Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**592**
Land:	Iran
Kilde:	Immigration and Refugee Board of Canada
Titel:	Iran: Government surveillance capacity and control, including media censorship and surveillance of individual Internet activity
Udgivet:	16. januar 2015
Optaget på baggrundsmaterialet:	17. juni 2015

Immigration and Refugee Board of Canada | Commission de l'immigration et du statut de réfugié du Canada

Iran: Government surveillance capacity and control, including media censorship and surveillance of individual Internet activity [IRN104972.E]

Research Directorate, Immigration and Refugee Board of Canada, Ottawa

1. Censorship of Traditional Media

Freedom House, in its report entitled *Freedom on the Net 2013*, states that in Iran "traditional media outlets are tightly controlled by the authorities" (Freedom House 2013, 3). The Committee to Protect Journalists (CPJ), a New York-based organization that "promotes press freedom worldwide and defends the right of journalists to report the news without fear of reprisal" (CPJ n.d.), ranked Iran as the fourth-most-censored country in the world in 2012 (ibid. Feb. 2014). Reporters Without Borders (Reporters sans frontières, RSF), a Paris-based NGO that monitors "attacks on freedom of information worldwide" (RSF 10 Mar. 2014), ranks Iran as 173rd of 180 countries in their press freedom index and describes Iran as "[o]ne of the world's most repressive countries as regards freedom of information" (ibid.18 June 2014).

An August 2014 report by the UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran states that despite government officials making statements in support of greater press freedoms, "laws and policies continue to place overly broad restrictions on the rights to freedom of expression and access to information" (UN 27 Aug. 2014, para. 22). Similarly, RSF stated in June 2014 that there "has been no significant improvement in freedom of information" in Iran despite the election of "moderate conservative" Hassan Rouhani as President of Iran in June 2013 (RSF 18 June 2014). RSF further noted that the judiciary and intelligence agencies continue to subject journalists and "netizens" [1] to "injustices and persecution" (ibid.). This is corroborated by the New York-based International Campaign for Human Rights in Iran (ICHRI) [2], which states in their report entitled *Internet in Chains: The Front Line of State Repression in Iran* that hardliners in the security and intelligence services are "active in the persecution of online activists" and that arrests of online activists has increased since Rouhani's inauguration (ICHRI Nov. 2014, 36).

Based on a joint submission by the International Federation for Human Rights (FIDH) and the Paris-based League for the Defence of Human Rights in Iran (LDDHI), the UN Human Rights Council indicates that in the period between 2009 and 2013, authorities banned 35 news publications, issued 106 warnings to news media, and revoked the licenses of 11 news publications and 1 news agency (UN 7 Aug. 2014, para. 49). RSF indicates that Iranian authorities closed 14 news media outlets between June 2013 and June 2014 (RSF 18 June 2014).

1.1 Islamic Republic of Iran Broadcasting (IRIB)

Sources indicate that the IRIB is the national radio and television broadcast service in Iran, which holds a state monopoly on broadcasted news within Iran (ICHRI June 2014, 3; IHRR [2011]; US 27 Feb. 2014, 20). On its website, the IRIB describes itself as taking a "key role in strengthening the country's cultural solidarity" in opposition to the "domineering empire of Western Media" (Iran n.d.).

In a June 2014 report entitled *Iran's State TV: A Major Human Rights Violator*, the ICHRI indicates that the IRIB interrupts, or "jams" television and radio signals entering Iran in order to control access to information, particularly targeting Persian-language foreign broadcasts (ICHRI June 2014, 4). Freedom House also states that satellite broadcasting from outside Iran is subjected to "heavy jamming" (Freedom House 2013, 3). ICHRI notes that satellite broadcasts are also blocked internally within Iran and the jamming is directed against both the broadcasting satellites and the local receptors (June 2014, 4-5).

The ICHRI describes the IRIB as "an integral part of the country's security and intelligence apparatus" and states that the IRIB "broadcasts show trials and false 'news' reports to conceal human rights violations, and airs defamatory content to discredit dissidents" (ICHRI June 2014, 3). The ICHRI explains:

> Detainees are routinely forced, often under torture or threats to themselves and their families, to 'confess' to crimes, and the IRIB films and broadcasts these forced confessions as a form of public intimidation and humiliation. ... These forced confessions are then the principal 'evidence' typically presented in courts to convict targeted individuals, usually on various national security-related charges. (ibid., 6)

Similarly, an Iranian journalist in France told RSF that "'investigators subject journalists to psychological pressure during questioning so that they confess to espionage activities'," and that the confessions are filmed and broadcast on TV (RSF 2013).

