber Army and the Iranian authorities. In May 2010, however, Iranian officials confirmed these suspicions by publicly announcing that the Iranian Cyber Army was under the command of the IRGC.[71] Since then, IRGC commanders have explicitly welcomed hackers willing to "work for the goals of the Islamic Republic."[72] In a sign of the further institutionalization of

[67] Golnaz Esfandiari, "Iran Announces New Restrictions For Internet Cafes," Payvand, January 5, 2012, http://www.payvand.com/news/12/jan/1048.html?utm_source=Payvand.com+List&utm_campaign=d6730c3065-RSS_EMAIL_CAMPAIGN&utm_medium=email.
[68] Norooz News, "Norooz is revealing the names of 4 governmental entities behind the attacks against reformist websites," October 17, 2010.
[69] "Bonyad Baran and Majma rohanioun's website have been hacked," Radio Farda, February 27, 2012, http://www.radiofarda.com/content/f12_two_khatami_related_sites_hacked/24497610.html.
[70] "Cyber-attack on BBC leads to suspicion of Iran's involvement," BBC News, March 14, 2012, http://www.bbc.co.uk/news/technology-17365416.
[71] "IRGC has formed the second cyber army in the world," Fars News, May 20, 2010, http://www.farsnews.com/newstext.php?nn=8902300353.
[72] "Iran Says It Welcomes Hackers Who Work For Islamic Republic," Radio Liberty, March 7, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html.

such efforts, an IRGC commander reported in November 2011 that the organization had established two Cyber War Centers and organized 2,000 officers to take part in the regime's Cyber War activities, which may include both hacking and production of pro-regime online content.