ARTICLE 19

Computer Crimes in Iran:
Risky Online Behaviour

2015

Country Report

ARTICLE 19
Free Word Centre
60 Farringdon Road
London,
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-910793-17-6

Contents

Glossary and Abbreviations

Bcc: Blind carbon copy: One of three fields listing recipients within the header of an email, the Bcc field is used to send an email to particular recipients, hiding their existence and identity from the recipients listed in the 'To' or 'Cc' (carbon copy) fields.

CCDOC: Committee Charged with Determining Offensive Content.

CCL: *Computer Crimes Law*.

Encryption: In cryptography [the action of protecting information by altering it into an unreadable format], encryption is the process of encoding messages or information so that only authorised parties can read it.

FATA: Iranian Cyber Police.

Graph Search: A search engine integrated with Facebook's social graphs, this processes natural language queries to return information from the user's social network of friends, connections etc.

IMEI: International Mobile Equipment Identity: the unique number used to identify each mobile phone device. Each mobile phone has a unique number IMEI which can be tracked at all times.

IRGC: Iranian Revolutionary Guard Corps (Army of the Guardians of the Islamic Revolution).

ISP: Internet Service Provider: the ISP is a company that providing access to the Internet, usually for a fee.MOI: Ministry of Intelligence.

Phishing: The attempt to acquire sensitive information such as usernames and passwords by masquerading as a trustworthy entity in an electronic communication.

RCDC or Gerdab: The Revolutionary Guards Cyber Defence Command.

SCC: Supreme Council on Cyberspace.

SCRC: Supreme Council of the Cultural Revolution.

SIM Cards: Also known as a subscriber identity module, is a smart card that stores data for GSM cellular telephone subscribers. This data can include the user's identity, location and phone number, personal security keys, contact lists and stored text messages.

Spyware: Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

VoIP: Voice over IP: A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the internet.

VPN: Virtual Private Network: a group of computers (or discrete networks) networked together over a public network—predominately, the internet. VPNs emerged as the leading circumvention tools used to dodge the Iran's filtering system by Iran's online users.

Foreword

For decades, governments have had unfettered access to the private communications of the general public through telecommunications licence mandates and technical standards which oblige the handing over of phone records to law enforcement agencies. Overnight, the internet challenged this historical expectation and international norm. People's conversations, both banal and subversive alike, had shifted away from local communications channels onto platforms outside the direct reach of the state, often encrypted and hosted in other countries. At the same time, governments were economically bound to at least nominal connectivity, since the same networks that facilitated the questioning of state-imposed orthodoxies had become necessary for modern development and international business.

The mechanisms for combating the 'soft war'[01], beyond overt censorship, were established relatively late in Iran in the form of the Revolutionary Guards' Cyber Defence Command (RCDC) and the Iranian Cyber Police. The security apparatus has struggled to assert its relevance and operate effectively, prosecuting digital fraud domestically at the same time as engaging in cyber warfare abroad. Arrests of online activists are increasingly accompanied by televised confessions and declarations by the authorities stating that 'those who think this space is safe for them must cease their activities' (February 2015), 'people should know we can read their messages' (September 2014), and 'we will definitely identify these people and deal with them' (May 2014). Through these nebulous and inflated claims, the state has sought to erode users' trust in their online privacy. When internet users believe that the authorities will be able to monitor their communications, no matter what precautions they take, they engage in the same self-censorship and passive security practices as they do offline.

Rhetoric differs greatly from reality. Security agencies around the world have been hindered, and often marginalised, by the adoption of information technologies. If strong encryption and privacy tools are effective against American and European intelligence, then they are certainly beyond the reach of Iranian surveillance. Threatened and disempowered, the security forces have sought to assert control over modern communications by projecting an image of their power that bears little resemblance to their actual capacity. As the case studies in this report illustrate, these bombastic claims are also the product of the bureaucracy's inferiority complex, encumbered by internal competition and a lack of

[01] A term coined by Seyyed Ali Khamneyi, Islamic Republic of Iran's Supreme Leader, referring to a continuous digital war inflicted on Iranians by the West.

technological sophistication. Any state capable of successfully monitoring the content of online communications would have little interest in asserting its capabilities in the aggressive, public manner routinely adopted by the Iranian authorities. Rather, they would be highly incentivised to keep quiet and collect everything.

As they are far from omniscient, the authorities are fundamentally dependent on users failing to take adequate precautions with their communications and personal data. Rather than attack weaknesses in cryptography or exploit vulnerabilities in infrastructure, the authorities and those associated with them routinely take advantage of basic human nature. A recurring theme arises across these accounts: the ego encourages social network users to identify themselves, sexual desire is used to infiltrate users' devices with spyware, and laziness means that users fail to protest their devices with adequate passwords. There is no collective learning process: the gravity of seemingly minor decisions is understood only when an individual's own information is used against them in court. An individual's failures are then used to persecute wider networks of contacts, with one interrogation leading to dozens of arrests. These individuals are put on display as evidence of the authorities' power over the internet to encourage a sense of an information asymmetry, the ultimate resource of a repressive state.

This study lends further confirmation to observations that I and other researchers have made about the often technically unsophisticated and poorly orchestrated behaviour of the Iranian security agencies in their campaign to stifle online dissent. These repressive practices have been documented over the past several years, seen in malware campaigns against Iranians in the lead-up to elections, and in attacks on international platforms hosting independent Persian-language media. The lessons learned start to demystify intelligence operations and reinforce common concerns about user behaviour which have never been directly addressed. For the ecosystem of organisations, developers and individuals interested in digital security and internet freedom in Iran, this research is a census of systemic failures describing both why it is inadequate to focus on tools alone and also the limits that we face. Disconcertingly, it also demonstrates that the ineffectiveness of the state is a product of addressable issues, and that the authorities will develop more sophisticated approaches to surveillance in line with the maturation of civil society.