The ICHRI also reports that the IRIB has targeted Iranian journalists working abroad:

> Intelligence and security agents have contacted these journalists abroad, through online and social networking sites, threatening harm to them and their families inside Iran, if they do not cease their journalistic and media activities. Several of these exiled journalists have told the Campaign [ICHRI] that such harassments and intimidations usually follow in tandem with broadcast of IRIB programs targeting and attacking them. This is another indication of the close working relationship between IRIB and the security and intelligence services in charge of implementing repression and censorship. (ICHRI June 2014, 8)

Further information about the IRIB's relationship with Iranian security and intelligence authorities could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

2. Government Bodies Related to the Internet

Iran has several regulatory bodies with mandates to control access to the Internet (Article 19 2013, 16; US 27 Feb. 2014, 23). Article 19, a London-based NGO with several offices worldwide and 90 global partners that campaigns to defend freedom of expression and freedom of information (Article 19 n.d.), expressed the opinion that all of these regulatory bodies are "ultimately accountable to and supervised by Iran's Supreme leader" (ibid., 16).

2.1. Supreme Council for Cyberspace (SCC)

Sources indicate that the Supreme Council for Cyberspace (SCC) [or Supreme Cyberspace Council] was established to determine Iran's Internet policies and coordinate Internet-related bodies (RSF 2013; Article 19 2013, 17; US 27 Feb. 2014, 23). According to ICHRI, it was established under the orders of Supreme Leader Khamenei and "is the highest authority responsible for general policy regarding cyberspace" (ICHRI Nov. 2014, 19). Small Media, a UK-based organization that promotes the "free flow of information in closed societies, especially Iran" (Small Media n.d.), explains that the SCC is responsible for "the general direction and manner of Internet filtering and infrastructure development" (ibid. Apr. 2014, 3). The SCC was reportedly created in 2012 (RSF 2013; Small Media Apr. 2014, 4; ICHRI Nov. 2014, 19). Members include Iran's President and the head of the judiciary (ibid.; Article 19 2013, 17).

2.2 Commission to Determine the Instances of Criminal Content (CDICC)

Sources indicate that Iran has a government body called the Commission to Determine the Instances of Criminal Content (CDICC) (Small Media Apr. 2014, 3), also referred to by sources as the Committee in Charge

of Determining Unauthorized Websites (Freedom House 2013, 11; US 27 Feb. 2014, 23) or the Committee Charged with Determining Offensive Content (CCDOC) (Article 19 2013, 17). It implements the SCC's decisions regarding Internet filtering and blocking sites (US 27 Feb. 2014, 23). Small Media explains that the CDICC is responsible for "the day to day decisions about individual filtering actions" and "tasked with monitoring cyberspace, and filtering criminal Internet content" (Apr. 2014, 3). Similarly, multiple sources state that the CDICC identifies the sites that carry prohibited content and communicates the information to the Telecommunications Company of Iran (TCI) [Iran's main provider of Internet and mobile phone service (Freedom House 2013, 6)] and other major Internet Service Providers (ISPs) for blocking (Article 19 2013, 17; Freedom House 2013, 11; ICHRI Nov. 2014, 18).

Sources indicate that the CDICC is headed by the Prosecutor General (Article 19 2013, 17; Small Media Apr. 2014, 3; Freedom House 2013, 11). According to Small Media, there are 13 members in the CDICC, most of whom are appointees of parliament or of the Supreme Leader Ayatollah Ali Khamenei (Small Media Apr. 2014, 3). Its membership includes the Chief of Police and representatives from the Ministry of Intelligence, the Ministry of Islamic Guidance, the Ministry of Science and the Ministry of Information and Communication Technology (Article 19 2013, 17; Small Media Apr. 2014, 3). According to Freedom House, there is little information about the internal processes of the committee and their "censorship decisions are often arbitrary and non-transparent" (2013, 11). Article 19 notes that the SCC and CCDOC have seven members in common, "which allows for effortless policy diffusion and institutional alignment" (2013, 17).

2.3 Internet Policing

Sources indicate that Iran has a Cyber Police unit (FATA) [or FETA (RSF 2013)] (Article 19 2013, 17; US 27 Feb. 2014, 23). According to Article 19, in November 2009, the Iranian authorities established a Web Crimes unit to police the Internet for "'insults and lies'" (2013, 20). The ICHRI states that the Cyber Police unit was established by the Iranian national police force in 2011, and its duties include monitoring the activities of activists (ICHRI Nov. 2014, 33). The same source states that the unit "pursues, through harassment, arrest, and interrogation, any citizen who expresses dissenting views online" (ibid.). According to the head of Tehran's Cyber Police unit, as reported by ICHRI, staff working in the Cyber Police's "Determination and Prevention Unit" are required to "surf the Internet and monitor different websites, blogs, social networks, chat rooms, and similar online spaces, to ensure that no crimes take place" (ICHRI 3 Feb. 2014). The head of Tehran's Cyber Police unit stated that their unit does not enter Internet users' "private domain," such as e-mails and two-person chat sessions (ibid.). However, ICHRI reports that the cyber police pressures Internet providers to supply them with evidence to pursue online activists and cited an example in which a Tehran-based Internet provider "publicized FATA's attempts to illegally obtain personal information about one of its online customers" (ICHRI Nov. 2014, 33).

