Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**571**
Land:	Iran
Kilde:	Udlændingestyrelsen
Titel:	Country of Origin Information; Internet Control and Filtering in Iran
Udgivet:	24. juni 2014
Optaget på baggrundsmaterialet:	25. juni 2014

UDLÆNDINGESTYRELSEN
DANISH IMMIGRATION SERVICE

Date: June 24, 2014

Internet Control and Filtering in Iran

Internet Control and Filtering in Iran

The following information is based on statements made by Mahmood Enayat, Director of Small Media (London) on Internet Control in Iran connection with a seminar in February of 2014,[1] followed by communications with Enayat in April of 2014. In addition, information from publications from Small Media (Small Media, Iranian Internet Infrastructure and Policy Report, February 2014) and The Iran Media Program on the control of Internet in Iran (Internet Censorship in Iran: An Infographic, March 13, 2013) and Freedom House's Freedom on the Net report from 2013 on Iran (Freedom House, Freedom on the Net 2013 - Iran, 3 October 2013 have been included).

Internet censorship in Iran

Mahmood Enayat, Director of Small Media, said that despite statements of intentions of acting towards a less censored Internet in Iran, the new president Hassan Rouhani has not done anything in respects to freedom of expression on the Internet. Nothing has been enacted or promoted. In fact, the number of internet activists that have been arrested has gone up in 2014.[2]

President Rouhani's behaviour internationally in which he can be perceived as a reformist for example with regards to nuclear negotiations and efforts towards lifting of sanctions, is no reflection of a true change of course in Iran, at least domestically. He and other Iranian officials may be avid users of channels such as Twitter and Facebook which most of all is a means of accessing different audiences and mostly for international consumption. There are no indications of focus on domestic issues in this respect.[3]

However, in terms of activism on the Internet, Mahmood Enayat considered that with the election of Rouhani as president, there has been a change of mood and people are generally more hopeful and optimistic which results in many online activists feeling less restricted to express themselves. Risks are indeed still there however and self-censorship among users has slightly decreased.[4]

---

[1] Seminar arranged by the Norwegian Country of Origin Information Centre, Landinfo, in Oslo Norway, February 24, 2014
[2] Mahmood Enayat, Director of Small Media (London), on Internet Control in Iran connection with a seminar, February 24 of 2014
[3] Enayat, February 2014
[4] Enayat, February 2014

It has been Iranian policy to build a national information network (also called SHOMA) which implies an intention to build the infrastructure in order to manage all data internally, so internet traffic does not go outside of the Iranian net. This policy has been motivated by both the wish to provide better service to Iranians as well as tightening of control and security so as to ensure that sensitive data does not leave the country. Security concerns have so far had the upper hand when it comes to Iranian Internet policy, however, development and economic interests are influencing factors that must be balanced against this. Iran wishes both to strengthen capacity to offer online services that the people want and to control the Iranians and what they access.[5]

Finally, it was mentioned that up to the presidential elections in 2013, the government went to extensive measures to shut down the Internet. The Internet was slowed down and all circumvention tools, used to bypass filters, were shut down. The day after the elections, the Internet was 'switched back' to normal. In 2014, there have been no disruptions of this sort. [6]

Obstacles to Internet

With regard to Iranians' access to internet, Mahmood Enayat considered speed and cost to be the principal obstacles. Firstly, the Internet is low-speed as most Iranians are still using dial-up connections to access it. This is the result of a general issue of lacking infrastructure that prevents the proper installation of hi-speed internet. Secondly, getting access to the Internet is also expensive and therefore not affordable to all. The government controls all gateways to the Internet and sets the price. Numbers of internet users vary widely, however an educated guess is that somewhere around 23-30% of Iranians have access. Lastly, access to the Internet is obstructed by censorship.[7]

Government institutions active in monitoring Internet

A number of government bodies are active in controlling the Internet in Iran. The Iran Media Program of the Center for Global Communication Studies at Annenberg School for Communication, University of Pennsylvania, is author to an infographic illustrating the bodies of Iranian government involved in Internet censorship in Iran. According to The Iran Media Program, since 2009, four new bodies have emerged that are involved in control of the Internet in Iran and between Iranians and the global cybersphere: the Supreme Council of Cyberspace

[5] Enayat, February 2014
[6] Enayat, February 2014
[7] Enayat, February 2014

(SCC), the Committee Charged with Determining Offensive Content (CDICC), the Cyber Police and the Cyber Army.[8]

