Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**937**
Land:	Iran
Kilde:	British Home Office
Titel:	Country Policy and Information Note. Iran: Social media, surveillance and sur place activities
Udgivet:	marts 2022
Optaget på baggrundsmaterialet:	20. juni 2022

Home Office

Country Policy and Information Note

Iran: Social media, surveillance and sur place activities

Version 1.0

March 2022

Preface

Purpose

This note provides country of origin information (COI) and analysis of COI for use by Home Office decision makers handling particular types of protection and human rights claims (as set out in the Introduction section). It is not intended to be an exhaustive survey of a particular subject or theme.

It is split into 2 parts: (1) an assessment of COI and other evidence; and (2) COI. These are explained in more detail below.

Assessment

This section analyses the evidence relevant to this note - that is information in the COI section; refugee/human rights laws and policies; and applicable caselaw - by describing this and its inter-relationships, and provides an assessment of, in general, whether one or more of the following applies**:**

- a person is reasonably likely to face a real risk of persecution or serious harm
- that the general humanitarian situation is so severe that there are substantial grounds for believing that there is a real risk of serious harm because conditions amount to inhuman or degrading treatment as within paragraphs 339C and 339CA(iii) of the Immigration Rules/Article 3 of the European Convention on Human Rights (ECHR)
- that the security situation is such that there are substantial grounds for believing there is a real risk of serious harm because there exists a serious and individual threat to a civilian's life or person by reason of indiscriminate violence in a situation of international or internal armed conflict as within paragraphs 339C and 339CA(iv) of the Immigration Rules
- a person is able to obtain protection from the state (or quasi state bodies)
- a person is reasonably able to relocate within a country or territory
- a claim is likely to justify granting asylum, humanitarian protection or other form of leave, and
- if a claim is refused, it is likely or unlikely to be certifiable as 'clearly unfounded' under section 94 of the Nationality, Immigration and Asylum Act 2002.

Decision makers **must**, however, still consider all claims on an individual basis, taking into account each case's specific facts.

Country of origin information

The country information in this note has been carefully selected in accordance with the general principles of COI research as set out in the Common EU [European Union] Guidelines for Processing Country of Origin Information (COI), April 2008, and the Austrian Centre for Country of Origin and Asylum Research and Documentation's (ACCORD), Researching Country Origin Information – Training Manual, 2013. Namely, taking into account the COI's relevance, reliability, accuracy, balance, currency, transparency and traceability.

The structure and content of the country information section follows a terms of reference which sets out the general and specific topics relevant to this note.

All information included in the note was published or made publicly available on or before the 'cut-off' date(s) in the country information section. Any event taking place or report/article published after these date(s) is not included.

All information is publicly accessible or can be made publicly available. Sources and the information they provide are carefully considered before inclusion. Factors relevant to the assessment of the reliability of sources and information include:

- the motivation, purpose, knowledge and experience of the source
- how the information was obtained, including specific methodologies used
- the currency and detail of information
- whether the COI is consistent with and/or corroborated by other sources.

Multiple sourcing is used to ensure that the information is accurate and balanced, which is compared and contrasted where appropriate so that a comprehensive and up-to-date picture is provided of the issues relevant to this note at the time of publication.

The inclusion of a source is not, however, an endorsement of it or any view(s) expressed.

Each piece of information is referenced in a footnote. Full details of all sources cited and consulted in compiling the note are listed alphabetically in the bibliography.

Feedback

Our goal is to provide accurate, reliable and up-to-date COI and clear guidance. We welcome feedback on how to improve our products. If you would like to comment on this note, please email the Country Policy and Information Team.

Independent Advisory Group on Country Information

The Independent Advisory Group on Country Information (IAGCI) was set up in March 2009 by the Independent Chief Inspector of Borders and Immigration to support him in reviewing the efficiency, effectiveness and consistency of approach of COI produced by the Home Office.

The IAGCI welcomes feedback on the Home Office's COI material. It is not the function of the IAGCI to endorse any Home Office material, procedures or policy. The IAGCI may be contacted at:

Independent Advisory Group on Country Information
Independent Chief Inspector of Borders and Immigration
5th Floor
Globe House
89 Eccleston Square
London, SW1V 1PN
Email: chiefinspector@icibi.gov.uk

Information about the IAGCI's work and a list of the documents which have been reviewed by the IAGCI can be found on the Independent Chief Inspector's pages of the gov.uk website.

Contents

Assessment

Updated: 11 March 2022

1. Introduction

1.1 Basis of claim

1.1.1 Fear of persecution and/or serious harm by the state because of the person's social media use and/or sur place activities.

Back to Contents

2. Consideration of issues

2.1 Credibility

2.1.1 For information on assessing credibility, see the instruction on Assessing Credibility and Refugee Status.

2.1.2 Decision makers must also check if there has been a previous application for a UK visa or another form of leave. Asylum applications matched to visas should be investigated prior to the asylum interview (see the Asylum Instruction on Visa Matches, Asylum Claims from UK Visa Applicants).

2.1.3 In cases where there are doubts surrounding a person's claimed place of origin, decision makers should also consider the need to conduct language analysis testing (see the Asylum Instruction on Language Analysis).

Official – sensitive: Start of section

The information on this page has been removed as it is restricted for internal Home Office use.

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: End of section

Back to Contents

2.2 Exclusion

2.2.1 Decision makers must consider whether there are serious reasons for considering whether one (or more) of the exclusion clauses is applicable. Each case must be considered on its individual facts and merits.

2.2.2 If the person is excluded from the Refugee Convention, they will also be excluded from a grant of humanitarian protection (which has a wider range of exclusions than refugee status).

2.2.3 For further guidance on the exclusion clauses and restricted leave, see the Asylum Instruction on Exclusion under Articles 1F and 33(2) of the Refugee Convention, Humanitarian Protection and the instruction on Restricted Leave.

Official – sensitive: Start of section

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: End of section

Back to Contents

2.3 Convention reason(s)

2.3.1 Actual or imputed political opinion, race, and/or religion.

2.3.2 Establishing a convention reason is not sufficient to be recognised as a refugee. The question is whether the person has a well-founded fear of persecution on account of an actual or imputed Refugee Convention reason.

2.3.3 For further guidance on the 5 Refugee Convention grounds see the Asylum Instruction, Assessing Credibility and Refugee Status.

Back to Contents

2.4 Risk

a. State treatment within Iran

2.4.1 Iran's constitution and legal framework restricts freedom of expression and freedom online. Penalties for breaching the 2011 Cyber Crime law range from the death penalty for crimes committed against public morality and chastity, to lengthy custodial sentences, fines, and judicial orders to close organisations and ban people from using electronic communications (see Legal context).