2.4 Cyber Army

Sources indicate that Iran has a "Cyber Army" [or "Cyber Defence Command" (Article 19 2013, 15)] that operates under the Revolutionary Guards (ICHRI 2013, 23; US 27 Feb. 2014, 23; Article 19 2013, 15). According to the ICHRI, it was created in the wake of the 2009 election protests and "is charged with attacking and bringing down any domestic website that engages in activities the authorities perceive as transgressive--as well as hacking and disrupting the websites of perceived foreign enemies" (Nov. 2014, 34). Similarly, Article 19 states that this body is "responsible for monitoring potentially subversive Internet activity and for hacking into various well-known platforms and websites that are perceived as threats to the regime's stability" (Article 19 2013, 15). The ICHRI states that there is little known about the structure and makeup of the Cyber Army and that it functions "extra-judicially," "without court order or any responsible official that a citizen or organization can question or hold accountable" (ICHRI Nov. 2014, 35).

The ICHRI reports that the Cyber Army has been responsible for mounting "denial of service attacks" (flooding the sites with so much traffic that they are unable to maintain online service) against websites critical of the government, as well as "actively hacking the e-mails, Facebook pages, and Twitter accounts of students and activists in order to access their private information, all without warrants or just cause" (2013, 23).

According to IHRDC, 13 websites belonging to human rights organizations and opposition groups outside Iran were hacked by Iran's "Cyber Army" (IHRDC 14 June 2013). The same source states that there were reports that Iranian government authorities tried to hack the e-mail accounts of several thousand Gmail users in Iran (ibid.).

According to Freedom House, Iranian authorities hacked "numerous" Facebook accounts of Iranian users that were deemed to be "un-Islamic" and posted a statement saying "'By judicial order, the owner of this page has been placed under investigation'" (Freedom House 2013, 18). The same source reports that Iran has "significantly increased its hacking capabilities in recent years" and has announced plans to recruit and train hackers (ibid.).

3. Iranian Internet Surveillance Practices

RSF explains that Iran "possesses a technological and legislative arsenal that allows it to keep its Internet under close surveillance" and that "[f]iltering, control of Internet Service Providers, prohibitions, and monitoring of email content, chats and VoIP conversations are all legal" (RSF 2013).

3.1 Filtering, Monitoring and Censoring

Several sources indicate that Iran has a centralized system for filtering, monitoring and censoring content on the Internet (UN 7 Aug. 2014, para. 50; RSF 2013; Freedom House 2013, 7, 14-15). According to RSF, Iran's government "controls infrastructure, technology and regulatory bodies" for the Internet (RSF 2013).

Sources indicate that there were approximately 150 Internet Service Providers (ISPs) in Iran as of 2013, and although many are privatized, they are not "fully independent" of the government (Article 19 2013, 9; RSF 2013). The largest ISP is the Data Communication Company of Iran (DCI), which is owned by the Revolutionary Guards (RSF 2013; Article 19 2013, 9). Article 19 explains that, in terms of policy,

> all private ISPs must be vetted by both the Data Communication Company of Iran (DCI) and the Ministry of Culture and Islamic Guidance [MCIG] for approval before being issued a licence to operate. ... This level of centralisation allows the government to monitor, filter, slow or shut off all Internet use in the country. (ibid., 13)

The US Department of State's *Country Reports on Human Rights Practices for 2013* similarly states that all ISPs must be approved by the MCIG and that websites and blogs within Iran must also register with the MCIG (US 27 Feb. 2014, 23).

Article 19 notes that Iran has a "sophisticated censorship apparatus" and suppresses "digital activism" (2013, 6). Similarly, *Country Reports 2013* states that the Iranian government used "sophisticated filtering technology" to rapidly restrict access to "newly published Internet content" (US 27 Feb. 2014, 23).

According to RSF, while the Iranian government "does not yet have the resources for keeping millions of Internet users under surveillance", Iranian authorities do monitor access to sites both within Iran and abroad and "anything straying from the official line is automatically deemed to be 'political' and subject to filtering or surveillance" (RSF 2013). Further, RSF notes that the Iranian authorities monitor the Internet using "filtering mechanisms" as well as "data interception tools of the Deep Packet Inspection (DPI) type," which "can be used to analyse email content, track browsing history and block access to sites" (ibid.). Similarly, the ICHRI reports that Iranian authorities are using "more complex and undetectable filtering methods" that, in addition to limiting access to Internet sites, "put users' communication security at risk, making them vulnerable to hackers wishing to access their Internet communications" (ICHRI 3 Feb. 2014). The ICHRI notes that "[t]he new filtering system has substantially improved the government's ability to perform wire tapping and online surveillance of users" (ibid.).

Sources indicate that products designed by Chinese and some Western companies have been used by Iranian authorities to monitor their citizens online (RSF 2013; Freedom House 2013, 17), despite international restrictions against selling surveillance equipment to Iran (ibid.).