According to Small Media's report on Iranian Internet Infrastructure and Policy from February of 2014, the Supreme Council of Cyberspace (SCC) was established on March 7, 2013 through an order signed by the Supreme Leader Ayatollah Seyyed Ali Khamenei. The body is responsible for coordinating and implementing cyberspace policy. Small Media's report on Iranian Internet Infrastructure and Policy Report from February 2014 states:

> *The SCC is invested with significant authority, and its decisions are legally-binding. It has the power to unilaterally dictate policies relating to the Internet, and its actions cannot be obstructed by the Iranian parliament. The SCC is also able to compel the Commission to Determine the Instances of Criminal Content (CDICC) to pursue particular policies on Internet censorship, with the body having no choice but to submit to the SCC's judgements.*
>
> *The two stated objectives of the SCC are:*
>
> - *To fully exploit the positive potential of Iranian cyberspace*
> - *To protect the country and people from the negative potential of cyberspace.*[9]

Mahmood Enayat, Director of Small Media, said that measures the government has with regards to controlling the use of the Internet include the strict regulations imposed on cyber cafés. A cyber café is required to keep a log book and have cameras. Logs of all user data has to be kept for 90 days, according to regulations. As a result, the authorities are theoretically and technically, able to control and monitor cyber cafés users. The same regulations apply for mobile companies.[10]

---

[8] The Iran Media Program, *Internet Censorship in Iran: An Infographic*, posted March 13, 2013, at http://www.iranmediaresearch.org/en/research/pdffile/1296, see full infographic on their site

9 Small Media, Iranian Internet Infrastructure and Policy Report, February 2014 http://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf

10 Enayat, February 2014.

According to report from Iran Media Program, the following site contains specifics on cyber cafés regulations, http://www.cyberpolice.ir/page/3031 and www.cyberpolice.ir/page/11631 (referenced in Liking Facebook in Tehran: Social Networking in Iran, file://hbgfile/personer/vao/Downloads/liking_facebook_in_tehran%20(1).pdf)

Additionally, Internet service providers (ISPs) in Iran must register with the authorities and all blogging platforms must register with Ministry of Culture and Islamic Guidance. Connecting to internet through satellite and thereby gain direct access to the Internet is not considered feasible, as it is a very risky act and one that is illegal.

Filtering and blocking

Mahmood Enayat stated that in order to limit content and communication considered illegal or against national interest, the government filters the Internet and regularly blocks websites. Any website that contains content that the government does not like, can risk being blocked. Additionally, obstruction of circumvention tools to bypass filtering is also carried out by the authorities.

The authorities can obstruct the Internet through various ways. Technically speaking, the Internet can be obstructed through DNS interception, port blocking which can shut down use of circumvention tools, as well by web content filtering. The latter entails intelligent filtering rather than blocking whole web sites and it is not as common as the other options as it is somewhat more technically advanced.

As illustrated, there are different state institutions and committees responsible for management of internet content, including a Committee for Determining of Internet content /filtering in Iran (CDICC). Mahmood Enayat explained that there is a legal framework regarding what sort of content should be filtered which is available in Farsi at www.internet.ir/crime_index.html.

Some examples of what the list contains regarding sites that should be filtered include:

- Content that the Iranian government considers to be against morality (for example insults against women)

- Content that insults shia religion (the government is for example censoring a lot of Sunni websites and websites belonging to sects etc.)

- Content that supports deviating from Islam (for example sites concerning conversion to another religion)

- Websites belonging to a group or person acting against national security (undefined what exactly is an act against national security and therefore wide scope)

- Content containing insults against Iranian officials, etc

- Sites regarding gambling/betting

- Information about satellite TV channels

Looking at Wikipedia Persian for example, many pages and articles have been blocked. For example, out of 963 blocked articles, 403 were in the category of civil and political and 51 in political opposition and 39 independent critics.[11]

Risks involved in overstepping Internet use regulations:

Overstepping these rules can lead to a site being blocked and it can also lead to prosecution. Mahmood Enayat stressed that there is a lot of room for interpretation concerning the type of content/site that is considered illegal. Namely, content that is deemed as against national security is hard to define. One is not informed of the reason behind a block or which authority is responsible, although the Committee for Determining of Internet content /filtering in Iran claims that a person can request information on why one's website was blocked. Generally, censorship decisions are often arbitrary and not transparent, and decisions to block sites are also made by judges in connection with court cases.[12]

Self-censorship is practiced by journalists, commentators and ordinary users. Increasingly, since 2009 bloggers have removed personal details from blogs.[13]