Despite investments in secure communications software and infrastructure, users continue to make decisions that are not rational from the point of view of privacy, either because they are highly incentivised in other ways to make poor decisions, or because their perception of the risk differs from our expectations. Moreover, we should acknowledge that the demands of training and technology for users who are under threat do not match normal online behaviour, are not commonly practised by either technologically savvy users outside Iran or those claiming security expertise, and are often impeded by the platforms themselves. We continually see individuals compromised and arrested for preventable reasons, and their stories are a testament to the expectation that independent media, minority communities, political dissidents and social activists will continue to be prosecuted based on their online activities.

Without fact-based research, the fictitious and disempowering narrative promoted by illiberal actors threatens to corrode the public's perception of the internet as being a safe space for marginalised voices. Read in this context, this study is a rare insight into how governments attempt to stifle online dissent. It demonstrates the human impact of poor security practices and reveals the limits of security efforts. Optimistically, it is also an important testimony to the limits of the state and the power of individuals to protect their own fundamental human rights in a manner never before available.

Collin Anderson

Introduction

‘If it hadn’t been for the data (text, photos, notes and open apps) that the authorities found on my phone after my arrest, there would have been no hard evidence for my conviction.’ [02]

Introduction

What is the correlation between the online and offline behaviour of Iranian citizens and the likelihood of their arrest in Iran today? Answering this question is the main focus of this report.

First introduced in Iran in 1993, the internet has accrued a steadily increasing number of users over the years. Between 2001 and 2009 – the year of the contested presidential elections – internet usage increased by nearly half each year.[03] In 2014, there were estimated to be more than 22 million internet users in Iran, just over 28 percent of the population.[04,05]

In the 1990s and early 2000s, access to the internet was expensive and it was mostly perceived as a luxury. But as its popularity grew, it became more affordable and the internet’s role in Iranian day-to-day life began to take shape.

The birth of blogging and the authorities’ response

In September 2001, Hossein Derakhshan, a young Iranian journalist, created one of the first ever weblogs (‘blogs’) critical of the regime, written in his native language Farsi. An inquisitive reader encouraged him to set up a basic how-to guide on blogging, which contributed to a rapid increase in online expression inside Iran and the formation of the Farsi blogosphere. At the time, it was one of the largest and most active in the world,[06] and constituted a serious challenge to

[02] Interview with ARTICLE 19

[03] OpenNet Initiative 2009

[04] Internet Live Stats 2014

[05] Domestic sources report the figure at around 40 million Internet users (http://www.iriu.ir/matma/) and 8 million GPRS, 3G and 4G users

[06] www.cyber.law.harvard.edu/publications/2008/Mapping_Irans_Online_Public

Iranian officials' hitherto unopposed monopoly on information. Leading Iranian author and blogger Abbas Maroufi described the use of the newfound platforms for free speech and commentaries as '[our] messages in bottles, cast to the winds.'[07]

The government reacted swiftly and forcefully, launching a crackdown that severely limited the freedom of expression and information of bloggers: in the same year that Iran's blogosphere appeared, Supreme Leader Ali Khamenei decreed that access to the World Wide Web be available only to state authorised entities.

Furthermore, from 2001, the Supreme Council of the Cultural Revolution (SCRC) began to implement a series of regulations that required Internet Service Providers (ISPs) to employ filtering systems, monitor and record customers' internet use, and remove all anti-government and anti-Islamic websites from their servers.[08] This continuous crackdown peaked in 2008, just before the 2009 presidential election, and forced most bloggers to use alternative information sharing techniques, including new social media platforms.[09] The authorities responded the same year with internet filtering and targeted legal action.

In December 2008, Omid Reza Mir Sayafi[10] was charged with insulting the religious leaders and engaging in propaganda against the Islamic Republic of Iran in his blogs, and was subsequently sentenced to two and a half years in prison. He died in prison on 18 March 2009, becoming the first ever blogger to die in custody. Despite poor mental and physical health, he was denied external medical treatment as requested by the prison's medical staff.

The dissident use of social media was particularly evident during the widely disputed 2009 presidential elections. Social media users – so-called 'citizen journalists' – played a significant role in coordinating and organising protests; amateur videos and photos could be uploaded to the internet instantly. Rallying like-minded people in a short period of time was easier with tools such as Facebook and Twitter.[11] However, the potential for social media to be used as a tool for socio-political mobilisation was not only identified by the activists, but also by the Iranian authorities.

[07] www.theguardian.com/technology/2004/dec/20/iran.blogging

[08] http://www.Iranhrdc.org/English/English/publications/reports/3157-ctrl-alt-delete-iran-039-s-response-to-the-internet.html?p=1

[09] such as Facebook and Twitter

[10] http://www.theguardian.com/world/2009/mar/20/omidreza-mirsayafi-iran-blogger-rouznegar

[11] http://news.bbc.co.uk/1/hi/world/middle_east/8099579.stm

Since then, Iran's administration has waged a continuous war against the internet, aiming to restrict its capacity to facilitate protest movements. This war has taken the shape of new legislation, policies and practices, which continue to fall outside the permitted limitations to freedom of expression and information according international human rights standards.[12] Internet censorship and surveillance has become a major priority. This stranglehold has been strengthened by a number of government regulatory initiatives, designed to assert control over online communications.

Cyber activities conflicting with the regime's norms have been criminalised, in breach of international standards, and the technical capacities of the authorities have been strengthened to enable sophisticated and comprehensive blocking. In January 2010, the Computer Crime Law was introduced, a vaguely-worded law banning the 'dissemination of lies' of the publication of materials considered damaging to 'public morality'.[13] The following year, the Iranian Cyber Police (FATA), was established. Iranian internet-repressing entities known as 'cyber squads', such as the Revolutionary Guards Cyber Defence Command (RCDC or Gerdab) were established, funded by the Iranian Revolutionary Guards Corps (IRGC). Other groups such as the so-called 'Iranian Cyber Army' also appeared in the news, notably in February 2011, when they reportedly hijacked the media outlets of Voice of America and the BBC.[14] The government never officially confirms or denies its relationship with them. Private sector hacker groups such as Ashyane, Simorgh and Shabgard have reportedly worked with the authorities. These groups, like the aforementioned 'cyber squads', are reported to have engaged in surveillance, hacking, threatening messages, content production/development, promotion of Iranian-specific technologies such as operating systems and browsers, and phishing.