According to RSF, mobile phone messaging through the Internet, such as through WhatsApp, Tango and Viber, is also subjected to blocking, interception and surveillance and is monitored by Iranian authorities (9 Oct. 2014). Similarly, according to *Country Reports 2013*, mobile communications, including cell phones, are subjected to the same restrictions as other Internet activity (US 27 Feb. 2014, 24).

RSF explains that on dates that could give rise to demonstrations, the Internet speed is slowed down to "prevent the circulation of photos and videos" (RSF 2013). According to the Iran Human Rights Documentation Center (IHRDC), a New Haven-based NGO whose mission is to establish a "comprehensive and objective historical record of the human rights situation in Iran" (IHRDC n.d.a), in the lead up to the June 2013 elections, people experienced difficulties with slow Internet speeds, accessing e-mail and faulty proxy servers (IHRDC n.d.b). Small Media explains that during the lead-up to the election, "within the course of six weeks, Iran's Internet progressed from its relative state of normality, to a nearly unusable network, whitelisted and throttling, and then overnight back to a routine set of restrictions" (Small Media June 2013, 2).

The Washington Post reported on a professor at the University of Michigan, who conducted a study on Iranian Internet censorship with the help of two Iranians inside Iran in the weeks before the June 2013 election (15 Aug. 2013). The professor's research found that Internet traffic that used "encrypted SSH protocol, which can be used to 'tunnel' other types of traffic out of the country" ran at less than 20 percent of the network's full speed, while traffic that the firewall did not recognize was severed after 60 seconds (ibid.). The study found that after the election, the throttling stopped and the Internet traffic returned to being transmitted at its normal speed (ibid.).

In the week leading up to the 2013 election, throttling and disruption also "increased in aggressiveness" and median Internet speeds slowed to less than 50 kbps, which is less than a dial-up modem (Small Media June 2013, 9).

Sources note that Iranian authorities limit the speed of the Internet for home users within Iran to 128 Kbps (ICHRI 2013, 23; *The Washington Post* 15 Aug. 2013), which is approximately 50 times slower than typical speeds in the US (ibid.). In 2012, the Minister of Communications said that the Internet speed was limited because of "security reasons" (ICHRI 2013, 23).

3.2 Blocking Sites

According to the UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, approximately five million websites are blocked in Iran (UN 27 Aug. 2014, para. 32). According to the IHRDC, authorities block 150,000 websites each month (IHRDC 23 May 2014). The UN Special Rapporteur indicates that the top 500 blocked websites include many dedicated to arts, news and social issues (UN 27 Aug. 2014, para. 32). Similarly, Freedom House reports that Iranian authorities restrict access to "tens of thousands" of websites, including international news sources, opposition, ethnic and religious minorities, and those related to human rights; in addition, authorities restrict access to Persian-language music blogs, dating sites, digital security information, and movie download hubs (Freedom House 2013, 6, 10). According to RSF, blocked websites include independent news and opposition websites, as well as fashion, cuisine and music websites (RSF 2013).

According to Article 19, the Skype and Viber websites were blocked during the lead up to the 2013 elections (2013, 22).

Sources indicate that many social media websites are blocked (UN 27 Aug. 2014, para. 33; BBC 21 May 2014), including:

- Facebook (UN 27 Aug. 2014, para. 33; IHRDC 23 May 2014; US 27 Feb. 2014, 23);
- Twitter (UN 27 Aug. 2014, para. 33; IHRDC 23 May 2014; US 27 Feb. 2014, 23);
- Instagram (UN 27 Aug. 2014, para. 33; IHRDC 23 May 2014);
- YouTube (US 27 Feb. 2014, 23), and
- WeChat (UN 27 Aug. 2014, para. 33).

Freedom House explains the process for filtering and blocking websites as follows:

> Iranian authorities employ a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private ISPs are forced to either use bandwidth provided by the government or route their traffic (which contains site-visit requests) through government-issued filtering boxes developed by software companies inside Iran. The filtering boxes search for banned test strings--either keywords or domain names--in the URL requests submitted by users, and block access accordingly. (2013)

3.3 Use of Virtual Private Networks (VPNs)

Sources indicate that millions of Iranians use Virtual Private Networks (VPNs) to circumvent the filters of the Iranian authorities (ICHRI 14 May 2014; Small Media Aug. 2014, 3). VPNs allow the user to send and receive encrypted and uncensored data through shared or public networks outside the country (ICHRI 14 May 2014). Freedom House notes that the use of VPNs and other circumvention tools has "grown dramatically since 2009" (Freedom House 2013, 3). Small Media reports that, according to a report by Iran's Ministry of Youth and Sports, 69.3 percent of Iranian youth use circumvention technologies, such as VPNs and proxies (Aug. 2014, 3). Small Media also states that although Iran's cyber police has tried to restrict the sale of VPNs, Iranians can buy them online (Small Media Aug. 2014, 4).

