Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**696**
Land:	Iran
Kilde:	Austrian Centre for Country of Origin and Asylum Research and Documentation. ACCORD
Titel:	Query response on Iran: Capacity and methods of authorities to monitor online activities and religious activities of Iranians living abroad
Udgivet:	12. juni 2017
Optaget på baggrundsmaterialet:	29. august 2017

EN | DE

- Source:
  ACCORD - Austrian Centre for Country of Origin and Asylum Research and Documentation
- Title:
  Query response on Iran: Capacity and methods of authorities to monitor online activities and religious activities of Iranians living abroad [a-10098]
- Publication date:
  12 June 2017
- ecoi.net summary: Query response on Iran: Capacity and methods of authorities to monitor online activities and religious activities of Iranians living abroad [ID 342092]
- Countries:
  Iran

Recommended citation:
ACCORD - Austrian Centre for Country of Origin and Asylum Research and Documentation: Query response on Iran: Capacity and methods of authorities to monitor online activities and religious activities of Iranians living abroad [a-10098], 12 June 2017 (available at ecoi.net)
http://www.ecoi.net/local_link/342092/472783_en.html (accessed 15 August 2017)

ACCORD
Austrian Centre for Country of Origin & Asylum Research and Documentation

Query response on Iran: Capacity and methods of authorities to monitor online activities and religious activities of Iranians living abroad [a-10098]

12 June 2017

This response was prepared after researching publicly accessible information currently available to ACCORD as well as information provided by experts within time constraints and in accordance with ACCORD's methodological standards and the Common EU Guidelines for processing Country of Origin Information (COI).

This response is not, and does not purport to be, conclusive as to the merit of any particular claim to refugee status, asylum or other form of international protection.

Please read in full all documents referred to.

Non-English language information is summarised in English. Original language quotations are provided for reference.

TABLE OF CONTENTS

1) Capacity and methods of authorities to monitor online activities inside Iran
2) Capacity and methods of authorities to monitor online activities of Iranians abroad
3) Iranian authorities' monitoring of religious activities of Iranians living abroad, including Christian converts
Sources

1) Capacity and methods of authorities to monitor online activities inside Iran

Amnesty International technologist Claudio Guarnieri and Collin Anderson, an independent cyber researcher, who have been studying Iranian hacking activities for several years, provide the following overview in a report published in August 2016:

> "[S]ince the propagandic defacements of international communications platforms and political dissident sites conducted by an organization describing itself as the 'Iranian Cyber Army' beginning in late 2009, Iranian actors have been attributed in campaigns of intrusions and disruptions of private companies, foreign government entities, domestic opposition, regional adversaries and international critics. […]
>
> Civil society and political opponents are a primary target of Iranian intrusion campaigns […].
>
> Our research incurs classic issues applicable to all reports on intrusion campaigns, primarily questions of attribution and intent. The end objective of particular CNO [Computer Network Operations] activities is not always discernable based on the tactics used or the data accessed, as the end implications of the disclosure of particular information is often distant and concealed from even the target. Where such intent is made evident, the reasons for Iranian intrusion campaigns range from retaliatory campaigns against adversaries, as a result of identifiable grievances, to surveillance of domestic opposition in support of the Islamic Republic establishment. Iranian intrusion sets appear to be interested in a broad field of challenges to the political and religious hegemony of the Islamic Republic. Previous reports on Iranian campaigns have referred to the targeting of Iranian dissidents, however, in practice those targeted range from reformists operating within the establishment from inside of Iran to violent extremist organizations outside. Therefore, Iranian CNO activities should be considered as a tool in the context broader state activities and policies, including offline events." (Guarnieri/Anderson, August 2016, pp. 1-2)

The March 2017 US Department of State (USDOS) country report on human rights practices 2016, which covers events of 2016, reports that the Iranian authorities "monitored private online communications" and "collected personally identifiable information in connection with citizens' peaceful expression of political, religious, or ideological opinion or beliefs" (USDOS, 3 March 2017, section 2a).