Concerning what bodies are making arrests of users that overstep regulations, the source explained that both the Cyber police and Revolutionary Guard could be behind arrests. It was added that in recent months, the revolutionary guards have been very active. With regard to how the authorities go about uncovering users who overstep regulations, the source explained that in is very hard to keep websites hosted in Iran anonymous. Technially, all websites in Iran should register the owner details with samandehi.ir and if the website in question is registered there and there is a problem with the content, the authorities will contact the website owner. Is the site is not registered and hosted inside of Iran, they will try and trace the owner through the server log. If the server is outside of Iran, they might try to find the owner through social engineering or other hacking techniques.[14]

How do Iranians access the unfiltered Internet

By using different circumvention tools however, one can bypass filtering and access the Internet and sites that have been blocked. These include tools such as VPNs, using Tor (anonymizer and anti-filter tool) as well as other tools such as

[11] Enayat, February 2014
[12] Enayat, February 2014
[13] Enayat, February 2014
[14] Enayat, February 2014

freegate and Psiphon. However, the Iranian government has on different occasions intensified efforts to obstruct the use of such tools.[15]

If one manages to bypass the restrictions set up, one can access a relatively good range of content and viewpoints. There is an online presence of the different political fractions and view points and online oppositional activists. Platforms such as Facebook and other social media are used by activists and to express opinions deemed unacceptable by the authorities as they are considered safer environments.[16]

All popular platforms are filtered in Iran, Facebook, Twitter, YouTube. These are accessible via circumvention tools. These could include VPN (virtual private network) that funnels request for forbidden content, encrypted, to servers outside of Iran, and then replies encrypted to the user in Iran. Iranians, for example, have FaceBook accounts, but they are accessing it through a low-speed internet which is then run through circumvention tools. However, setting up a circumvention tool and keeping it enabled requires having a technical person in one's circle in order.[17]

Iranian authorities cannot monitor one's communication via encrypted mails and closed social networks, (https:// in front of the URL indicates that a user is in a secure session). This is part of the reason why the authorities try to block such platforms. It was added that the only way for the authorities to monitor non-public content on Facebook is either through weak privacy settings, posing as a friend or hacking into the accounts.[18]

Another popular communication channel that the Iranian authorities have blocked is WeChat. The day WeChat was blocked, the Iranian govt. launched an Iranian version of the platform. It was considered by Mahmood Enayat, that the Iranian government would likely attempt to launch more and more alternatives as popular channels are blocked. However, these Iranian alternatives will most likely be unable to provide the same level of service and quality and thus not live up to the expectations of the users. Iranians are therefore going to keep accessing 'the real thing' via circumvention tools. [19]

---

[15] See report from Freedom House, *Freedom on the Net 2013 - Iran*, 3 October 2013, available at: http://www.refworld.org/docid/52663aec14.html [accessed 21 March 2014]

[16] Enayat, February 2014
[17] Enayat, February 2014
[18] Enayat, February 2014
[19] Enayat, February 2014

Risks involved to online activists

Mahmood Enayat stated that there has been an increase in reports of arrests of internet users since November 2013. For example in that month, 16 bloggers who ran a gadget website (Narenji.ir) from Kerman were arrested. For three months they have not had access to lawyers and have no knowledge of basis of allegations/arrest. The arrests that have happened lately have all been conducted by the Revolutionary Guards.[20]

According to Mahmood Enayat, the recent spike in arrests could be a way by which the Revolutionary Guard is signaling to President Rouhani that this matter remains question of domestic policy in which he has no role. It also indicates that the present issues and risks towards internet activists will continue.[21]

When considering the risk to internet users that post content that is considered unacceptable, it is important to consider the website's visibility, i.e. the number of links to a site over a period of time, in order to establish the popularity of a site and whether the Iranian authorities would put resources into surveillance of such a site.[22]

On the question of whether the Iranian authorities could monitor Facebook profiles and Gmail accounts, Mahmood Enayat said that such sites are most often encrypted (SSL / https) and therefore the Iranian authorities would not actually be able to monitor such sites. However, no matter how secure Gmail or Facebook is, it is often the security hygiene of the user that can make an individual(s) vulnerable. For example the most used and quite simple attack from hackers, etc., is phishing by which personal details are conned out of the user and as a result, a hacker may be able to access a whole network.[23]

Risk of hacking:

Mahmood Enayat said that Iran's Cyber Army is actually more of a loose network of hackers that hack opposition websites. There are no signs of this 'army' being a unified structured entity. This is partly reflected in the screen dumps that appear if one's website has been hacked. These can vary a great deal. Reference was made to zone-h.org which is a sort of gallery for hackers where a hacker puts up information on sites they have hacked.[24]

[20] Enayat, February 2014
[21] Enayat, February 2014
[22] Enayat, February 2014
[23] Enayat, February 2014
[24] Enayat, February 2014