ICHRI reports that Iranian authorities have targeted access to VPNs, "by shutting down VPN ports and simultaneously offering and encouraging the use of 'legal VPNs' that are provided by a government organization" (ICHRI Nov. 2014, 29). ICHRI notes that government efforts to shut down VPNs have come in waves, including during the 2009 post-election crackdown, in October 2011, and again in May 2013 (ibid., 30). Other sources similarly report that in the run-up to the June 2013 elections, most VPNs, which were used to bypass government filters, were blocked (Article 19 2013, 22; Small Media June 2013, 8). Small Media notes that after most VPNs were blocked in March of 2013 and the public shifted to a different set of circumvention tools, Iranian authorities responded in May of 2013 by "imposing a 'white list' system, blocking unknown connections after exactly sixty seconds" (ibid.). Freedom House likewise reports that Iranian authorities blocked VPNs in March and May of 2013 during the led up to the June 2013 election (Freedom House 2013, 3).

According to ICHRI, the Iranian parliament is discussing a bill that would ban VPNs (ICHRI Nov. 2014, 30), which Iran's Cyber Police chief reportedly supports (ICHRI 14 May 2014).

Small Media reported that, despite the fact that VPN sales are not "explicitly outlawed," Iran's Cyber Police have arrested a number of people for selling VPNs, and provided examples of four arrests in 2013 and 2014 that occurred in Qazvin, Tehran, Razavi and Kerman provinces (Small Media Aug. 2014, 4). Corroborating information could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

3.4 National Internet

Sources indicate that the Iranian government is in the process of creating a national Internet for use within Iran (RSF 2013; Freedom House 2013, 2; UN 27 Aug. 2014, para. 31), which is known by several names, including "National Information Network" (RSF 2013; Small Media Mar. 2014, 3). SHOMA (Small Media Mar. 2014, 3), "Halal Internet" (RSF 2013; Small Media Mar. 2014, 3), and "Clean Internet" (ibid.).

According to ICHRI, key components of the National Information Network are to include:

- national data centres, which will "house the various telecommunications and storage systems used by the network and process all the information flowing across the Network",
- national SSL security certificates issued by the government or government-controlled agencies,
- A national web browser,
- A national operating system,
- national search engines and social networks,
- national e-mail programs, and
- national VPNs (ICHRI Nov. 2014, 22-30).

RSF explains that Iran's national Internet is planned to have a high connection speed, but to be "fully monitored and censored" and to have the development of e-mail, search engines and social networks under government control (2013). ICHRI similarly states that the national Internet "will only provide access to content approved by the Iranian government and will include built-in surveillance of all online activity, including e-mail and other personal correspondence" (2013, 22, 23).

Small Media explains that the government's objectives in the development of the National Information Network is not intended to replace the access to the worldwide Internet, but is intended to be a "private and secure internal network," with a private component for internal communication between governmental organizations, and a public component for users to make use of public services with higher speeds and lower costs for accessing data within Iran (Mar. 2014, 3).

According to RSF, the government plans to decrease the speed of the international Internet and to increase its cost, in order to make subscribing to the national Internet more appealing (RSF 2013).

According to Small Media, the national Internet is scheduled to launch in March of 2016, but has missed several earlier launch dates ranging from 2006 to 2013 and has had a "lengthy and troubled development process" (Small Media Mar. 2014, 3, 6). The ICHRI reports that the different components of the national Internet are progressing, although "unevenly and behind schedule," and that an official announced in April 2014 that the national Internet became "fully operational for government offices" (ICHRI Nov. 2014, 30).

3.5 Internet Cafes

Sources indicate that in 2012, new guidelines were introduced that require Internet cafes to install surveillance cameras and retain personal information of users, along with a record of the websites that they visited, for six months (Article 19 2013, 22; RSF 2013; Freedom House 2013, 17). According to RSF, these guidelines were introduced by the cyber police (RSF 2013). The Secretary-General of the UN reported that the "cyber-police have shut down numerous Internet cafes that had permitted access to social media websites" (UN 12 Aug. 2014, para. 34). *Country Reports 2013* similarly notes that in July of 2013, the police inspected 352 Internet cafes and closed 67 of them for providing "'illegal services' to youth" (US 27 Feb. 2014, 24).

4. Legislation

According to RSF, the 1986 Press Law does not allow news providers to "attack the Islamic Republic," "insult the Supreme leader," or "disseminate false information" (RSF 2013). Amendments in 2000 and 2009 include the addition of online publications to the law and requiring online publications to obtain a license (ibid.).

The Iranian parliament approved the Computer Crime Law (CCL) in January 2010 (Article 19 2013, 9). According to Article 19, the law contains "vaguely" defined offences, such as "'crimes against public morality and chastity' and the 'dissemination of lies'" that "criminalise legitimate expression" (ibid.). Sources indicate that the death penalty can be imposed for computer crimes committed "against public morality and chastity" (ibid.; Freedom House 2013, 14). Other punishments include "lengthy" prison sentences, "draconian fines," (ibid.; Article 19 2013, 9) and "judicial orders for the closure of organisations and the banning of individuals from using electronic communications" (ibid.). According to RSF, "posting illegal content or using roundabout methods to access blocked content is punishable by long jail terms" (RSF 2013). Sources indicate that the CCL also punishes the service providers if material is posted contrary to government restrictions (Freedom House 2013, 14; Article 19 2013, 9). According to Article 19, the CCL has been "instrumental in persecuting and repressing cyber-activists and bloggers" (ibid.).