2.4.2 The Iranian authorities have widespread control over the country's internet, which has approximately 57.4 million users in a total population of around 82 million. Iran improved and widened its cyber intelligence capabilities after the 2009 post-election Green Movement protests. Since then, significant restrictions on content have been in place. The Basij Cyber Council, the Cyber Police (FATA), the Cyber Army, the Iranian Revolutionary Guards Corps (IRGC) and its affiliated Centre to Investigate Organized Crimes (CIOC) are known to monitor and track alleged cyberthreats to national security or opposition to the government. This sometimes led to the arrest of online activists who may face charges for vaguely-worded offences such as 'anti-revolutionary behaviour', 'corruption on earth', 'siding with global arrogance', 'waging war against God', and 'crimes against Islam'. Iran increases its monitoring, and imposes local (and, on one occasion, nationwide) internet shutdowns, in the lead up to significant events, in times of political uncertainty and during outbreaks of protests (see Cyber surveillance in Iran).

2.4.3 Users have to use VPNs (virtual private networks) and other circumnavigation tools to access blocked websites and apps. A bill designed to give the armed forces and security services near total control of the internet, criminalise the use and distribution of VPNs, further restrict access to global providers and require people to register with an ID to access the internet, is expected to be passed by 20 March 2022 (see Legal context, Cyber surveillance in Iran, and Social media usage in Iran).

2.4.4 The online sphere is heavily monitored by the state, though there is no evidence to suggest that Iran operates a mass surveillance programme to monitor the online activity of all its citizens. Persons posting content critical of the government may attract adverse attention, especially if the content is shared on domestic messaging platforms. The authorities or its affiliates target social media accounts using spearphishing attacks (a targeted attack that uses a deceptive email to trick the recipient into performing an on-line action for the benefit of the adversary) or use malware to infect software. Primary targets of such attacks include government officials, reformist politicians, media professionals, religious minorities, cultural figures, opposition groups, terrorist organisations and ethnic separatist movements (see Cyber surveillance in Iran and Social media usage in Iran).

2.4.5 Thousands of people in Iran have been arrested and detained for their online activities, including for their criticism of the government, 'immoral' content, content deemed a national security issue, and for 'spreading false rumours'. Almost 75,000 people were arrested for online activities between 2010 and 2018, and 3,600 people were arrested between March 2020 and April 2021 for spreading online rumours relating to COVID-19. Those affected in recent years include prominent activists, Instagram 'celebrities', editors at independent news outlets, and citizen journalists associated with certain minority religious groups, such as Gonabadi dervishes and Baha'is. Charges brought against persons detained by FATA include the sale of illegal goods or services, financial crimes, and moral crimes, which particularly affect women. Those convicted may face harsh sentences, torture and mistreatment in prison and harassment and intimidation short of

imprisonment was reportedly common (see Arrest, detention and convictions).

2.4.6 The Iranian authorities are able to monitor the online activities of persons to varying degrees, depending on the platforms used, and any additional precautions taken by individuals, such as the use of an alias or VPN. Decision makers must be satisfied that the person is able to demonstrate that their online/social media activity has brought them, or will bring them, to the adverse attention of the authorities. Whether a person is at risk of persecution or serious harm from the state will depend on particular factors specific to them, for example, the person's profile, ethnic origin or religion, and/or the level and nature of their online activity. Each case must be considered on its facts with the onus on the person to show that they would be at real risk of serious harm or persecution on account of their actual or perceived political opinion, race or religion.

2.4.7 Social media users whose posts are deemed critical of the state or against its high moral standards, or who comment on sensitive issues, may be subject to treatment, including harassment, arrest, ill-treatment, torture and criminal charges, that is sufficiently serious, by its nature or repetition, to amount to persecution.

2.4.8 See also the Country Policy and Information Note on Iran: Kurds and Kurdish political parties.

2.4.9 For further guidance on assessing risk, see the instruction on Assessing Credibility and Refugee Status.

Back to Contents

b. Sur place activity – demonstrations

2.4.10 Sources indicate that Iranian intelligence officials or its affiliates monitor and target high profile Iranian dissidents living outside the country. Whilst numerous demonstrations occur in the UK against the Iranian government, as well as for Kurdish rights, the extent to which the Iranian authorities monitor such events is unclear (see Sur place activity).

2.4.11 In the Country Guidance case of BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC), heard on 5 and 6 October 2010 and promulgated on 10 February 2011, the Upper Tribunal (UT) held that:

'Given the large numbers of those who demonstrate here and the publicity which demonstrators receive, for example on Facebook, combined with the inability of the Iranian Government to monitor all returnees who have been involved in demonstrations here, regard must be had to the level of involvement of the individual here as well as any political activity which the individual might have been involved in Iran before seeking asylum in Britain.

'Iranians returning to Iran are screened on arrival. A returnee who meets the profile of an activist may be detained while searches of documentation are made. Students, particularly those who have known political profiles are likely to be questioned as well as those who have exited illegally.

'There is not a real risk of persecution for those who have exited Iran illegally or are merely returning from Britain. The conclusions of the Tribunal in the

country guidance case of SB (risk on return -illegal exit) Iran CG [2009] UKAIT 00053 are followed and endorsed.

'There is no evidence of the use of facial recognition technology at the Imam Khomeini International airport, but there are a number of officials who may be able to recognize up to 200 faces at any one time. The procedures used by security at the airport are haphazard. It is therefore possible that those whom the regime might wish to question would not come to the attention of the regime on arrival. If, however, information is known about their activities abroad, they might well be picked up for questioning and/or transferred to a special court near the airport in Tehran after they have returned home.

'It is important to consider the level of political involvement before considering the likelihood of the individual coming to the attention of the authorities and the priority that the Iranian regime would give to tracing him. It is only after considering those factors that the issue of whether or not there is a real risk of his facing persecution on return can be assessed' (headnotes 1 to 3).

2.4.12 The UT in BA also held that:

'The following are relevant factors to be considered when assessing risk on return having regard to sur place activities:

'(i) Nature of sur place activity

- Theme of demonstrations – what do the demonstrators want (e.g. reform of the regime through to its violent overthrow); how will they be characterised by the regime?
- Role in demonstrations and political profile – can the person be described as a leader; mobiliser (e.g. addressing the crowd), organiser (e.g. leading the chanting); or simply a member of the crowd; if the latter is he active or passive (e.g. does he carry a banner); what is his motive, and is this relevant to the profile he will have in the eyes of the regime?
- Extent of participation – has the person attended one or two demonstrations or is he a regular participant?
- Publicity attracted – has a demonstration attracted media coverage in the United Kingdom or the home country; nature of that publicity (quality of images; outlets where stories appear etc)?