Iran's authorities have invested heavily in their administrative, legal and logistical capacity to restrict freedom of expression and information for what they perceive as threats associated with communication technologies. In March 2012, Supreme Leader Khamenei founded the Supreme Council on Cyberspace (SCC) – a policymaking body whose members include Iran's President, the Head of the Judiciary, the Minister of Intelligence, the Minister of Culture and other law

[12] In 2013 ARTICLE 19 made recommendations to state actors and policy makers about what they should do to promote and protect the rights of bloggers domestically and internationally: ARTICLE 19, The Rights to Blog. 2013. Policy brief. http://www.article19.org/data/files/medialibrary/3733/Right-to-Blog-EN-WEB.pdf

[13] *ARTICLE 19*, Computer Crimes in Iran: Online Repression in Practice

[14] Ibid

enforcement officials – to oversee the use of the internet in Iran.[15] The SCC is just one of a number of regulatory groups aimed at restricting free access to the internet.[16] Another, the Committee Charged with Determining Offensive Content (CCDOC) identifies sites with illegal content, and makes the final decision as to whether a site should be blocked due to its content.

The Iranian authorities domination of Iran's online sphere has been widely reported,[17,18] as has the high number of internet users who have been – and continue to be – arrested.[19]

Improving digital security in Iran

ARTICLE 19 released reports in 2012[20] and 2013[21] analysing the contents of Iran's 2010 *Computer Crimes Law* and its effects on Iran's online community. Dissecting the legislation and documenting testimonies by victims of the law, ARTICLE 19 provided recommendations for a range of actors, including technical experts, private companies, and the Iranian government in order to protect and enforce the right to free expression in Iran.

It is still difficult to determine whether Iran's online community has made real progress in safeguarding its own digital security. This third report is intended to bridge that gap. Its aim is to identify what progress – if any – has been made by Iran's internet-using public in maintaining their own digital security, and also, where necessary, to define areas where more behavioural and technical changes are required.

[15] Ibid

[16] Ibid

[17] https://cpj.org/reports/2012/05/10-most-censored-countries.php

[18] https://globalvoicesonline.org/2015/03/23/internet-in-iran-evaluating-rouhanis-first-two-years-as-president/

[19] http://www.iranhumanrights.org/2015/03/facebook-users-arrested/

[20] Iran: *Computer Crimes Law* (2012) http://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf

[21] Computer Crimes in Iran: Online Repression in Practice (2013) http://www.article19.org/data/files/medialibrary/37385/Computer-Crimes-in-Iran-.pdf

To achieve this, the report focuses on the following questions:

- What do the authorities know about internet users in Iran?
- How do they know this?
- What else do they want to know?
- What methods do they use to get more information?

Analysing these findings will define what types of online and offline behaviour are leading to higher rates of arrest, and this will, in turn, give a key insight into how the Iranian authorities are carrying out monitoring and surveillance. Lastly, the report recommends which behavioural changes, contingency plans and technical assistance are required, and indicates potential areas for further research.

Methodology

Methodology

This report aims to explain the correlation between the online and offline behaviour of online activists in Iran today and the likelihood of their arrest. The report’s recommendations will suggest ways of substantially reducing the risk of arrest for these individuals.

The first step was to identify and interview a diverse group of individuals who had been targeted by the Iranian authorities as a result of their online and offline activities. To qualify for selection, the candidates had to have been prosecuted for their online actions. This included individuals who had been arrested for other reasons, but whose online presence represented a key component in their detention. All in all, data from 25 respondents was selected and analysed for this report.

The group comprised of journalists, legal activists, activists involved in underground political parties, members of student groups and student unions, minority rights activists, and citizens who use social media platforms to share their opinions with larger audiences. In order to maintain as diverse an assessment as possible of these individuals’ online behaviour and habits, a mixture of well – and lesser-known activists was selected. The aim of this was twofold: firstly, to see if a difference exists between the monitoring of well-known and lesser-known activists; and secondly, to understand how this difference manifests itself.

In the interest of maintaining an objective and decentralised stance, those living in smaller cities were given greater attention than those living in the capital Tehran. This was also intended to encourage future research in those areas outside Iran’s capital which often receive less exposure in such cases.

Finally, care was taken to interview a balanced representation of age groups, genders, levels of technical expertise and socio-economic background.

The interviews – and subsequent collation of data – were conducted in accordance with strict privacy regulations to ensure anonymity for the respondents.
In addition, the analysis itself was stripped of any private information or details that might compromise their safety. Apart from such safety measures, the data used in this analysis remains unchanged.

Qualitative research methodology was used to ascertain the beliefs, feelings, opinions, experiences and attitudes of the respondents.

The interviewer worked from a set list of questions, but the structure of the interview was such that spontaneous relevant questions could be asked where appropriate. The questions were tailored in order to establish the following: firstly, the typical mistakes that had compromised the respondents' online security; secondly, the most common types of information sought by the authorities; and finally, the methods used to extract this information. Questions were also intended to identify the correlations between online and offline activism. A complete list of the questions can be found in Annex 1.

The collated data was statistically analysed and the responses coded: the outcome of this analysis is detailed in the next chapter.

Findings

Findings

Disclaimer

This document has been prepared in good faith on the basis of information made available to the researcher through in-depth interviews. As explained in the Methodology (above), the findings of this study are explicitly derived from the information gathered from the respondents who participated in the study and whose details are kept confidential for security concerns. Statements of fact in this study and conclusions drawn accordingly have been obtained from sources considered reliable, but no representation is made by ARTICLE 19 or any of its affiliates as to their completeness or accuracy. In certain cases, ARTICLE 19 has not published evidence for statements if it risks compromising the safety and security of the respondents.