5. Arrests and Detention of Journalists and Netizens

The UN Special Rapporteur reported that at least 35 journalists are in detention and many others allege "harassment, interrogations and surveillance" (UN 27 Aug. 2014, para. 24). Similarly, CPJ states that Iranian reporters are routinely subjected to "detention, investigation, and criminal charges" (CPJ Feb. 2014). According to CPJ, there were at least 40 journalists imprisoned in Iran during the lead-up to the 2013 elections, on charges such as "spreading propaganda against the state," "acting against national security," or "insulting the supreme leader" (Feb. 2014).

RSF reports that a journalist who was arrested in 2010 said that intelligence officers had printouts of his e-mails, SMS messages, and transcripts of phone conversations when questioning him, and that other inmates had similar experiences (RSF 2013). The same source stated that "[s]uch interrogation methods are widespread and are indicative of the degree to which journalists are spied on in Iran" (ibid.).

According to RSF, there were 25 journalists and netizens arrested between June 2013 and June 2014, a total of 58 journalists and netizens being held in detention as of June 2014 (RSF 18 June 2014), and a total of 28 netizens detained as of October 2014 (RSF 9 Oct. 2014).

Freedom House reports that Iranian Internet users face "routine surveillance, harassment, and the threat of imprisonment for their online activities" and that, since June of 2009, "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" (2013, 14-15).

Freedom House also reports that in 2011 and 2012, four people were sentenced to death because of web designing or online blogging on charges related to "insulting religion" or "conspiring with foreign enemies" (ibid., 15). In one example, Freedom House notes that a web designer was sentenced to death for "insulting and desecrating Islam" because a software program he designed was used to upload pornography without his knowledge (ibid.).

Freedom House further reports that there has been an increase in arrests of Internet users based on their Facebook activity (2013, 16). For example, in October 2012, the same source reported that four people were arrested in Sirjan for "antigovernment activities and insulting officials on Facebook" and people who created a Facebook page that published photos of Iranian girls were charged with "promoting 'vulgarity and corruption among Iranian youths'" (ibid.).

Several sources indicate that in 2012, a blogger died while being held in custody (CPJ Feb. 2014; AI 7 Mar. 2013, 2; Freedom House 2013, 15). He had reportedly been held in custody for four (Freedom House 2013, 15) or five days (CPJ Feb. 2014). CPJ reported that the blogger was never charged or tried (ibid.). Amnesty International (AI) noted that there were "allegations of torture," but that as of March 2013, no alleged perpetrators had been brought to court (7 Mar. 2013). According to Freedom House, the head of the Tehran Cyber Police was dismissed for "'shortcomings in the supervision and handling of the case'" (2013, 15).

Sources report that a dual Iranian-UK citizen, who was arrested when travelling to see family in Iran, was sentenced in May 2014 to 20 years in prison because of comments she posted on Facebook (*The Times* 30 May 2014; *The Independent* 31 May 2014; UN 27 Aug. 2014, para. 27). Her husband reportedly told *The Independent* that she had made Facebook comments calling the government "'too Islamic'" and was charged after confessing "'under duress'" (*The Independent* 31 May 2014). The same source notes her charge sheet accused her of "'gathering and participation with intent to commit crime against national security'" and "'insulting Islamic sanctities'"(ibid.). According to the UN, in May of 2014, she was one of eight people who were convicted and sentenced to a total of 123 years in prison for "blasphemy, insulting the Supreme Leader and spreading propaganda against the system, among other charges" because of their activity on Facebook (UN 27 Aug. 2014, para. 27). Media sources corroborate this and note that the prison sentences of the other individuals ranged from 7 years to 20 years (*The Times* 30 May 2014; *The Independent* 31 May 2014).

Sources report that in May 2014, six people were arrested for making a YouTube video, in which they danced to the song "Happy" (UN 12 Aug. 2014, para. 35; ICHRI 11 Sept. 2014; BBC 21 May 2014). The video featured three men and three unveiled women dancing in the streets and on rooftops in Tehran (ibid.). The police chief said the video "'hurt public chastity'" (ibid.). The video participants reportedly confessed on Iran's state-run TV to making the video (ibid.; ICHRI 11 Sept. 2014) before being formally charged (ibid.). According to ICHRI, the six youths were detained for two days in May 2014 and released after posting bail of approximately $10,000 to $16,000 each (ibid.). The director of the video was arrested on 20 May 2014 and released 9 days later after posting bail of $16,000 (ibid.). The trial against the seven individuals began on 9 September 2014, where they faced charges for "'participation in producing a vulgar video clip' and conducting 'illicit relations' with one another" (ibid.). The defendants' lawyers reportedly "objected to the brutal police treatment of the suspects and raids on their homes during the arrests" (ibid.).