The same report refers to the Basij 'Cyber Council' and the Cyber Police (FATA) as examples of state organisations involved in "targeted citizens' activities on social networking websites officially banned":

> "Government organizations, including the Basij 'Cyber Council,' the Cyber Police, and the Cyber Army, which observers presumed to be controlled by the IRGC, monitored, identified, and countered alleged cyber threats to national security. These organizations especially targeted citizens' activities on social networking websites officially banned by the Committee in Charge of Determining Offensive Content, such as Facebook, Twitter, YouTube, and

> Flickr, and reportedly harassed persons who criticized the government or raised sensitive social problems.“ (USDOS, 3 March 2017, section 2a)

A brief summary of the objectives of the Cyber Police (FATA), an institution created in 2011, can be found on the organisation’s undated website:

> “The purpose of establishing cyber police is to secure cyber space, to protect national and religious identity, community values, legal liberty, national critical infrastructure against electronic attacks, to preserve interests and national authority in cyberspace and to assure people in all legal affairs such as economic, social and cultural activities in order to preserve national power and sovereignty.
>
> Cyber police of Islamic Republic of Iran was established in 2011 based on internal and international standards in order to prevent, investigate and combat cybercrime.” (FATA, undated)

The Freedom House Freedom on the Net 2016 report of November 2016, which covers developments from June 2015 up to May 2016, gives the following overview of efforts by the Iranian state to monitor cyberspace:

> “The online sphere is heavily monitored by the state in Iran. In preparation for elections to the legislature and Assembly of Experts, Iran’s deputy interior minister for security announced a new ‘Elections Security Headquarters’ would be established ‘to monitor cyberspace.’ Similarly, the IRGC [Islamic Revolutionary Guards Corps] launched a military exercise named ‘Eghtedare Sarallah’ in September 2015, which included the monitoring of social media activities. In June 2015, Iran’s Cyber Police (FATA) created a new unit for monitoring computer games.
>
> It remains unclear how the authorities can technically monitor the content of messages on foreign social networks, given that some apps encrypt their messages. However, all platforms and content hosted in Iran are subject to arbitrary requests by various authorities to provide more information on their users. Local equivalents of international platforms do not guarantee an adequate level of protection for users, which may explain users’ hesitancy to adopt domestic platforms. An August 2015 survey of 904 Iranian internet users found that they felt less comfortable using Iranian social networks.
>
> In a troubling development, the Supreme Council on Cyberspace announced in May 2016 that all foreign messaging apps must move all data on Iranian users to servers located within the country. The order seemed targeted at Telegram, used by some 20 million Iranians, which has been under increased pressure by the authorities over the past year. Storing data on local servers would make it easier for the authorities to compel the company to hand over data on government critics and censor unfavorable views.” (Freedom House, November 2016)

Freedom House goes on to note with regard to the legal status of encryption:

> “The legal status of encryption in Iran is somewhat murky. Chapter 2, Article 10 of the Computer Crimes Law prohibits ‘concealing data, changing passwords, and/or encoding data that could deny access of authorized individuals to data, computer and telecommunication

> systems.' This could be understood to prohibit encryption, but enforcement is not common. Nonetheless, the Iranian authorities have periodically blocked encrypted traffic from entering the country through international gateways, particularly during contentious moments such as elections." (Freedom House, November 2016)

The March 2017 USDOS report provides details on government measures taken with regard to the above-mentioned Telegram messaging application:

> "An estimated 20 million Iranians use the online messaging application Telegram, which has security features that make the content of users' communications more difficult to be read by a third party. CPJ [Committee to Protect Journalists] nevertheless reported in June that users were at risk of being monitored, as had happened with other similar applications in the past. Iran's Supreme Council of Cyberspace announced on May 29 [2016] that Telegram had one year to move all of its data to servers inside Iran or risk being closed entirely. Telegram users in Iran continued to be harassed for content posted through its servers. According to local media reports, the Iranian Cyber Police arrested three Telegram channels administrators on August 9 [2016] for publishing material 'insulting religious sanctities.'" (USDOS, 3 March 2017, section 2a)

An August 2016 article of the Reuters news agency reports that over a dozen Telegram accounts belonging to "political activists involved in reformist movements and opposition organizations" have been hacked:

> "Iranian hackers have compromised more than a dozen accounts on the Telegram instant messaging service and identified the phone numbers of 15 million Iranian users, the largest known breach of the encrypted communications system, cyber researchers told Reuters.
>
> The attacks, which took place this year and have not been previously reported, jeopardized the communications of activists, journalists and other people in sensitive positions in Iran, where Telegram is used by some 20 million people, said independent cyber researcher Collin Anderson and Amnesty International technologist Claudio Guarnieri, who have been studying Iranian hacking groups for three years. […]
>
> Telegram's vulnerability, according to Anderson and Guarnieri, lies in its use of SMS text messages to activate new devices. When users want to log on to Telegram from a new phone, the company sends them authorization codes via SMS, which can be intercepted by the phone company and shared with the hackers, the researchers said. Armed with the codes, the hackers can add new devices to a person's Telegram account, enabling them to read chat histories as well as new messages. […]
>
> The Telegram hackers, the researchers said, belonged to a group known as Rocket Kitten, which used Persian-language references in their code and carried out 'a common pattern of spearphishing campaigns reflecting the interests and activities of the Iranian security apparatus.' Anderson and Guarnieri declined to comment on whether the hackers were employed by the Iranian government. Other cyber experts have said Rocket Kitten's attacks were similar to ones attributed to Iran's powerful Revolutionary Guards. The researchers said the Telegram victims included political activists involved in reformist movements and opposition organizations. They declined to name the targets, citing concerns for their safety.