How the authorities gather information before arrest

According to respondents, the two main authorities conducting arrests and surveillance are the Ministry of Intelligence (MOI) and the IRGC. The former is said to use more traditional surveillance methods such as monitoring landlines, mobile phones, residences, meeting places or offices, while the latter employs more sophisticated online monitoring via content production, infiltration[22] and phishing.

The IRGC is typically more aggressive than the MOI, with a higher number of arrests and a greater incidence of violent techniques.[23] The majority of monitoring and arrests relating to ethnic and religious minorities and criticism of Supreme Leader Khamenei are conducted by the IRGC.

Mobile phones

Activists who use text messaging and/or phone calls to mobilise others or arrange group meetings are particularly vulnerable. Many respondents reported that their phones were tapped by the IRGC and their phone records regularly accessed over a period of several years from 2009 to 2014. One respondent who was interrogated recalls '…I denied an accusation, [and] they showed me a log of my text messages 'dating back two years.'[24]

[22] See 'Online infiltration' below

[23] Violent raids on houses or offices, harsher treatment during arrest/detention, and more aggressive threats and use of vulgar language were all reported by interviewees dealt with by the IRGC.

[24] Interview with ARTICLE 19.

Storing incriminating photos, text messages, documents and other types of information and data on mobile phones can also be dangerous. One respondent stated that there would have been 'no hard evidence' for their conviction had it not been for data retrieved from their mobile phone after their arrest.

In another instance, the interviewee received a call from a foreign Persian language news channel. Just a few hours later they were called in for questioning by the MOI. 'They showed me my phone and text records for the last six months.' This indicates not only the extent of phone tapping by the authorities, but also their awareness of calls made by certain news channels.

Another widespread and erroneous belief among Iranian activists is that constantly changing SIM cards makes them untraceable. This is not the case, however, as mobile phones can be tracked via their IMEI number[25] regardless of the SIM card used as a result of Nokia-Siemens selling particular mobile phone equipment to the Iranian authorities.[26]

Phishing and Malware attacks

Phishing is a frequently used strategy which aims to exploit the carelessness of activists and ordinary citizens alike. The most common method is to use the promise of sexual content (such as photos) to entice the victim into clicking on an image. Alternatively, journalists are sent executable files (such as word documents, PDFs, or images) disguised as urgent headline news. When the victim clicks on the content, malware is downloaded and installed onto their device. This either activates the computer's inbuilt microphone or camera, installs spyware which sends key information to an external user (such as the authorities), or creates a fake email login page that captures the victim's password. This last method is a combination of phishing and what is known as a 'man-in-the-middle attack', whereby a third party is able to monitor a conversation taking place between two parties who mistakenly believe they are communicating only with one another.[27]

[25] A SIM card identifies you, but your mobile phone can get you into trouble. Each mobile phone has a unique number, the International Mobile Equipment Identity (IMEI). This number can be tracked at all times.

[26] *Nokia-Siemens rues Iran crackdown rule*, Bloomberg, 03.06.2010, accessed online at http://www.businessweek.com/globalbiz/content/jun2010/gb2010063_509207.html [17.03.2015]

[27] DuPaul, N., *Man in the Middle (MITM) Attack*, accessed online at http://www.veracode.com/security/man-middle-attack (17.03.2015)

Online infiltration

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.[28] 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.

Another vulnerability identified in the way Iranian users communicate online is that they tend not to use the Blind Carbon Copy (BCC) function when sending mass emails. This means that the names and email addresses of all those on the mailing list are visible to everyone, including unreliable contacts. When the authorities have access to such mass emails and group messages, they are able to gather names and email addresses without having to access mailservers or the need to perform other more complicated attacks. This problem is especially prevalent in Viber and Facebook group messages.[29] Many of the interviewees who participated in our report had had their identities discovered when the authorities infiltrated bulk emails and group messages.

[28] The individual using the fake ID initiates conversations and exchanges a few personal and private details about her/himself to attract the target’s attention and gain her/his trust. Once trust has been established, the target feels comfortable sharing more details about her/himself and voluntarily compromises her/his identity and beliefs. This was particularly what had happened with a few group administrators interviewed for this study.

[29] Viber is the most popular instant messaging app in Iran with VoIP capabilities, and it is free of charge. Facebook is also very popular. For more information and statistics, please visit http://www.amarestan.com/vdcjfaevzuqeo.sfu.html (in Farsi)

Use of real names

A significant number of respondents used their real names in the online realm, believing it to carry more impact and authenticity than a pseudonym. Another motive for using their real name was the prospect of fame and popularity. This practice indicates a considerable lack of awareness of the risk of arrest that such behaviour could incur, as their online activities could easily be traced back to them by the authorities.

Facebook

> 'During my interrogation, I realised that whatever information the authorities claimed to have on me had been gathered from my Facebook page, or [the pages] of my friends where I am tagged.'[30]

Despite being blocked, Facebook is by far the most popular social media platform in Iran as it is fairly easy to connect with large numbers of like-minded individuals and groups. For those bloggers whose blogs were shut down, or whose blogs had not received the desired number of visitors, Facebook has also been a convenient alternative platform to express themselves freely.

While there are advantages to an increased flow of information and the promotion of differing voices and views, Iranian users are generally unaware how the data that they willingly share on Facebook can be used against them. Privacy preferences, for example, are poorly understood, meaning that sharing information and tagging others in photos can lead to legal harassment by the authorities, not only for the users themselves but others as well.

Common vulnerabilities noted in Facebook privacy settings include:

- Allowing lists of friends to be visible to the public
- Distributing mass invitations to events
- Creating open or public groups that allow anyone to join, enabling them to see the details of all group members and activities.

[30] Interview with ARTICLE 19.

Facebook has also recently created a ‘graph search’ option, by which detailed information about the public activities of a member can be accessed quickly and easily by everyone, including the authorities.