'(ii) Identification risk

- Surveillance of demonstrators – assuming the regime aims to identify demonstrators against it, how does it do so, through filming them, having agents who mingle in the crowd, reviewing images/recordings of demonstrations etc?
- Regime's capacity to identify individuals – does the regime have advanced technology (e.g. for facial recognition); does it allocate human resources to fit names to faces in the crowd?

'(iii) Factors triggering inquiry/action on return

- Profile – is the person known as a committed opponent or someone with a significant political profile; does he fall within a category which the regime regards as especially objectionable?
- Immigration history – how did the person leave the country (illegally; type of visa); where has the person been when abroad; is the timing and method of return more likely to lead to inquiry and/or being detained for more than a short period and ill-treated (overstayer; forced return)?

'(iv) Consequences of identification

- Is there differentiation between demonstrators depending on the level of their political profile adverse to the regime?

'(v) Identification risk on return

- Matching identification to person – if a person is identified is that information systematically stored and used; are border posts geared to the task?' (headnote 4).

2.4.13 See also the Country Policy and Information Note on Iran: Kurds and Kurdish political parties.

2.4.14 For further guidance on assessing risk, see the instruction on Assessing Credibility and Refugee Status.

Back to Contents

c. Sur place activity – online

2.4.15 Whilst a number of sources reported on the Iranian state's ability to access and monitor user data by using malware and spearphishing, including in the diaspora, the level to which Iranian authorities can monitor the content of foreign social media platforms is unclear. Requests have been made to external providers by the Iranian authorities for mobile device data and/or Facebook user data, though the extent of how much data, if any, was provided is not known (see Cyber surveillance in Iran and Surveillance outside Iran).

2.4.16 In the country guidance case XX (PJAK – sur place activities - Facebook) Iran CG [2022] UKUT 23 (IAC), heard 8 to 10 June 2021 and promulgated on 20 January 2022, the Upper Tribunal (UT) held that:

'The cases of BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC); SSH and HR (illegal exit: failed asylum seeker) Iran CG [2016] UKUT 00308 (IAC); and HB (Kurds) Iran CG [2018] UKUT 00430 continue accurately to reflect the situation for returnees to Iran. That guidance is hereby supplemented on the issue of risk on return arising from a person's social media use (in particular, Facebook) and surveillance of that person by the authorities in Iran' (paragraph 120).

2.4.17 Regarding surveillance by the Iranian authorities, in the country guidance case XX the UT held that:

- Surveillance

'There is a disparity between, on the one hand, the Iranian state's claims as to what it has been, or is, able to do to control or access the electronic data

of its citizens who are in Iran or outside it; and on the other, its actual capabilities and extent of its actions. There is a stark gap in the evidence, beyond assertions by the Iranian government that Facebook accounts have been hacked and are being monitored. The evidence fails to show it is reasonably likely that the Iranian authorities are able to monitor, on a large scale, Facebook accounts. More focussed, ad hoc searches will necessarily be more labour-intensive and are therefore confined to individuals who are of significant adverse interest. The risk that an individual is targeted will be a nuanced one. Whose Facebook accounts will be targeted, before they are deleted, will depend on a person's existing profile and where they fit onto a "social graph;" and the extent to which they or their social network may have their Facebook material accessed.

'The likelihood of Facebook material being available to the Iranian authorities is affected by whether the person is or has been at any material time a person of significant interest, because if so, they are, in general, reasonably likely to have been the subject of targeted Facebook surveillance. In the case of such a person, this would mean that any additional risks that have arisen by creating a Facebook account containing material critical of, or otherwise inimical to, the Iranian authorities would not be mitigated by the closure of that account, as there is a real risk that the person would already have been the subject of targeted on-line surveillance, which is likely to have made the material known.

'Where an Iranian national of any age returns to Iran, the fact of them not having a Facebook account, or having deleted an account, will not as such raise suspicions or concerns on the part of Iranian authorities.

'A returnee from the UK to Iran who requires a laissez-passer or an emergency travel document (ETD) needs to complete an application form and submit it to the Iranian embassy in London. They are required to provide their address and telephone number, but not an email address or details of a social media account. While social media details are not asked for, the point of applying for an ETD is likely to be the first potential "pinch point, " referred to in AB and Others (internet activity - state of evidence) Iran [2015] UKUT 257 (IAC). It is not realistic to assume that internet searches will not be carried out until a person's arrival in Iran. Those applicants for ETDs provide an obvious pool of people, in respect of whom basic searches (such as open internet searches) are likely to be carried out' (paragraphs 121 to 124).

2.4.18 In regard to Facebook and social media evidence generally, the UT in XX held that:

- Guidance on Facebook more generally

'There are several barriers to monitoring, as opposed to ad hoc searches of someone's Facebook material. There is no evidence before us that the Facebook website itself has been "hacked," whether by the Iranian or any other government. The effectiveness of website "crawler" software, such as Google, is limited, when interacting with Facebook. Someone's name and some details may crop up on a Google search, if they still have a live Facebook account, or one that has only very recently been closed; and provided that their Facebook settings or those of their friends or groups with

whom they have interactions, have public settings. Without the person's password, those seeking to monitor Facebook accounts cannot "scrape" them in the same unautomated way as other websites allow automated data extraction. A person's email account or computer may be compromised, but it does not necessarily follow that their Facebook password account has been accessed.

'The timely closure of an account neutralises the risk consequential on having had a "critical" Facebook account, provided that someone's Facebook account was not specifically monitored prior to closure (paragraphs 125 to 126).

- Guidance on social media evidence generally

'Social media evidence is often limited to production of printed photographs, without full disclosure in electronic format. Production of a small part of a Facebook or social media account, for example, photocopied photographs, may be of very limited evidential value in a protection claim, when such a wealth of wider information, including a person's locations of access to Facebook and full timeline of social media activities, readily available on the "Download Your Information" function of Facebook in a matter of moments, has not been disclosed.

'It is easy for an apparent printout or electronic excerpt of an internet page to be manipulated by changing the page source data. For the same reason, where a decision maker does not have access to an actual account, purported printouts from such an account may also have very limited evidential value.