> 'We see instances in which people ... are targeted prior to their arrest,' Anderson said. 'We see a continuous alignment across these actions.'
>
> The researchers said they also found evidence that the hackers took advantage of a programing interface built into Telegram to identify at least 15 million Iranian phone numbers with Telegram accounts registered to them, as well as the associated user IDs. That information could provide a map of the Iranian user base that could be useful for future attacks and investigations, they said. […]
>
> While Facebook and Twitter are banned in Iran, Telegram is widely used by groups across the political spectrum. They shared content on Telegram 'channels' and urged followers to vote ahead of Iran's parliamentary elections in February 2016. […]
>
> Amir Rashidi, an internet security researcher at the New York-based International Campaign for Human Rights in Iran, has worked with Iranian hacking victims. He said he knew of Telegram users who were spied on even after they had set passwords." (Reuters, 2 August 2016)

In a May 2015 press release, Article 19, a London-based human rights NGO focusing on defending and promoting freedom of expression and information, notes that "Operation Ankaboot" (or "Spider"), "a surveillance operation", is "believed to have been launched in the fall of 2014 to identify and root out Facebook pages and activities that spread 'corruption' and western-inspired lifestyles". The operation was acknowledged by the IRGC in January 2015:

> "Operation Ankaboot was acknowledged by officials on January 31st, 2015, when the IRGC Center for Investigation of Organised Cyber Crimes, a subsidiary of the IRGC Cyber Defense Command, put out a press release to inform the public about the shutting down of 130 Facebook pages, the arrest of 12 and detainment of 24 individuals." (Article 19, 14 May 2015)

The March 2017 USDOS report mentions that the government's operations "Spider I" and "Spider II" have led to the arrest of [e]ight online models" and the closure of an "unannounced number of online Instagram, Telegram, and Facebook pages in May 2016 "for 'immoral content' after images were posted that did not adhere to government-sanctioned dress requirements" (USDOS, 3 March 2017, section 2a).

The May Article 19 press release notes with regard to the Iranian authorities' online monitoring capabilities:

> "Beyond anecdotal evidence, documenting and confirming evidence of surveillance and monitoring of social media has proved difficult. However, at times, officials have publicly stated that they are actively monitoring Iranian citizens' activities on both blocked and unblocked websites and platforms. For instance, in September of 2014, The Chief of Iran's Cyber Police (FATA), warned the public about FATA's ability to monitor messaging applications such as Viber and Whatsapp. This announcement was made subsequent to the arrest of a number of Viber users who were targeted based on the exchange of 'inappropriate content.' While not offering conclusive evidence of surveillance, public statements by officials acknowledging surveillance activities does work to perpetuate concern, if not fear over

> whether the government's activities and capacity to monitor online activity, in particular social media. […]
>
> Following the press release announcing Operation Ankaboot, Mostafa Alizadeh, a cyber expert with the IRGC explained that the IRGC can monitor all social networks, and those who have deemed these platforms a safe place should reconsider, as they are being watched. However, from a technical perspective, the possibility of this level of surveillance and scale of probing remains unverifiable [...]." (Article 19, 14 May 2015)

An older query response of the Immigration and Refugee Board of Canada (IRB) of January 2014 refers to several sources as saying that Iran's authorities "monitor online activities […] including online activities outside of Iran". The query response quotes a professor of political science and and public policy at York University (Canada) as saying that "all Iranian websites are closely monitored by the regime". The query response also quotes a professor of modern Middle Eastern history at the University of Toronto with research experience in Iran as indicating that Iranian authorities are "very active' in cyber-monitoring, including monitoring e-mail and online conversations". Meanwhile, the IRB, with reference to the Director of the UK-based NGO Small Media and the history professor, notes that the authorities do not monitor all online activities of Iranians:

> "The Director of Small Media indicated that Iranian authorities do not have the technical capacity to conduct 'blanket monitoring,' which means that they do not follow all Iranian citizens' online activities (14 Jan. 2014). Similarly, the Professor of history indicated that the government does not seem to monitor all online activities (Professor of History 13 Jan. 2014)." (IRB, 20 January 2014)