Use of public computers and printers

Some respondents reported having been identified through activity logs on public computers and printers in places such as university campuses or the workplace. Internet café computers also log their clients’ personal information and browsing data.[31]

Constant surveillance

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.[32]

ISPs and secure connections

Respondents were asked about their Internet Service Providers (ISPs) to see whether different ISPs in Iran apply different policies to their subscribers. The findings of this report show that ISPs in Iran do not generally protect the personal information of their subscribers. In fact, Iranian ISPs are mandated by law[33] 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

[31] The cybercafé law regulates the type of services internet cafés may provide, the type of content they may allow their users to transfer using their equipment, and requires cafés to document and store the identities and user histories of their customers for ‘at least six months’. In his third report on the situation of human rights in the Islamic Republic of Iran presented to the United Nations General Assembly (UNGA) Third Committee on 13 September 2012, the UN Special Rapporteur on Iran flagged this practice as limiting freedom of expression and right to information for Iranians.

[32] Freedom House, Freedom in the Net – Iran: https://freedomhouse.org/report/freedom-net/2012/iran#.VToNt47F_C8

[33] See ARTICLE 19’s analysis of the *Computer Crimes Law*: http://www.article19.org/resources.php/resource/2922/en/iran:-computer-crimes-law

policies on filtering and censorship.[34] 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 calledinto 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.

Methods used to extract information during and after arrest

Physical access to (confiscated) laptops and other devices

'It was all there…all the information that harmed me was readily available on my laptop. No encryption and no password.'[35]

Examining confiscated laptops and other devices is the easiest way for authorities to extract information from detained persons. According to interviewees, it often happened that additional information gathered from their confiscated laptop computers further complicated their own cases after being arrested. In many cases, for instance, respondents only realised how much unprotected information they had saved on their computer devices after being arrested. This subsequently harmed them during prosecution. Often, respondents stated that had it not been for the examination of their confiscated devices, there would not have been enough evidence to sentence them.

The majority of respondents either failed to have a password, or had weak passwords for their online accounts on their electronic devices and/or personal computers. Often the respondent used a single password for multiple accounts, providing easy access for the authorities. One participant even admitted to having saved all their passwords to the desktop, owing to their poor memory. The use of password managers was never reported.

[34] For further information on national policies on filtering and censorship and the role of ISPs, see the OpenNet Initiative report on Internet Filtering in Iran (2009): https://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf (15.02.2015)

[35] Interview with ARTICLE 19.

Some respondents disclosed their passwords to the authorities immediately, thinking that they either had nothing to hide, or that they would be treated more leniently if they cooperated. However, interviewees who had acted in this way – in the belief that they would be treated less harshly by the authorities – found that they were mistaken.

In contrast, those respondents who did not volunteer their passwords to the authorities during interrogations, or who gave false passwords, managed to keep their accounts safe.

None of the respondents used encryption software on their devices. In several instances, data found on the computers of people arrested led to the identification, compromise and (in one case in this study) arrest of other individuals. In one case, a respondent who had failed to delete their chat message history inadvertently revealed the identity of an individual who had been diligently deleting their chat history on their own device, and this revelation led to the arrest of the second individual.

Use of fragmented and incomplete intelligence

Fragmented intelligence gathered by the authorities from various sources was used as a means of intimidation, resulting in the individual surrendering more information about themselves in the (mistaken) belief that the authorities already knew everything about the arrested individual.[36]

This method, reinforced by the pervading climate of fear in Iranian society, had an impact on the online behaviour of some respondents who believed that no matter how much they tried to be careful, the authorities already knew every detail of their lives. As a result they believed safety precautions to be useless.

Psychological pressure

Some respondents reported that the authorities threatened to share embarrassing private information about them unless they cooperated. Others reported that threats were made against their family members to put additional pressure on them. Family members were threatened by the authorities that their relatives would be treated harshly if they spoke out about their imprisonment. In various instances, the authorities made false promises to family members that if they cooperated and revealed information to the authorities, this would make it easier for their loved one in jail.

[36] According to findings in the interviews.

Torture and other forms of ill-treatment

Many respondents reported torture and other forms of ill-treatment being used by the authorities during their detention to force them into a confession. Respondents reported excessively long periods of interrogation, repeated beatings by law enforcement officers, slapping, verbal abuse, and being kept in detention conditions that could constitute cruel, inhumane or degrading treatment.

Interrogations as the primary source of information

All respondents were asked during interrogations for passwords and information about their contacts, networks, and the organisers of protests movements or gatherings. Some of the less high-profile respondents were asked to write down all they knew about certain friends, co-workers and other contacts. One interviewee stated that a ‘large part’ of their interrogation consisted of writing down all the information they had about every single contact detail stored on their mobile phone.

This latter method was typically used by the authorities when they had flagged an individual but lacked information and intelligence on them.[37] This suggests that the authorities might not usually have the capability to access online accounts before arrest (apart from a few, infrequent cases of phishing), and therefore use arrests and interrogations as their primary means of gathering information.[38]

[37] The tactic is called singling out, ‘Tak-nevisi’ in Farsi, which forces the arrested individual to write about a particular (normally a high-level) member of their network.

[38] For more information about Iran’s internet infrastructure and capabilities refer to Small Media’s Iranian *Internet Infrastructure and Policy Report*: http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf

The impact on the online community in Iran

Social control

Summonses, temporary detentions and arrests are used to maintain social control and to spread fear amongst the internet user and activist communities. It is clear that, from the authorities' point of view, these tools and methods have been effective in encouraging the self-censorship of legitimate expression in these groups.

In small cities, the impact varied according to how well-known the activist was. Low-profile activists reported that they stopped their online activities entirely. Those activists considered more high-profile, on the other hand, only interrupted their online and offline activities temporarily.

The situation in Tehran was different. The respondents believed that intimidation was markedly less effective in the capital owing to the large population of the city, which rendered the authorities' task of following through after intimidation significantly more difficult due to a lack of resources.