'In deciding the issue of risk on return involving a Facebook account, a decision maker may legitimately consider whether a person will close a Facebook account and not volunteer the fact of a previously closed Facebook account, prior to application for an ETD: HJ (Iran) v SSHD [2011] AC 596. Decision makers are allowed to consider first, what a person will do to mitigate a risk of persecution, and second, the reason for their actions. It is difficult to see circumstances in which the deletion of a Facebook account could equate to persecution, as there is no fundamental right protected by the Refugee Convention to have access to a particular social media platform, as opposed to the right to political neutrality. Whether such an inquiry is too speculative needs to be considered on a case-by-case basis' (paragraphs 127 to 129).

2.4.19 The UT in XX also found that:

'The evidence about Facebook account closure is unequivocal. It may be reversed before 30 days, but not after that time, and after deletion, the data on the person's Facebook account is irretrievable, even if their password is later discovered. The only exceptions to this are two limited pieces of residual data - limited caches of data, for a temporary period, on internet search engines; and photographs (but not links) on other people's Facebook accounts and messages sent to other people. Facebook account closure causes the data to be wholly inaccessible through or from Facebook or the user. However, if the data has been exported by a third party, that third party will continue to have access to the exported data, as stored' (paragraph 84).

2.4.20 The UT in XX acknowledged that, '… the Iranian state targets dissident groups, including religious and ethnic minorities, such as those of Kurdish ethnic origin' (paragraph 85).

2.4.21 In respect of the finding that a person of significant interest is, in general, reasonably likely to have been the subject of targeted Facebook surveillance, the UT in XX added:

'We refer to the level of political involvement of an individual, as in BA and HB; and the nature of "real-world" sur place activity, which would prompt such surveillance. By way of summary, relevant factors include: the theme of any demonstrations attended, for example, Kurdish political activism; the person's role in demonstrations and political profile; the extent of their participation (including regularity of attendance); the publicity which a demonstration attracts; the likelihood of surveillance of particular demonstrations; and whether the person is a committed opponent' (paragraph 92).

2.4.22 In XX the UT also found, 'Discovery of material critical of the Iranian regime on Facebook, even if contrived, may make a material difference to the risk faced by someone returning to Iran. The extent of the risk they may face will continue to be fact sensitive. For example, an Iranian person of Kurdish ethnic origin may face a higher risk than the wider population' (para 103).

2.4.23 In the 2015 reported case of AB and Others the UT also made reference to the opportunistic use of material deemed critical of the Iranian regime and held that:

'We do not find it at all relevant if a person had used the internet in an opportunistic way. We are aware of examples in some countries where there is clear evidence that the authorities are scornful of people who try to create a claim by being rude overseas. There is no evidence remotely similar to that in this case. The touchiness of the Iranian authorities does not seem to be in the least concerned with the motives of the person making a claim but if it is interested it makes the situation worse, not better because seeking asylum is being rude about the government of Iran and whilst that may not of itself be sufficient to lead to persecution it is a point in that direction' (paragraph 464).

2.4.24 The UT also went on to say:

'It is very difficult to establish any kind of clear picture about the risks consequent on blogging activities in Iran. Very few people seem to be returned unwillingly and this makes it very difficult to predict with any degree of confidence what fate, if any, awaits them. Some monitoring of activities outside Iran is possible and it occurs. It is not possible to determine what circumstances, if any, enhance or dilute the risk although a high degree of activity is not necessary to attract persecution' (paragraph 466).

2.4.25 The factors cited in XX, that is, Kurdish political activism and persons of Kurdish ethnic origin (paragraphs 92 and 103), and in AB and Others regarding the opportunistic use of material critical of the Iranian regime (paragraph 464), should be taken into account when assessing risk of directed Facebook surveillance against a person of Kurdish ethnic origin, in view of the findings in HB, in that:

'Even "low-level" political activity, or activity that is perceived to be political, such as, by way of example only, mere possession of leaflets espousing or supporting Kurdish rights, if discovered, involves the same risk of persecution or Article 3 ill-treatment. Each case, however, depends on its own facts and an assessment will need to be made as to the nature of the material possessed and how it would be likely to be viewed by the Iranian authorities in the context of the foregoing guidance' (paragraph 98 (9)).

2.4.26 See also the Country Policy and Information Note on Iran: Kurds and Kurdish political parties.

2.4.27 For further guidance on assessing risk, see the instruction on Assessing Credibility and Refugee Status.

Back to Contents

2.5 Protection

2.5.1 Where the person has a well-founded fear of persecution from the state they will not, in general, be able to obtain protection from the authorities.

2.5.2 For further guidance on assessing the availability of state protection, see the instruction on Assessing Credibility and Refugee Status.

Back to Contents

2.6 Internal relocation

2.6.1 Where the person has a well-founded fear of persecution or serious harm from the state, they are unlikely to be able to relocate to escape that risk.

2.6.2 For further guidance on internal relocation see the instruction on Assessing Credibility and Refugee Status.

Back to Contents

2.7 Certification

2.7.1 Where a claim is refused, it is unlikely to be certifiable as 'clearly unfounded' under section 94 of the Nationality, Immigration and Asylum Act 2002.

2.7.2 For further guidance on certification, see Certification of Protection and Human Rights claims under section 94 of the Nationality, Immigration and Asylum Act 2002 (clearly unfounded claims).

Back to Contents

Country information

Section 3 updated: 11 March 2022

3. Legal context

3.1 Domestic legal framework

3.1.1 A 2012 report by Article 19, a UK-based organisation which promotes the right for freedom of expression, provided an overview of the domestic legal framework relating to freedom of expression in Iran, including the Constitution of the Islamic Republic of Iran, which Article 19 said, '… lays the foundations for the institutionalisation of censorship.'[1] The report also noted, '… the Press Law of 1986 [amended 2000] and the Islamic Penal Code provide for content-based restrictions on freedom of expression and have been the principal instruments of repressing electronic and Internet-based expression.'[2]

3.1.2 Article 19 went on to cite the 2011 Cyber Crime Law (CCL), noting it was, '… saturated with provisions that criminalise legitimate expression. Crimes against "public morality and chastity" and the "dissemination of lies" are engineered to ensnare all forms of legitimate expression.'[3] The report added that the CCL was:

'… made up of 56 articles divided into 3 parts: Part One, Crimes and Punishment; Part Two, Civil Procedure; Part Three, Other Regulations. No article in the legislation indicates the overarching purpose of the law, nor provides for definitions of key terms. A handful of generally inadequate definitions are provided for with sporadic specificity in footnotes to a minority of articles. The law contains no guarantee for the right to freedom of expression or access to information.'[4]

3.1.3 The report provided an analysis of the CCL's various articles and also noted the penalties, which included:

'… the death penalty for crimes committed against public morality and chastity. Other sanctions on legitimate expression include lengthy custodial sentences, draconian fines, and judicial orders to close organisations and ban individuals from using electronic communications. These penalties also apply to Internet Service Providers that fail to enforce content-based restrictions, incentivising the private sector to promulgate Iran's censorship culture.'[5]

3.1.4 The US Department of State (USSD) noted in its human rights report, covering 2020 events, that:

'The government often charged political dissidents with vague crimes, such as "antirevolutionary behavior," "corruption on earth," "siding with global arrogance," "waging war against God," and "crimes against Islam."