Small Media, a UK-based NGO providing digital research, training and advocacy solutions to civil society actors who assist groups at risk, notes in an older September/October 2013 article that "[g]enerally, Iranian organisations", including the cyber police [FATA], have had "problems securing access to skilled workers and technical resources". As a result, the article states, FATA has been using "unconventional methods" to identify and track down persons online, including "acts of manipulation on social networking sites":

> "One of the most popular methods used by FATA is the creation of fake Facebook profiles, through which they may encourage other users to divulge personal information. Over the course of an investigation, a FATA agent can collect numerous pieces of information about a user from their social network accounts, linking them together to build a more complete and accurate image of the user." (Small Media, September/October 2013, p. 3)

The same report further notes with regard to FATA's capabilities:

> "FATA's Central Unit has always shared the latest technical research on surveillance and enforcement methods with other FATA offices around the country. In addition, this unit attempts to locate loopholes and zero-day vulnerabilities in Iranian computer systems and software, in an effort to prevent security weaknesses from being exploited.
>
> Besides this Central Unit, FATA is also composed of a number of more specialist sections, with the Technical Department being one of them. Here, a number of technical workers

> receive regular training regarding Internet and computer networks and security issues (though it should be noted that most staff at FATA are not technically-trained). Regardless, FATA claims that its activities are incredibly far-ranging, with FATA's chief in Kerman Province, Kambiz Esmaeili, stating that the organisation monitors all activity on websites, blogs and forums on a 24/7 basis." (Small Media, September/October 2013, pp. 3-4)

A November 2015 article of Al-Monitor, an online news platform focusing on coverage of the Middle East, notes that "Iran's security apparatus has been accumulating the skills and expertise to limit the security risks presented by social media ever since the protests in the aftermath of the disputed 2009 presidential election". The article goes on to state that the government has acquired expertise in "data-mining techniques, enabling it to find potential troublemakers who use the web as a tool for stirring political unrest". (Al-Monitor, 8 November 2015)

A January 2015 Small Media report quotes analysts as saying that the authorities have been using Deep Packet Inspection (DPI) technology since the disputed 2009 presidential election to "analyse email content and track browsing history" of Internet users (Small Media, January 2015, p. 27).

In a July 2015 report, Article 19 describes the infiltration of internet groups as a method commonly used by Iranian authorities:

> "Infiltrating online groups is a commonly used strategy by the authorities. They use a variety of methods to ascertain the offline identities of individuals such as moderators or administrators of online groups. The methods employed vary, depending on the platform. Facebook, for instance, has been the platform the authorities have most commonly used. Methods employed in order to gather information and personal data have included the following:
>
> • Creating fake online identities to make friend requests.
>
> • Writing provocative comments or messages to encourage responses in order to trap the conversant. This style of entrapment is known as an 'agent provocateur'.
>
> • Monitoring the public interactions of users to identify and flag trends. This includes using other group members to gather intelligence on specific individuals." (Article 19, 2 July 2015, p. 22)

Citing an Iranian web provider, a 2016 article of the CHRI notes that "strict censorship and 'security' laws" compel internet service providers (ISPs) to "expose their customers' information and online activities":

> "Iranian Internet service providers are particularly handicapped by strict censorship and 'security' laws that expose their customers' information and online activities. 'Since a few years ago, web hosting companies have been forced to cooperate with Internet monitoring agencies and as a result they can order the removal of any content,' said the web provider, speaking on condition of anonymity. […]

> Deleting information from a website requires web hosting companies to violate privacy agreements so that state agencies can access the server's information bank. Internet providers are thus unable to protect customer data." (CHRI, 14 March 2016)

The same report points to several patterns of online behaviour among Iranian internet users that put them at risk of being monitored by the state. These include a tendency of not using the Blind Carbon Copy (BCC) function when sending emails to multiple addressees (thus making the names and email addresses of all persons on the mailing list visible to everyone, "including unreliable contacts"), the use of real names in online activities, and general unawareness of the way information shared on Facebook can be used against them by authorities (including a poor understanding of privacy settings on Facebook). With regard to Facebook, the report specifies that users' common vulnerabilities include "[a]llowing lists of friends to be visible to the public", "[d] istributing mass invitations to events" and "[c]reating open or public groups that allow anyone to join, enabling them to see the details of all group members and activities". The same report further points to some cases where users have been "identified through activity logs on public computers and printers in places such as university campuses or the workplace" and notes that Internet café computers also log their clients' personal information and browsing data". The report goes on to note that Internet Service Providers (ISPs) are obliged to provide information on subscribers to the authority as requested and points to possible risks in the use of Virtual Private Networks (VPNs) as a means of circumventing the filtering and blocking and websites:

> "The findings of this report show that ISPs [Internet Service Providers] in Iran do not generally protect the personal information of their subscribers. In fact, Iranian ISPs are mandated by law to provide all information about their subscribers as the authorities require. All ISPs are subject to strict control and regulations by the authorities and follow national policies on filtering and censorship. As a result, some internet users take steps to access the internet in ways that avoid the authorities' filtering and blocking of websites, such as setting up Virtual Private Networks (VPNs). VPN use is common as it is very easy to set up. However, the reliability of VPNs was sometimes called into question; one interviewee believed that his VPN – purchased online – was corrupt, claiming that the authorities had access to it. In some interrogations, the authorities claimed to have gathered information directly from users' VPNs which, whether true or false, decreased Iranians' trust in VPNs. Iranians do not always pay attention to the source of the VPNs, or the software used to run them, that they use to access filtered websites such as Facebook. In some cases, the authorities established their own VPNs, enabling them to channel users' information through a monitored route, which made surveillance easy." (Article 19, 2 July 2015, pp. 22-25)

The March 2017 USDOS report refers to internet activists as saying that there is a lack of clarity as to whether or not the use of VPNs is illegal:

> "The computer crimes law makes it illegal to distribute circumvention tools and virtual private networks, but the law is not clear whether the use of such tools is illegal, according to internet activists." (USDOS, 3 March 2017, section 2a)

Freedom House states in its Freedom on the Net 2016 report of November 2016 that "[t]he use of VPNs does not appear to be criminalized, unlike the selling or promoting of VPN use", indicating

that "several individuals were arrested in late 2015 for promoting, selling, or training individuals to use circumvention tools" (Freedom House, November 2016).

A November 2016 article by Guarnieri and Anderson, which partly refers to information presented at "Black Hat" information security events, notes apparent attempts by Iranian authorities to collect IP addresses using so-called WebRTC protocols. These efforts appear to target political opposition activists and human rights activists:

> "In late December, several domains were registered in the name of the Oshkosh Corporation, an American defense industrial firm with subsidiaries in Saudi Arabia. The activities of fictitious social media profiles further indicated a sustained interested in the company, and aligned with a broader campaign of espionage directed at the defense industrial base. The typographic domains impersonated internal VPN resources to obtain employee credentials to private network resources, such as email accounts and shared file servers. Based on common patterns and registration information, the Oshkosh Corporation domains appeared to be maintained by Iranian actors – the same group behind the Ghambar malware documented at Black Hat that we believe to be related to Cylance's Operation Cleaver. The impersonation sites themselves contained another function we had not seen amongst Iranian actors previously – an attempt to enumerate internal IP addresses in order to conduct network reconnaissance. This approached has continued to arise in subsequent spearphishing attempts, including more banal Google credential phishing sites targeting Iranian dissidents, across different campaigns and different groups. While at first this tactic could be directed at identifying security researchers, subsequent campaign indicates a deeper purpose.
>
> The WebRTC protocol was designed to enable responsive real-time communications over the Internet, and is instrumental in allowing streaming video and conferencing applications to run in the browser. In order to easily facilitate direct connections between computers (bypassing the need for a central server to act as a gatekeeper), WebRTC provides functionality to automatically collect the local and public IP addresses of Internet users (ICE or STUN). These functions do not require consent from the user, and can be instantiated by sites that a user visits without their awareness. The potential privacy implications of this aspect of WebRTC are well documented, and certain browsers have provided options to limit its behavior." (Guarnieri/Collins, 11 November 2016)

The same article goes on to describe the context in which these intrusions have taken place, pointing to government censorship of social media platforms (and users' strategies of circumventing them) and to arrests of members of banned online communities such as dissidents and religious activists and, more recently, of "modelling communities, artists, and other social groups engaged in activities persecuted by the hardline establishment":

> "The Iranian government's aggressive censorship of social media platforms has inadvertently supported a culture of privacy amongst Internet users. In response to high-publicized campaigns against online activists prior to and during the Green Movement, use of pseudonyms on social media is common in Iran. Individuals frequently use initials or locations as their profile names. Moreover, the necessary use of VPNs or circumvention services to bypass the government's filter has afforded an additional degree of protection against passive network surveillance. This also aligns with our direct observation that a significant portion of