Summonses and warnings not involving a prison sentence were used as a deterrent by the authorities, but were only reported in smaller cities.

Forced migration

The majority of respondents who were released on bail left the country. Significantly, almost half of these left the country between 2010 and 2012. Long gaps between court dates gave them the opportunity to cross the border to neighbouring countries – either on foot or by other means that avoided detection – suggesting that the granting of bail and the long gaps between court dates might have been a planned strategy by the authorities to allow activists to leave the country rather than keeping them in jail. Such a strategy decreases the cost to the authorities,[39] reduces the ability of activists to mobilise others, and weakens the legitimacy and sense of unity of those activists who choose to remain in Iran. The majority of the respondents who left Iran are no longer active online. Findings indicate that this is due to the readjustment and resettlement process in the country where they have taken refuge, as well as feelings of isolation.

[39] The Iranian government normally responds to international pressure on its human rights record. The number of people in jail increased drastically after the disputed elections of 2009 and Iran was in the international spotlight for its high volume of arrests. The government appeared to turn a blind eye when people took advantage of being out on bail and left the country.

Changes in habits

‘I am more aware of the friend requests I receive on Facebook now, and more aware of my privacy settings on social media platforms.’[40]

Many respondents no longer use their mobile phones to mobilise or contact others. Most try to use stronger passwords and do not save their passwords on their browsers or devices. They also try to delete their chat/conversation history more frequently. Respondents trust the reliability of built-in encryption offered by certain platforms, but most do not use extra encryption for communication due to its complexity.

Respondents also reported switching from what they understood to be less secure communication tools (including text messages and apps such as Tango and Viber) to what they considered to be more reliable secure platforms such as iMessage, WhatsApp, FaceTime, and Skype. However, respondents admitted that the switch to more secure platforms was actually motivated by facility of use rather than increased security. The use of dedicated secure messaging apps, such a Chatsecure[41] or Textsecure[42] was not reported.

Shared experience

Almost all respondents attempted to share the lessons they had learned with their peers after their release. However, they reported reluctance within the Iranian community to take online security measures seriously, due to apathy, carelessness or impatience. There is still a perception that security is a complicated task and therefore not worth the trouble. Many people believe that no matter what security procedures they put in place, the Iranian authorities will still be capable of breaching their digital security, illegally monitoring their online activities, and illegally gathering their personal data. These attitudes reflect a lack of understanding and a failure to grasp the opportunities for safe digital behaviour.

[40] Interview with ARTICLE 19.

[41] More information about the app can be found here: https://chatsecure.org/

[42] More information about the app can be found here: https://securityinabox.org/en/guide/textsecure/android

Online vs offline activism

For the interviewed respondents, online and offline activism amounts to the same thing. The life of an activist, particularly one who uses their real identity, takes place in both realms. Consequently the focus of Iran's authorities – and the methods they use – correspond to both online and offline monitoring and infiltration.

However, the majority of respondents reported that they were initially identified by the authorities for their offline activities. Their online activities only began to be monitored after they had been flagged offline. This could suggest that the authorities might not have the capacity to conduct widespread online surveillance and instead prefer to focus their efforts initially on provocative offline behaviour.

Those few respondents who were summoned exclusively due to their online activities, regardless of their background, had either criticised the Supreme Leader Khamenei, organised gatherings, or had a significant number of online followers. This suggests that political criticism, organising unauthorised gatherings or having a large number of online followers are the online activities deemed most worthy of surveillance and investigation by the Iranian authorities.

Major points of concern for the authorities

The authorities respond strongly to any group activities, and to any acts or public or private calls[43] organised by a network or group. When they discover networks, the authorities try to publically discredit them by making ties to foreign countries or funds, portraying them as a threat to national security[44]. This push to discover a network and ties to foreign aid is prevalent. The first questions the authorities ask during interrogations seek to establish, first, who/what organisation(s) outside Iran comprises the activist's 'network', and second, the activist's funding source.

Respondents also stated that the authorities gave particular attention to advocacy for armed struggle on online platforms, and 'secessionism' in certain areas where ethnic minorities are concentrated. Yet another sensitive area for the authorities is assemblies in universities. Regular summonses and systematic crackdowns on university students and their unions are used to spread a fear of persecution

[43] N.B. The word 'calls' here denotes a call for a public action, demonstration or protest.

[44] *Amnesty International Condemns Arrest of Six Individuals -- Documentary Filmmakers and a Film Producer -- in Iran*: http://www.amnestyusa.org/news/press-releases/amnesty-international-condemns-arrest-of-six-individuals-documentary-filmmakers-and-a-film-producer

and to deter gatherings and group mobilisation. In 2011, four members of the Democratic Union of Kurdish Students were arrested and several others summoned to security and intelligence offices[45].

Actual technical capability of the authorities

'My interrogator told me, 'You're in trouble now – we have discovered the internet in your house!' I didn't know whether to laugh or cry.'[46]

The assertion by the Iranian authorities of their ability to run universal surveillance contradicts the evidence, which shows a pattern of arrests followed by the seizure of technical equipment. Respondents suggested that the authorities sometimes make random arrests and then try to put together a case against the person arrested based on what is found on their computer or other device. Random arrests are normally followed by hefty fines, as set out in the *Computer Crimes Law*.

According to interviewees, the actual technical knowledge of interrogators is very limited, although that of IRGC interrogators is said to be higher than MOI interrogators. The interrogators did not manage to hack into the computer of any of the respondents; access to passwords was only achieved as a result of personal error or carelessness, or given up under pressure.

However, trends show that since 2009 the technical know-how and resources of the authorities have increased.[47] Again, this coincides with their realisation that online platforms have mobilisation potential. Once this had been understood, they invested heavily in capacity building and the recruitment of experts and professionals[48], who are often intimidated or offered generous incentives.

[45] *Joint Statement on the Right to Education and Academic Freedom in Iran* – http://www.iranhrdc.org/english/news/press-statements/1000000163-joint-statement-on-the-right-to-education-and-academic-freedom-in-iran.html

[46] Interview with ARTICLE 19.