In September 2014, approximately 11 people were arrested for circulating jokes about the Ayatollah Khomeini through the mobile phone apps WhatsApp, Tango and Viber (RFE/RL 22 Sept. 2014; RSF 9 Oct. 2014; BBC 23 Sept. 2014). The Iranian judiciary also reportedly instructed government authorities to ban access to WhatsApp, Viber and Tango (ibid.; RFE/RL 22 Sept. 2014).

This Response was prepared after researching publicly accessible information currently available to the Research Directorate within time constraints. This Response is not, and does not purport to be, conclusive as to the merit of any particular claim for refugee protection. Please find below the list of sources consulted in researching this Information Request.

Notes

[1] A "netizen" is a blend of "net" and "citizen" and is defined as "an active participant in the online community of the Internet" (Merriam-Webster n.d.).

[2] The International Campaign for Human Rights in Iran (ICHRI) is a New York-based human rights organization composed of lawyers, researchers and journalists, that aims to provide "relevant, verified, and up-to-date information about the human rights situation in Iran" (ICHRI n.d.).

References

Amnesty International (AI). 7 March 2013. *Letter to the Permanent Representatives of Members of the UN Human Rights Council*. (MDE 13/011/2013) <http://www.amnesty.org/en/library/asset/MDE13/011/2013/en/b0aa91a8-eda0-4788-a424-2b20c8d7530b/mde130112013en.pdf> [Accessed 2 Dec. 2014]

Article 19. 2013. *Computer Crimes in Iran: Online Repression in Practice*. <http://www.article19.org/data/files/medialibrary/37385/Computer-Crimes-in-Iran-.pdf> [Accessed 13 Nov. 2014]

_____. N.d. "What We Do." <http://www.article19.org/pages/en/what-we-do.html> [Accessed 2 Dec. 2014]

British Broadcasting Corporation (BBC). 23 September 2014. "Iran Police Chief not in Favour of Blocking Social Networks." (Factiva)

_____. 21 May 2014. "Iranian Pharrell Fans Arrested for Happy Tribute Video." <http://www.bbc.com/news/entertainment-arts-27499642#> [Accessed 21 May 2014]

Committee to Protect Journalists (CPJ). February 2014. D. Parvaz. "Hassan Rouhani and the Hope for More Freedom in Iran." <http://cpj.org/2014/02/attacks-on-the-press-iran.php> [Accessed 17 Nov. 2014]

_____. N.d. "Our Mission." <http://www.cpj.org/about/video.php> [Accessed 2 Dec. 2014]

Freedom House. 2013. "Iran." *Freedom on the Net 2013*. <https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Iran.pdf> [Accessed 14 Nov. 2014]

The Independent. 31 May 2014. Chris Green. "Briton 'Gets 20 Years for Criticising Iran on Facebook'." (Factiva)

International Campaign for Human Rights in Iran (ICHRI). November 2014. *Internet in Chains: The Front Line of State Repression in Iran*. <http://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf> [Accessed 3 Dec. 2014]

_____. 11 September 2014. "'Happy' Youths Go on Trial in Tehran." <http://www.iranhumanrights.org/2014/09/happy-trial-2/> [Accessed 13 Nov. 2014]

_____. June 2014. *Iran's State TV: A Major Human Rights Violator. IRIB Briefing Paper*. <http://www.iranhumanrights.org/wp-content/uploads/IRIB_Briefing-FINAL.pdf> [Accessed 13 Nov. 2014]

_____. 14 May 2014. "Bill to Ban VPNs Would Cut Internet Access." <http://www.iranhumanrights.org/2014/05/vpn-bill/> [Accessed 17 Oct. 2014]

_____. 3 February 2014. "Iran's New Methods of Internet Filtering Put Users at Risk." <http://www.iranhumanrights.org/2014/02/internet-ssl/> [Accessed 14 Oct. 2014]

_____. 2013. *Fulfilling Promises: A Human Rights Roadmap for Iran's New President*. <http://www.iranhumanrights.org/wp-content/uploads/Fulfilling-Promises-English-web.pdf> [Accessed 13 Nov. 2014]

_____. N.d. "Background." <http://www.iranhumanrights.org/background-2/> [Accessed 2 Dec. 2014]

Iran. N.d. Islamic Republic of Iran Broadcasting. "IRIB at a Glance." <http://www.irib.ir/English/AboutUs/index.php> [Accessed 21 Nov. 2014]

Iran Human Rights Review (IHRR). [2011]. Ali Sheikholeslami. *The Role of Iran Broadcasting in Blocking Access to Information*. <http://www.ihrr.org/wp-content/uploads/ihrr/articles/2011/5//528_auto-draft.pdf> [Accessed 21 Nov. 2014]