[1] Article 19, 'Islamic Republic of Iran: Computer Crimes Law', 5 April 2012
[2] Article 19, 'Islamic Republic of Iran: Computer Crimes Law', 5 April 2012
[3] Article 19, 'Islamic Republic of Iran: Computer Crimes Law', 5 April 2012
[4] Article 19, 'Islamic Republic of Iran: Computer Crimes Law', 5 April 2012
[5] Article 19, 'Islamic Republic of Iran: Computer Crimes Law', 5 April 2012

'Prosecutors imposed strict penalties on government critics for minor violations.

'The political crimes law defines a political crime as an insult against the government, as well as "the publication of lies." Political crimes are those acts "committed with the intent of reforming the domestic or foreign policies of Iran," while those with the intent to damage "the foundations of the regime" are considered national security crimes. The court and the Public Prosecutor's Office retain responsibility for determining the nature of the crime.'[6]

3.1.5 An article dated 14 October 2021 in The Iran Primer, a project of the United States Institute of Peace, stated:

'In July 2021, Parliament introduced a new bill that could further limit public access. The legislation is called "Cyberspace Users Rights Protection and Regulation of Key Online Services." … The bill would essentially place Iran's Internet gateways in the hands of the armed forces; make it illegal to use virtual private networks (VPNs); and potentially criminalize those who use and distribute VPNs (although the language on the legal repercussions in the latest draft are still quite vague).'[7]

3.1.6 Also reporting on the new bill, the Committee to Protect Journalists (CPJ) stated that it would, '… require people to register with an ID to access the Internet…', adding that, according to media reports, it was due to be ratified in early 2022[8].

3.1.7 On 22 February 2022, a special parliamentary committee approved the general outline of the bill and those backing it hoped it would be finalised by 20 March 2022[9] [10] [11]. Though yet to be approved, observers said the scope of the bill had widened to include 'all online platforms, businesses and shops.'[12]

Back to Contents

Section 4 updated: 11 March 2022

4. Cyber surveillance in Iran

4.1 State control of online activity

4.1.1 In February 2017, Article 19 reported on Iran's so-called 'Soft-War', in reference to the government's restrictions on online activity, noting:

'The widely-disputed 2009 elections and their immediate aftermath, including the rise of online communication and content as part of the "Green Movement", were met with a crackdown on expression online: a response to the surge in usage of online fora and communications for expressing dissent and civic organisation… To counter this trend, the government has implemented monitoring and filtering techniques, alongside a far-reaching

[6] USSD, '2020 Country Reports on Human Rights Practices…' (section 1E), 30 March 2021
[7] The Iran Primer, 'New "Protection" Bill on Internet Freedom', 14 October 2021
[8] CPJ, 'Iran's parliament moves forward with troubling bill to further restrict internet', 1 November 2021
[9] Al Jazeera, 'Iran: Controversial internet control bill passes committee stage', 22 February 2022
[10] Al Monitor, 'Iran pushes ahead with internet "protection" bill', 23 February 2022
[11] OWP, 'Iran's "Protection Bill" To Enhance Internet Clampdown', 6 March 2022
[12] Al Jazeera, 'Iran: Controversial internet control bill passes committee stage', 22 February 2022

legal framework, to aid the prosecution of those suspected of undesirable online expression and activities.'[13]

4.1.2 A 2018 paper on Iran's Cyber Threat, published by the Carnegie Endowment for International Peace (CEIP) reported on the state's capabilities in surveilling and intercepting the communications of its citizens, both in Iran and in the diaspora. The report noted:

'During the Green Movement, pro-regime hackers engaged in a multipronged strategy of intrusions, disruption of websites, and network surveillance. Between December 2009 and June 2013, a group calling itself the Iranian Cyber Army defaced websites associated with Iran's political opposition, Israeli businesses, independent Persian-language media, and social media platforms, posting pro-government messages.

'Ultimately, the brutality, surveillance, and censorship exercised by the security forces debilitated the Green Movement, and by 2011 public protests had subsided. Security agencies had adapted to the modern digital environment, with interrogations by the IRGC including an intimate review of an arrestee's personal life based on printed copies of his or her online communications and social media. An IRGC chief later said that suppressing the demonstrations required widespread arrests, massive repression, and cutting off means of mass communication, such as cellphones and the internet.'[14]

4.1.3 The Australian Department of Foreign Affairs and Trade (DFAT) published a country report on Iran on 14 April 2020, based on a range of sources. The report stated:

'Iranians are able to criticise the government of the day robustly, both in public conversation and online in social media, although this freedom is not unlimited – a number of well-established "red line" topics are off-limits and critical commentary may lead to prosecution under national security legislation… Social media accounts of well-known figures and celebrities attract particular scrutiny… Authorities are more likely to crack down on dissent during times of political uncertainty, such as during ongoing political demonstrations, and may restrict the ability of individuals to comment or communicate online at such times.'[15]

4.1.4 The USSD human rights report for 2020 noted that, 'The Ministries of Culture and of Information and Communications Technology are the main regulatory bodies for content and internet systems and maintain monopoly control over internet traffic flowing in and out of the country. The Office of the Supreme Leader also includes the Supreme Council of Cyberspace, charged with regulating content and systems.'[16]

4.1.5 A September 2020 report by Article 19 noted, 'Iran's authorities have extensive control over around 57.4 million Internet users in a total population of about 82 million. This control has been achieved through extreme

[13] Article 19, 'Tightening the Net Part 2: The Soft War and…' (pages 12 and 16), 3 February 2017
[14] CEIP, 'Iran's Cyber Threat: Espionage, Sabotage, and Revenge' (page 11), 4 January 2018
[15] DFAT, 'Country Information Report Iran' (paragraph 3.81), 14 April 2020
[16] USSD, '2020 Country Reports on Human Rights Practices…' (section 2A), 30 March 2021

centralisation of both the infrastructure and authority over telecommunications companies and actors.'[17]

4.1.6 The Freedom on the Net 2021 report by Freedom House, covering the period 1 June 2020 to 31 May 2021, noted that, 'Internet freedom remained highly restricted in Iran during the coverage period. The government ordered localized internet shutdowns amid antigovernment protests and continued to block access to independent news sites as well as a number of social media and communication platforms.'[18]

4.1.7 Reporting on internet shutdown trends between November 2019 and July 2021, Filterwatch, a project working for a free and open internet in Iran, noted:

'Iran experienced its first nationwide Internet shutdown during protests against fuel price increases in November 2019, when government authorities imposed a near total internet shutdown for at least a week to provide cover for a violent crackdown against protestors. While we have not observed any nationwide shutdowns in Iran since then, this is due to a shift in information control tactics, rather than a lifting of restrictions.