[47] For more information about Iran's current internet infrastructure and capabilities refer to Small Media's *Iranian Internet Infrastructure and Policy Report:* http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf

[48] See ARTICLE 19's 2013 report *Computer Crimes in Iran: Online repression in practice:* http://www.article19.org/resources.php/resource/37385/en/computer-crimes-in-iran:-online-repression-in-practice

Lack of coordination and the intelligence gap

The findings of this report reveal that there is a clear intelligence and communication gap between the different bodies and offices of the Iranian authorities.

Geographical trends

Many respondents were evidence of the trend for the majority of arrests and intimidation to take place in Tehran, closely followed by Fars province. It is thought that the authorities in Fars province attempt to assert their intelligence and security capabilities with a combination of random arrests with heavy charges, a high volume of group arrests and significant levels of social control. Respondents believe that this is either due to a factional conflict within the security system, or has promotional incentives for those units involved.

Arrests, charges and imprisonment

In most cases, evidence about a person's case is based on what is found on their confiscated digital devices. Vague rules and regulations laid out in the *Computer Crimes Law* or Penal Code make it easy for the authorities to charge citizens with serious offences.

The majority of respondents were arrested with a warrant at their place of residence. A group of them turned themselves in after receiving an arrest warrant. A few of them had previously been arrested for their activities and some had had frequent briefing sessions with a designated security agent for months prior to their arrest.

The most common charges included: propaganda against the regime; acting against national security; insulting Supreme Leader Khamenei; secessionism and participation in armed struggle (for ethnic minority activists); spreading lies and acting against public morality and chastity.

Despite little mention of the fact throughout the interviews, almost all of the vague charges correspond to and are covered by the *Computer Crimes Law* (CCL) and the Penal Code. This indicates that although the arrests still continue to occur arbitrarily, as evidenced by the interviews, the Iranian authorities are ensuring the arrests are done in accordance with Iran's evolving national legislation.

Under such laws, individuals face severe criminal sanctions for trying to exercise their fundamental human rights, including their rights to freedom of expression, peaceful assembly and association and freedom of religion, and attempting to access or share legitimate information online.

Final Analysis and Conclusion

Final Analysis and Conclusion

The Iranian authorities have fostered a climate of fear and paranoia in Iran's online community. The high volume of arrests (including random arrests leading to severe penalties) of those engaged in online activities has allowed the authorities to maintain social control and this has resulted in legitimate use of the rights to freedom of expression and information being restricted. However, close scrutiny of the ways in which the authorities operate – especially how they gather information – neither proves nor disproves the authorities' skills and resources in successfully maintaining comprehensive countrywide surveillance and monitoring.

Based on our research, ARTICLE 19 believes that Iranian citizens, whether human rights defenders and activists, journalist or bloggers, will continue to be identified, monitored and targeted by the authorities of Iran on the basis of the cybercrime legislation. Insights from our research reveal that online users who exhibit some of the following characteristics are more vulnerable than others to unlawful arrest, torture and other ill-treatment and unfair trial:

- Those who take part in offline activities with established links to their online identity and records
- Those from much smaller cities who can easily be singled out
- Those with online influence and the potential to reach significant numbers, determined by the size of their audiences and levels of endorsement
- Those who use only the most little or no protective measures.

ARTICLE 19 believes that Iran's online community could improve their physical security, and thereby effectively improve their digital security practices. The digital security sentiment it still weak amongst Iranians, and users are generally reactive to incidents. They do not take preventative measures, which leaves them and their networks exposed. As long as nothing has happened to them personally, they are reluctant to change their online habits – either because of apathy, carelessness or the belief that it is pointless.

Our research also reveals that many Iranian online users do not commit to safer technologies (apps, platforms, guides, manuals and other tools) because they find the technology too complicated to use.

The extent of the authorities' know-how and resources is still to be determined, as the scope of this research gave ARTICLE 19 minimal and subjective data on the matter. However, ARTICLE 19 recognises that some identified gaps suggest that it is essential to have multi-sectorial[49] contingency plans in order to support those at imminent risk of danger.

[49] An approach where a multitude of organisations with various expertise intervene e.g. technology and business companies, NGOs, the UN and so forth.

The Way Forward: Recommendations

The Way Forward: Recommendations

Recommendations to the Islamic Republic of Iran

- Iran must stop targeting activists or subjecting them to surveillance. All targeted surveillance must be in accordance with Article 17 of the International Covenant on Civil and Political Rights. Mass surveillance (or 'bulk collection') is an inherently disproportionate interference with human rights[50], and the Islamic Republic of Iran must ensure it complies with international human rights standards in this regard.

- Iran's state-sponsored censorship activities, including the systematic filtering of internet content, should be stopped immediately. Any content filtering by the government or commercial service providers that is not end-user controlled is a form of prior censorship, not justifiable as a restriction on freedom of expression.[51]

- The legislative of the Islamic Republic of Iran must repeal the *Computer Crimes Law* in its entirety, and make comprehensive legal reform to legitimise the exercise of freedom of expression.

- Any law, such as the *Computer Crimes Law*, that imposes liability on Internet Service Providers for the content of expression that passes through their systems must be repealed immediately.

[50] ARTICLE 19, Privacy International, Human Rights Watch et al, OHCHR consultation in connection with General Assembly Resolution 68/167 *The right to privacy in the digital age*, 1 April 2014, available at: https://www.ef.org/fles/2014/04/17/ngo_submission_ fnal_31.03.14.pdf

[51] Joint declaration on freedom of expression and the Internet by the four special mandates on freedom of expression clearly stated in their 2011: http://www.osce.org/fom/78309

Recommendations to non-governmental organisations (NGOs) and technology developers working on digital rights in Iran

- Increase cooperation between NGOs and technology developers involved in digital rights in Iran. With further cooperation the following should be implemented:NGOs and technology developers should improve the usability of their materials and tools. Privacy by design should be standardised to protect users' right to privacy and freedom of expression. They must be designed to be seamlessly secure and bring about behavioural and cultural change that supports internet security, including for those with minimal knowledge of the technology involved.