> the Iranian activists compromised by the Infy malware campaign regularly used VPN services […].
>
> Taken in the context of increased adoption of HTTPS, the government has little direct awareness of the content of certain Internet traffic. In absence of compliance by foreign technology companies to Iranian government requests, the use of anti-filtering tools and consistent maintenance of pseudonyms affords a meaningful degree of privacy to online activists against identification by domestic security agencies. Quite simply, without intrusions or social engineering, the Iranian government has little visibility into who is participating in certain online communities – or whether they are even in the country.
>
> The response from the government – notably the Islamic Revolutionary Guard Corps – has been highly-public arrests of members of prohibited online communities, such as dissidents or religious minorities. These arrests, given names such as Operation Spider, have intended to send a chilling message to the public that the state is watching online – even to exaggerate its technical capacities. While earlier campaigns targeted activists, in recent months, announced arrests have also included modelling communities, artists, and other social groups engaged in activities persecuted by the hardline establishment. The arrested are often forced to confess on television, delete their accounts, or turn them over to authorities, which are then taken over to post public warnings.
>
> The IRGC has not disclosed investigatory techniques, unsurprisingly. In at least one case, an individual arrested had posted personal information on their profile and would have been easy to identify. However, based on records sourced from infrastructure of Iranian threat groups, it appears that intrusion groups (e.g. Flying Kitten) have engaged in spearphishing against the same sets of targets.
>
> While the recording of internal IPs in spearphishing attempts against private companies or other institutions could reasonably be attributed to reconnaissance, in other documentations cases, the sole purpose of an engagement was to collect addresses of private individual with no other action in the attack. Taken in the context of the targeting of those attempts, these incidents suggest that certain Iranian groups appear to be leveraging privacy issues with WebRTC toward de-anonymizing social network users." (Guarnieri/Collins, 11 November 2016)

The same article highlights the following cases where human rights defenders have been approached through their social media accounts, apparently with the purpose of collecting IP addresses:

> "In one case, a social media profile with the name 'Maryam Javadifar' – which used pictures of DJ and model Mellisa Clarke – approached a human rights activist over Facebook. In a series of messages, Javadifar claimed that the individual's password was found online, on a site hidden behind an Iranian short URL service. The site (rinpid.com) promised visitors the ability to buy psychoactive drugs, sex products, and other items prohibited by the 'Islamic regime.' Although poorly implemented, with errors and failing to hide messages from the copied code, the sole function of that bait site is to collect visitor IP addresses and report them back to operators. The Javadifar profile is over two years old, and clearly fake. While Iranian

> threat actors are known for their sustained use of fictitious profiles, it is also notable that the Javadifar has demonstrated a clear interest in specifically targeting hundreds of political dissidents, primarily members of the Green Movement and Monarchists (supporters of the deposed royal family). […]
>
> The same approach would arise again targeting Human Rights Activists in Iran (HRA), a well-known human rights organization with deep connections within the country. HRA has been repeatedly targeted by different Iranian threat groups, and was amongst those targeted in the early IRGC crackdowns. HRA was approached on one of its Telegram accounts by an unknown individual asking about reports that one of its administrators was arrested. The bait posed as an image (domain name: 'tntnet.ir') and was once again designed to collect IPs. Perhaps ironically, the IP collection site is based on code copied from a service intended to educate users on such leakages, IPLeak.net. After the approach failed, the attacker then modified the previous messages to clean up their tracks." (Guarnieri/Collins, 11 November 2016)

The March 2017 USDOS report states that in Iran's "National Information Network", which is "intended to act like an 'intranet' system, with full content control and user identification", was launched in August 2016, according to local media reports (USDOS, 3 March 2017, section 2a).

A March 2016 Article 19 report elaborates on the National Information Network (referred to here as the "National Internet Project"), its relevance for monitoring Internet users and its status of implementation at the time of reporting:

> "For years, there has been discussion amongst the Iranian Authorities of a 'national' or 'clean' Internet, while taking steps towards the completion of the 'National Internet Project'. This project aims to create a national, secure and 'clean' Internet, which would be hosted inside the country and have limited access to the content of the World Wide Web. Content within the National Internet would be blocked or filtered according to political, cultural or religious criteria, and its users' activity would be monitored. It was planned that the National Internet Project would be fully implemented by the end of 2015, in three major phases […]
>
> Execution of this three-phase plan has already deviated considerably from expectations. From the onset, severe delays and disorganisation have plagued the already daunting task. According to the latest government budget proposal, full implementation of the National Internet Project is not expected before 2019. However, there has been progress in certain areas of implementation, as an example, Iranian authorities celebrate the fact that 40 percent of the content visited by Iranian users is now hosted domestically. […]
>
> The Iranian government has repeatedly stated its intention to monitor citizens through the National Internet." (Article 19, 29 March 2016, pp. 1-2)