'In fact, we have seen a steady increase in the number of internet shutdowns implemented at the local level, in order to contain protests, and limit information emerging about other forms of unrest. Since November 2019, there have been at least five instances of localised Internet shutdowns across Iran, with the most recent imposed in July 2021 following the outbreak of protests about water shortages in Khuzestan province.'[19]

4.1.8 The Freedom on the Net 2021 report noted:

'Authorities restrict access to tens of thousands of websites, particularly those of international news and information services, the political opposition, ethnic and religious minority groups in Iran, and human rights organizations. Websites are also blocked if they contradict state doctrine regarding Islam or government narratives on domestic or international politics. News stories that cover friction between Iranian political institutions are frequently censored.'[20]

4.1.9 The September 2020 Article 19 report explained Iran's National Information Network (NIN), noting:

'In 2012, Iran initiated the development of a NIN, a domestic Internet infrastructure hosted inside Iran, with the aim of being secure from foreign attacks, but may potentially be disconnected from the global Internet.

'Elements of the NIN have already been launched, including national infrastructure for banking and payment methods. The existence of the NIN has not yet resulted in long-term disconnection from the global Internet, but it has been a short-term tool to support shutdowns during protests and unrest.'[21]

[17] Article 19, 'Iran: Tightening the Net 2020, After Blood and Shutdowns' (page 13), September 2020
[18] Freedom House, 'Freedom on the Net 2021: Iran' (Overview), 21 September 2021
[19] Filterwatch, 'Internet Shutdown Trends in Iran: November 2019 to July 2021', 3 September 2021
[20] Freedom House, 'Freedom on the Net 2021: Iran' (B1), 21 September 2021
[21] Article 19, 'Iran: Tightening the Net 2020, After Blood and Shutdowns' (page 23), September 2020

4.1.10 The Freedom on the Net 2021 report noted, 'In February 2020, the Supreme Council for Cyberspace (SCC), Iran's top internet policymaking body, began dedicated meetings to set five-year targets for the expansion of the National Information Network (NIN), the country's localized internet architecture. The new plan was approved by the SCC in September 2020.'[22]

4.1.11 Users must use VPNs (virtual private networks) and other circumnavigation tools to access blocked websites and apps[23] [24]. The Freedom on the Net 2021 report cited a May 2019 media interview with the head of the circumvention provider Psiphon, who claimed that between one and 2 million people in Iran used its service daily[25]. Iran International reported, 'Almost every Iranian uses a circumvention method to gain unrestricted access to the Internet, although the connection speed is usually slow.'[26] However, as noted in the Freedom on the Net 2021 report, '…the government regularly seeks to disrupt access to VPNs and has also made efforts to establish a "legal VPN" scheme in order to control access to the tools.'[27]

Back to Contents

4.2 Cyber police (FATA)

4.2.1 A joint report on Iran's criminal procedures based on a range of sources, dated December 2021, by the Norwegian Country of Origin Information Centre (Landinfo), the Office of the Commissioner General for Refugees and Stateless Persons (CGRS – Belgium) and the Swiss State Secretariat for Migration (SEM), noted:

'The Iranian Cyberspace Police, literally "police of the virtual space and information exchange" (polīs-e fazā-ye toulīd va tabādol-e ettelā'āt), commonly referred to by its acronym FATA was created in 2011. FATA is tasked with combating cybercrimes, such as financial scams and violations of privacy, as well as suppressing any form of online criticism perceived as propaganda against the state (political, religious, or otherwise). It is also involved in monitoring, tracking, intimidating, and arresting online activists, especially bloggers and those active on social media. Its responsibilities also include targeting those who create and sell virtual private network (VPN) accesses. Their responsibilities overlap with those of the Centre to Investigate Organized Crimes (CIOC) of the IRGC… However, while the latter mostly deals with issues related to national security, FATA is also tasked with monitoring morality-related offences in cyber space. They can include videos on social media of girls modelling, dancing or generally not complying with national Islamic dress codes or web sites advertising gambling. FATA has offices in major cities.'[28]

Back to Contents

[22] Freedom House, 'Freedom on the Net 2021: Iran' (A1), 21 September 2021
[23] Article 19, 'Iran: Tightening the Net 2020, After Blood and Shutdowns' (page 13), September 2020
[24] Iran International, 'Foreign Social Media Apps Remain Highly Popular In…', 18 September 2021
[25] Freedom House, 'Freedom on the Net 2021: Iran' (B1), 21 September 2021
[26] Iran International, 'Foreign Social Media Apps Remain Highly Popular In…', 18 September 2021
[27] Freedom House, 'Freedom on the Net 2021: Iran' (B1), 21 September 2021
[28] Landinfo and others, 'Iran; Criminal procedures and documents' (page 20), December 2021

4.3 Islamic Revolutionary Guard Corps (IRGC) Cyber Defense Command

4.3.1 The joint Landinfo, CGRS and SEM report noted:

'The IRGC Cyber Defense Command (qarārgāh-e defā'-e sāiberī) is the cyber intelligence organization of the IRGC. Its tasks include monitoring and prosecuting organized cybercrime, terrorism, espionage, fighting against "online destruction of cultural and social values", and tracking insults or defamation of revolutionary values. Affiliated with the Cyber Defense Command is the Centre to Investigate Organized Crimes (CIOC) (markaz-e barrasī-ye jarā'em-e sāzmān-yāfteh). This unit has been involved in various prominent cyber operations.

'The responsibilities of the IRGC Cyber Defense Command and the CIOC overlap with those of the Cyber Police (FATA). However, the CIOC mostly deals with issues related to national security, such as online material produced by Kurdish parties or other political movements. The IRGC Cyber Defense Command and the CIOC also deal with people advocating for Christianity on social media, as this is considered a matter of national security. The responsibilities of FATA focus more on common cybercrimes, including "moral crimes"…'[29]

Back to Contents

4.4 State monitoring of online activity

4.4.1 Citing an Iranian web provider, a 2016 article by CHRI noted that:

'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.'[30]

4.4.2 Article 32 of the Cybercrimes Bill requires ISPs (internet service providers) to maintain information related to their traffic for at least six months, as well as personal information on their users for a minimum of six months after the end of their subscription[31].