Iran Human Rights Documentation Center (IHRDC). 23 May 2014. Ben Richmond. "Why Iran Is Banning Instagram." <http://www.iranhrdc.org/english/english/news/in-the-news/1000000472-why-iran-is-banning-instagram.html?print> [Accessed 13 Nov. 2014]

_____. 14 June 2013. "Harassment and Censorship Continue on Election Day." <http://www.iranhrdc.org/english/news/inside-iran/1000000333-harassment-and-censorship-continue-on-election-day.html> [Accessed 28 Oct. 2014]

_____. N.d.a. "About Us." <http://www.iranhrdc.org/english/mission.html> [Accessed 8 Jan. 2015]

_____. N.d.b. "IHRDC News." <http://www.iranhrdc.org/english/ihrdc-news.html> [Accessed 28 Oct. 2014]

Merriam-Webster Dictionary. N.d. "Netizen." <http://www.merriam-webster.com/thesaurus/netizen> [Accessed 2 Dec. 2014]

Radio Free Europe/Radio Liberty (RFE/RL). 22 September 2014. "Iranians Arrested Over Khomeini-Insult Texts." (Factiva)

Reporters sans frontières (RSF). 9 October 2014. "Iran--Twelve Arrested Over Mobile Phone Message Content." <http://en.rsf.org/iran-twelve-arrested-over-mobile-phone-09-10-2014,47080.html> [Accessed 17 Nov. 2014]

_____. 18 June 2014. "Freedom of Information Still Flouted a Year After Rouhani's Election." <http://en.rsf.org/iran-freedom-of-information-still-18-06-2014,46470.html> [Accessed 20 Nov. 2014]

_____. 10 March 2014. "Who We Are." <http://en.rsf.org/who-we-are-12-09-2012,32617.html> [Accessed 2 Dec. 2014]

_____. 2013. "Iran." *The Enemies of Internet*. <http://surveillance.rsf.org/en/iran/> [Accessed 25 Sept. 2014]

Small Media. August 2014. *Iranian Internet Infrastructure and Policy Report*. <http://smallmedia.org.uk/sites/default/files/u8/IIIP_Aug2014.pdf> [Accessed 14 Nov. 2014]

_____. April 2014. *Iranian Internet Infrastructure and Policy Report*. <http://smallmedia.org.uk/sites/default/files/u8/IIIP_April2014.pdf> [Accessed 14 Nov. 2014]

_____. March 2014. *Iranian Internet Infrastructure and Policy Report*. <http://smallmedia.org.uk/sites/default/files/u8/IIIP_March2014.pdf> [Accessed 14 Nov. 2014]

_____. June 2013. *Iranian Internet Infrastructure and Policy Report. Election Edition 2013*. (April-June 2013). <http://www.smallmedia.org.uk/IIIPJune.pdf> [Accessed 14 Nov. 2014]

_____. N.d. "Get in Touch." <http://smallmedia.org.uk/content/get-touch> [Accessed 2 Dec. 2014]

The Times. 30 May 2014. Anna Dubuis. "Briton 'Devastated' Over 20-year Sentence for Criticising Iran Leadership." (Factiva)

United Nations (UN). 27 August 2014. *Situation of Human Rights in the Islamic Republic of Iran. Note by the Secretary-General*. (A/69/356) <http://www.ecoi.net/file_upload/1226_1414752324_n1451883iran.pdf> [Accessed 17 Nov. 2014]

_____. 12 August 2014. *Situation of Human Rights in the Islamic Republic of Iran. Report by the Secretary-General*. (A/69/306) <http://www.ecoi.net/file_upload/1226_1414498522_n1450284-iran.pdf> [Accessed 17 Nov. 2014]

_____. 7 August 2014. Human Rights Council. *Summary Prepared by the Office of the United Nations High Commissioner for Human Rights in Accordance with Paragraph 15 of the Annex to Human Rights Council Resolution 5/1 and Paragraph 5 of Annex to Council Resolution 16/21*. (A/HRC/WG.6/20/IRN/3) <http://www.ecoi.net/file_upload/1930_1414592765_g1411344.pdf> [Accessed 17 Aug. 2014]

United States (US). 27 February 2014. "Iran." *Country Reports on Human Rights Practices for 2013*. <http://www.state.gov/documents/organization/220564.pdf> [Accessed 21 Nov. 2014]

The Washington Post. 15 August 2013. Timothy B. Lee. "Here's How Iran Censors the Internet." <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/heres-how-iran-censors-the-internet/> [Accessed 25 Sept. 2014]

Additional Sources Consulted

Internet sites, including: ecoi.net; Factiva; Human Rights Watch; Institute for War and Peace Reporting; International Federation for Human Rights; Iran – Ministry of Information and Communication Technology, President's website; Iran Media Program; Observatory for the Protection of Human Rights Defenders; Telecommunication Company of Iran; United States – Congressional Research Service; United Nations – Refworld, ReliefWeb.