    - There must be in-depth analysis of, and investigation into the Islamic Republic of Iran's actual capabilities and strategies for surveillance and censorship. It is also important for the power structure of internet control and policing in Iran to be analysed in order to confirm the findings presented in this report; namely that the authorities in charge of monitoring and arrests are decentralised and uncoordinated.

    - Contingency plans should be established and tailored for stakeholders, enabling them to take immediate action for individuals facing the highest levels of risk and threat.

- NGOs must place higher emphasis on lesser-known human rights defenders, particularly those from minority groups, ensuring that they receive equal support from NGOs and technology developers. Such groups must also be provided with the necessary recourse and tools to protect themselves from digital threat.

Recommendations to online users in Iran

- Online users should ensure they keep abreast of the latest security developments to the communication tools they use because of the impact on themselves and the people they communicate with. This requires giving both importance and attention to the information guides and packages provided by NGOs and technology developers.

- Users should use more secure platforms with built-in encryption (that have been audited), but should also familiarise themselves with and use extra layers of encryption for communication and storage of data. This must include the use of hard disk encryption to protect their data even if their phone, computer or laptop is confiscated by the authorities. Security practices should always be part of a 'threat model' where is also taken into account that the use of encryption software can also make one more identifiable by the authorities.

- Those taking part in online activism must ensure that they adopt basic security habits, such as deleting their correspondence, which may implicate them and their networks in online crimes; avoiding the use of real names; using secure passwords and password managers; mitigating risks when using smartphones and cell/mobile phones; deleting chat and browser histories; and creating a sense of shared accountability among individuals who participate in groups in the online realm.

- Online users must be highly vigilant when using public computers (especially in internet cafés) and printers in places such as university campuses or the workplace. As their personal data is regularly logged, along with browsing data, users must not use these devices for communication or to browse sensitive information.

- Online users should use only secure Virtual Private Networks (VPNs) or software that enables anonymous communication[52] when attempting to access filtered websites.

[52] Such as Tor. You can read more about Tor here: https://www.torproject.org/

- Facebook users must develop an understanding of the security vulnerabilities of Facebook's privacy settings and follow the basic security protocols on Facebook including:

  - Ensuring that their 'friends lists' are not visible to the public

  - Avoiding the use of public posts. Posts made about sensitive issues that may trigger the attention of the authorities should either be avoided or kept private.

  - Carefully selecting trusted members to participate in events that may be deemed a threat by the authorities rather than sending mass invitations.

  - When creating Facebook groups around sensitive issues, making groups private to ensure the contents of conversations remain secure and members are protected.

- Online users should remain wary and be alert to the existence of fake online accounts and 'agent provocateurs' when using social media. Those most exposed – such as group moderators and administrators – should be aware of and alert to the dangers of phishing and the growing use of online infiltration by the authorities.

- Online users and their family members should develop contingency plans for immediate use in case of arrest:

  - As there is usually a 'buffer zone' between the time of arrest and the removal of content from an individual's device or online accounts, one measure could be for a trusted third party to change passwords remotely, and/or delete sensitive information from hard drives.

  - In the event that the devices are not immediately confiscated during the arrest, friends and family should immediately move devices to a safe location.

Risky Online Behaviours which could land you in Jail

Stay uninformed of latest security developments

Never do hard-disk or email encryption to protect your sensitive data and correspondence.

Never delete sensitive email correspondence, chat and browsing history.

d*g

Always use super easy passwords

Always use your smart phones for everything that is deemed sensitive!

Always use unsafe, non-audited VPNs

Use Facebook and other social media platforms with no cautionary measures.

Never have a contigency plan for your digital footprint if you are arrested.

Appendix 1

List of questions

1 Briefly describe your recent or current activism. If none, please explain why you are not active.

2 Please describe the circumstances of your arrest by Iranian authorities, including roughly where it took place, when and how you were arrested.

3 What was the accusation brought against you and did your arrest result in prosecution?

4 To the best of your knowledge, how much did authorities know about you before you were arrested and how had they collected this information?

5 Did the authorities try to extract information from you during your arrest? If yes, please describe what they wanted to know and what methods they used to find out this information.

6 In what ways do you think your activities on the web contributed to your arrest and/or hardship you experienced during and after you were detained/prosecuted?

7 Were there any actions that you took on the web or while using digital technologies that you now think could have been avoided or carried out differently?

8 In your opinion, is there any information that you shared online prior to your arrest that harmed your case?

9 During and after the period of your prosecution, did you get in touch with other individuals who were being or had been prosecuted for their activities on the web or while using digital technologies? What similarities, if any, did you find between your case and theirs?

10 Did the experience of prosecution change any of your habits in using digital technologies?

11 Do you believe in and use safe communication such as encryption? If so, do you always use it?

12 Some argue that they notice and arrest individuals because of their online activity, while an opposite opinion is that activists are tagged because of their activities in the offline world and then their online activities provides a framework for finding out more about them. What do you think?

13 On a scale of one to five, how proficient was/were your interrogator(s) in IT and online activities? (Five being highly proficient and one being not proficient). Please explain.

14 On a scale of one to five, how sophisticated is the ability of authorities to monitor online activities and identify online activists? Please explain.

15 Do you have any suggestions for others who use digital technologies for social/political activism? How have you tried to communicate this to others and what feedback have received?

16 What recommendations do you have for tools or resources needed to help people improve online security? In what ways should these tools and resources be distributed?

17 What was your ISP?

18 Please share any other comments, suggestions or additional information you would like to add.

19 Please choose: Male, Female, Choose not to identify, Other-comment box

20 Age at the time of arrest. Please choose: Under 20, 20–25, 25–30, 30–35, 35+

DEFENDING FREEDOM OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org