4.4.3 The 2018 CEIP paper on Iran's Cyber Threat cited incidences in which social media accounts, including Facebook, had been targeted (with spearphishing attacks[32]) by the Iranian state or its affiliates, noting that the targets were primarily: Government officials, reformist politicians, media professionals,

[29] Landinfo and others, 'Iran; Criminal procedures and documents' (page 24), December 2021
[30] CHRI, 'Iranians Looking Abroad to Escape State-Controlled Internet', 14 March 2016
[31] SHERLOC, UNODC, 'Iran Computer Crimes Act', no date
[32] Spearphishing: A targeted attack that uses a deceptive email to trick the recipient into performing some kind of dangerous action for the adversary

religious minorities, cultural figures, and opposition groups, terrorist organisations and ethnic separatist movements[33].

4.4.4 The report noted:

'While the internet has afforded Tehran's security agencies new possibilities for surveilling and intercepting the communications of its citizens, concurrent information technologies also limit the reach of the state. Iran was one of the first countries in the Middle East to connect to the internet, and as a result over half of the population was frequently using the internet as of March 2017. Iranian internet users have been quick to embrace social media and chat applications in large numbers as forums where there are more social freedoms.

'As Iranian citizens have moved their communications to internet platforms hosted outside Iran and protected their communications from eavesdropping by using encryption, they have also evaded the more traditional means by which Iranian law enforcement and intelligence agencies perform surveillance. Whereas local hosting providers and social media could be compelled to remove content and disclose account ownership information, platforms hosted outside Iran are beyond the direct reach of the state.'[34]

4.4.5 However, the same report added, 'Since at least July 2014 a pattern has emerged: individuals in the custody of the IRGC are forced to provide access to their online accounts and devices, which are then immediately used to conduct spearphishing attacks associated with known threat actors.'[35]

4.4.6 According to the DFAT report of April 2020:

'The authorities monitor social media. Individuals posting content openly critical of the Islamic Republic, its institutions and policies or deemed to be pushing moral boundaries may attract adverse attention, including individuals based abroad. Local sources told DFAT that Iranians with links to Iran-based foreigners are more likely to have their social media accounts monitored. To avoid detection, it is common for persons critical of the Islamic Republic on permitted social media platforms to use aliases to conceal their identity.'[36]

See also Surveillance outside Iran.

4.4.7 The USSD's human rights report for 2020 noted 'The government monitored meetings, movements, and communications of its citizens and often charged persons with crimes against national security and for insulting the regime, citing as evidence letters, emails, and other public and private communications. Authorities threatened arrest or punishment for the expression of ideas or images they viewed as violations of the legal moral code.'[37]

4.4.8 The same source reported:

[33] CEIP, 'Iran's Cyber Threat: Espionage, Sabotage, and Revenge' (pages 41 to 47), 4 January 2018
[34] CEIP, 'Iran's Cyber Threat: Espionage, Sabotage, and Revenge' (page 39), 4 January 2018
[35] CEIP, 'Iran's Cyber Threat: Espionage, Sabotage, and Revenge' (page 26), 4 January 2018
[36] DFAT, 'Country Information Report Iran' (paragraph 3.111), 14 April 2020
[37] USSD, '2020 Country Reports on Human Rights Practices…' (section 2A), 30 March 2021

'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 cyberthreats to national security. These organizations especially targeted citizens' activities on officially banned social networking websites such as Telegram, Facebook, Twitter, YouTube, and Flickr, and they reportedly harassed persons who criticized the government or raised sensitive social problems.'[38]

4.4.9 Reporting on to nationwide protests, which took place in November 2019 against the hike in fuel prices, the Danish Immigration Service, citing a range of sources, noted that:

'The Iranian authorities used footage from closed-circuit cameras (CCTV) and videos on social media platforms to identify protesters, and a number of people were arrested in their homes and workplaces. Ehsan Mehrabi [a freelance Iranian journalist based in Germany] explained that since the November 2019 demonstrations took place in relatively small towns, it was easier for the authorities to identify people by use of local networks, because people in smaller towns typically know more of each other's activities.

'According to a human rights activist cited by CHRI, detainees who had shared news or videos of the protests were being treated more harshly, especially if they had any history of activism.'[39]

4.4.10 According to the USSD's 2020 human rights report, the Iranian authorities 'monitor private online communications' and 'collected personally identifiable information in connection with citizens' peaceful expression of political, religious, or ideological opinion or beliefs.'[40]

4.4.11 The Freedom on the Net 2021 report by Freedom House noted:

'The Telecommunication Company of Iran (TCI) retains a monopoly on internet traffic flowing in and out of the country. In addition, the TCI's dominance of the ISP [internet service provider] market creates opportunities for the security apparatus to monitor online activity, since the company's majority shareholder is the Islamic Revolutionary Guard Corps (IRGC), a powerful branch of the security forces that also controls large portions of the economy…'[41]

4.4.12 The same report noted:

'The online sphere is heavily monitored by the state despite Article 37 of the nonbinding Citizens' Rights Charter, which states that online privacy should be respected. In April 2018, supreme leader Khamenei issued a fatwa related to users' privacy on social media and online messaging, saying, "the officials must safeguard the people's and the country's security and privacy. Invading the privacy and security of the people is religiously forbidden, and against the Islamic law and must not be undertaken." However, the fatwa

[38] USSD, '2020 Country Reports on Human Rights Practices…' (section 2A), 30 March 2021
[39] Danish Immigration Service, 'Iran: November 2019 Protests' (pages 24 and 40), July 2020
[40] USSD, '2020 Country Reports on Human Rights Practices…' (section 2A), 30 March 2021
[41] Freedom House, 'Freedom on the Net 2021: Iran' (A3), 21 September 2021

has not been enshrined into law. There are currently no comprehensive data-protection laws in place in the country.'[42]

4.4.13 The report also stated, 'The state monitors social media for activity it deems illegal. In May 2020, FATA announced that not wearing the hijab online would be considered a crime, and that those who do not follow this rule would be prosecuted.'[43] Furthermore, 'Given that the operation of domestic messaging apps is based inside the country, content shared on them is more susceptible to government control and surveillance.'[44]