Reporters Sans Frontières (RSF) reports on the launch of the first phase of the National Information Network in August 2016:

> "Two news agencies and several information websites have been blocked since 4 September, a week after the official unveiling of the 'National Information Network,' also known as 'Halal

> Internet,' while the Centre for Monitoring Organized Crime (a Revolutionary Guard offshoot) has reported the arrest of around 100 Internet users in recent weeks. […]
>
> The first phase of the National Information Network was formally celebrated on 27 August by several government officials including the first vice-president, the minister of communication and information technology and the secretary-general of the Cyberspace Supreme Council. However, they restricted their statements to the usual slogans and did not explain how this National Information Network will work and what consequences it will have for Iran's Internet users, who are officially estimated to number 30 million. […]
>
> Communication minister Mahmoud Vaezi said, 'the National Information Network imposes no limits on Internet users' but this was contradicted by deputy minister Nasrolah Jahangard, who said: 'In the Network, all connections including mobile connections have identification; without identification, you will not be able to use the Network's services.' As well as such propaganda-style statements, the authorities cite the need for protection as justification for the network – protection against cyber-attacks, protection of the country's sensitive data and the personal data of individual users, and finally protection of Iranian society's 'morality.' In fact, this National Information Network can be likened to a big Intranet, in which content is controlled and all users are identified, an Intranet that can be completely disconnected from the World Wide Web when the authorities so decide. It is a personal Internet or 'Halal Internet' based on 'intelligent filtering.' […]
>
> For the past year, different sections of the Revolutionary Guards have been announcing the dismantling and systematic arrest of networks of people who act 'against society's moral security,' 'modelling criminals' (those who have photos and videos of models) and those who 'insult religious beliefs.'" (RSF, 6 September 2016)

A March 2017 report of the UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran to the UN Human Rights Council (HRC) mentions reports of intimidation and prosecution of "Internet users, bloggers and social media activists" (HRC, 6 March 2017, p. 13).

Article 19 reported in 2 July 2015:

> "According to the findings of this study, ethnic and religious minority activists (the Baha'i's and the Dervishes more than others), as well as members of known political groups, are kept under constant offline and online surveillance. This is intended both to control and suppress those activities of members of these groups that may lead to their recognition, and it is often carried out by special units of the intelligence services dedicated to monitoring minority activists. Methods used by the authorities include continuous blocking of websites, as well as ordering hosting providers to remove data and stop providing services to particular groups." (Article 19, 2 July 2015, p. 24)

Extensive information on Iranian authorities' efforts for internet control and can be found in the following reports:

- Guarnieri, Claudio/ Anderson, Collin: Iran and the Soft War for Internet Dominance, August 2016

https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf

2) Capacity and methods of authorities to monitor online activities of Iranians abroad

The query response of the Immigration and Refugee Board of Canada (IRB) of January 2014 refers to several sources as saying that Iran's authorities "monitor online activities […] including online activities outside of Iran" (IRB, 20 January 2014).

No further information could be found on the Iranian authorities' capacity and methods of monitoring online activities of Iranians living abroad.

3) Iranian authorities' monitoring of religious activities of Iranians living abroad, including Christian converts

No information published after 2014 could be found on the Iranian authorities' monitoring of religious activities of Iranians living abroad.

A fact-finding-mission report of the Danish Immigration Service (DIS), published in June 2014, refers to a non-governmental organization in Turkey as saying that Iranian Christian who come to Turkey "feel that they are at risk of surveillance by Iranian agents in Turkey" (DIS, 23 June 2014, p. 37). The DIS quotes an international organization in Turkey as saying that there are reports saying that Iranian authorities have agents and informants in some churches in Turkey, although the source expressed uncertainty as to whether the Iranian authorities' have the capabilities to "monitor those who are visiting Turkey in order to get baptized, for example, in a systematic way". The DIS report states with reference to information provided by Amnesty International (AI)'s International Secretariat:

> "Regarding risks to individuals who return to Iran after having received religious training in Turkey, AIIS (Amnesty International International Secretariat) said that it was possible that Iranian security officials were monitoring activities that take place in Turkey. It was considered that generally, it is probably easier to monitor what goes on in Turkey due to the geographical proximity and the ease with which Iranians can travel to Turkey." (DIS, 23 June 2014, p. 39)

The DIS report goes on to say with reference to Elam Ministries, a UK-based Iranian Christian group that engages in missionary work in Iran and has a presence in Turkey:

> "Elam Ministries stated that the organization knows of many cases of individuals who came for training in Turkey who upon return to Iran, were immediately arrested. Over 500 individuals that were connected to Elam have been arrested and interrogated for shorter or longer periods, within the past three years, and within the past year, the number has been about 200 individuals. The reason behind this high number is that the authorities have obtained quite a bit of information about how the house churches operate. It also seems that the Iranian authorities have agents in Turkey that know of what work Elam is doing there." (DIS, 23 June 2014, p. 39)

The same report further notes with reference to representatives of the Union Church in Istanbul which aids asylum-seekers while their cases are processed by the United Nations High Commissioner for Refugees (UNHCR):

> "When asked what obstacles a convert to Christianity faces in Iran, the representatives of the Union Church considered that if a convert returns to Iran, he or she lives in fear of being discovered. […] According to the source the Iranian secret police are reported to be active in Istanbul. Many Iranians who approach the church are cautious and will often use a different name from their own because they fear that news of their contact with other believers will pass on to Iran." (DIS, 23 June 2014, p. 40)

No further information could be found on the Iranian authorities' monitoring of religious activities of Iranians living abroad.

Sources (all links accessed 4 May 2017)

- Al-Monitor: How Internet censorship protects Iranian businesses, 8 November 2015 http://www.al-monitor.com/pulse/originals/2015/11/iran-filtering-policies.html
- Article 19: The State of Surveillance in Iran's Cyberspace, 14 May 2015 (available at Refworld) http://www.refworld.org/docid/55657d924.html
- Article 19: Computer Crimes in Iran: Risky Online Behaviour, 2 July 2015 (available at Refworld) http://www.refworld.org/docid/559d21a74.html
- Article 19: Tightening the Net: Internet Security and Censorship in Iran; Part 1: The National Internet Project, 29 March 2016 (available at Refworld) http://www.refworld.org/docid/56fe32ea4.html
- CHRI - Center for Human Rights in Iran: Iranians Looking Abroad to Escape State-Controlled Internet, 14 March 2016 https://www.iranhumanrights.org/2016/03/security-risks-iranian-itc-comanies/
- DIS - Danish Immigration Service: Update on the Situation for Christian Converts in Iran; Report from the Danish Immigration Service's fact-finding mission to Istanbul and Ankara, Turkey and London, United Kingdom, 23 June 2014 (available at ecoi.net) http://www.ecoi.net/file_upload/1226_1403600474_rapportiranffm10062014ii.pdf
- FATA - Cyber Police: About us, undated http://cyber.police.ir/index.jsp?fkeyid=&siteid=46&fkeyid=&siteid=46&pageid=609
- Freedom House: Freedom on the Net 2016 - Iran, November 2016 (available at ecoi.net) http://www.ecoi.net/local_link/332079/460024_en.html
- Guarnieri, Claudio/ Anderson, Collin: Iran and the Soft War for Internet Dominance, August 2016 https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf
- Guarnieri, Claudio/ Anderson, Collin: Fictitious Profiles And WebRTC's Privacy Leaks Used To Identify Iranian Activists, 11 November 2016 https://iranthreats.github.io/resources/webrtc-deanonymization/
- HRC - UN Human Rights Council: Report of the Special Rapporteur on the situation of human rights in the Islamic Republic of Iran [A/HRC/34/65], 6 March 2017 (available at

ecoi.net)
http://www.ecoi.net/file_upload/1930_1489059332_a-hrc-34-65-auv.doc

- IRB - Immigration and Refugee Board of Canada: Iran: Treatment of anti-government activists by authorities, including those returning to Iran from abroad; overseas monitoring capabilities of the government (2012-2013), 20 January 2014 [IRN104730.E]
http://www.refworld.org/docid/533923f74.html
- Reuters: Exclusive: Hackers accessed Telegram messaging accounts in Iran – researchers, 2 August 2016
http://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM
- RSF - Reporters Sans Frontières: Iran creates “Halal Internet” to control online information, 6 September 2016 (available at ecoi.net)
https://www.ecoi.net/local_link/330161/457796_en.html
- Small Media: Iranian Internet Infrastructure and Policy Report, September/October 2013
https://smallmedia.org.uk/sites/default/files/u8/IIIPSepOct.pdf
- Small Media: Revolution Decoded: Iran’s Digital Media Landscape, January 2015
https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded.pdf
- USDOS - US Department of State: Country Report on Human Rights Practices 2016 - Iran, 3 March 2017 (available at ecoi.net)
http://www.ecoi.net/local_link/337185/466945_en.html