4.4.14 In its Yearbook 1398, covering the period March 2019 to March 2020, Filterwatch reported:

'Although there is no evidence to suggest that Iran operates a mass surveillance programme to monitor its citizens, the enforcement practices and public statements made by Iran's Cyber Police (FATA) nonetheless indicate the existence of active and far-reaching policing operations in online spaces…

'Their actions, and the large-scale arrest of individuals based on their online activities also demonstrate that these surveillance measures are not being implemented solely for protection against exceptional national security threats, but to crack down on online expression – including political speech, but also other forms of expression that contravene state sanctioned moral standards.'[45]

4.4.15 According to the Association of Human Rights in Kurdistan – Geneva (KMMK-G), an independent organisation with partners in the Kurdistan Region of Iran (KRI) and in Iranian Kurdistan, who were interviewed by the Danish Immigration Service for its report on Iranian Kurds published in February 2020, '… the IRGC has created a cyber-army of an estimated 45,000 personnel whose main task is to monitor and collect information on people opposing the Iranian government, including critics, academics, intellectuals, students and activists.'[46]

4.4.16 In 2020, a special task force was created by cyber police '… to tackle "cyber rumours" and "fake news" related to COVID-19 on social media…', according to Amnesty International[47].

4.4.17 IranWire, a joint venture of a group of Iranian journalists in the diaspora[48], reported in June 2020 that:

'On June 23, 2020, the Public Security chief Ali Zolghadri announced that in addition to the monitoring carried out by Iran's Cyber Police [FATA], law enforcement would also assign additional police to monitor Instagram posts and Instagram Live videos. Zolghadri said this extra surveillance would focus on various issues such as "criminals, thugs and gangsters," "weapons smugglers and arms dealers" and "troublemakers and those who violate

[42] Freedom House, 'Freedom on the Net 2021: Iran' (C5), 21 September 2021
[43] Freedom House, 'Freedom on the Net 2021: Iran' (C5), 21 September 2021
[44] Freedom House, 'Freedom on the Net 2021: Iran' (B5), 21 September 2021
[45] Filterwatch, 'Filterwatch Yearbook 1398 (March 2019 – March 2020)' (page 18), 10 June 2021
[46] Danish Immigration Service, 'Iranian Kurds…' (page 54), February 2020
[47] Amnesty International, 'Iran 2020', 17 April 2021
[48] IranWire, 'About us', no date

moral standards." … In his announcement on June 23, Ali Zolghadri also confirmed that some online activists had been under surveillance and that they had been summoned to face legal action.'[49]

4.4.18 IranWire noted other comments made by cyber security officials:

'Prior to Zolghadri's announcements, on April 14, 2020, Touraj Kazemi, the Head of Tehran's Cyber Police Force, announced that the force would be monitoring Instagram Live videos and added that any user who used Instagram Live within the country would be monitored. He said: "Even if it is not possible for the police to monitor all the live broadcasts, other pages that repost the live broadcasts will be also reviewed by the police."

'Ramin Pashaei, Deputy for Social Affairs of the Iranian Cyber Police, also said on April 12, 2020, that those who do not wear their hijab when they appear in online videos will be considered to be "violators" of moral standards. Pashaei also said it did not matter whether the individual in question had a popular following on social media or not.

'Pashaei said: "There is no difference between crimes committed online and those committed in person, any act that disturbs the public opinion will result in definitive legal repercussions." He went on to say that any previously undefined or uncertain action [shown on Instagram] could be legally prosecuted within the criminal definition of "disturbing the public opinion."'[50]

4.4.19 For the period March 2020 to March 2021, Filterwatch reported in its Yearbook 1399:

'Iran's Cyber Police (FATA) continues to play a leading role in the implementation of online surveillance in Iran. In late 2018, we have seen high-ranking FATA officials boasting about "society-based surveillance" in which "every citizen is a police officer", relying on thousands of volunteers to help them monitor online spaces. Since then, our FATAwatch project has documented many hundreds of arrests for charges stretching from online fraud, to vague accusations of "spreading rumours", and to loosely-defined morality charges.'[51]

See also Arrest, detention and convictions.

4.4.20 In August 2021, IranWire reported on identity theft and fake accounts created on the domestic messaging app, Rubika, whose sole shareholder was owned by the IRGC at the time of the apps creation in 2017. One social media expert claimed the fake accounts were created to make it appear the app was trusted and approved by users. IranWire noted:

'Iranian social media users have denounced a domestic messaging app, Rubika, for serial identity theft. The row broke out at the weekend after Twitter user and social media marketing specialist Houman Ghorbanian searched for his name on Rubika. He discovered the app had registered a fake account using his name and photo, crawling and uploading all his real Instagram posts onto the fake page on a daily basis. Within a few hours,

[49] IranWire, 'Police crackdown on live Instagrams', 26 June 2020
[50] IranWire, 'Police crackdown on live Instagrams', 26 June 2020
[51] Filterwatch, 'Filterwatch Yearbook 1399 (March 2020 – March 2021)' (page 22), 11 June 2021

hundreds of Twitter users were posting identical allegations. The furious victims included ordinary citizens, footballers and artists.'[52]

4.4.21 In November 2021, Filterwatch also referred to the unauthorised Rubika profiles, noting:

'In a statement Rubika claimed that these accounts were likely created by other users, though the app requires a phone number for account creation. Initially, users were able to check if an account had been created in their name via a weblink, however the feature was eventually disabled, forcing users to download the app in order to check for the copied accounts. Meanwhile, Iran's Cyber Police (FATA), announced that they would investigate the "unauthorised use of personal user data and creation of accounts without [users'] consent." However, at the time of writing, there was no information on FATA taking any action on Rubika's behaviour.'[53]

4.4.22 Citing a 2015 report, the Freedom on the Net 2021 report noted that, 'State agencies such as the IRGC have pressured or coerced detained activists into handing over log-in details for their social media accounts, which the authorities have then used for surveillance and phishing attacks. This seems to be part of a broader pattern, as a number of activists have reported phishing attempts that were apparently sponsored by the government.'[54]

4.4.23 The Atlantic Council, an American think tank on international affairs, published a report on 22 January 2022 on social media in Iran, based on a range of sources, reported numerous instances where social media users were forced to delete posts or have their accounts suspended, or actually had their accounts closed or suspended by the authorities. In some cases, users were arrested and detained, or convicted and imprisoned or given suspended sentences[55].

See also Arrest, detention and convictions.

Back to Contents

4.5 Use of malware

4.5.1 In May 2019, the Center for Human Rights in Iran (CHRI) reported on the Iranian state's use of malware targeting religious minority groups, both inside and outside, Iran and noted:

'The malware has multiple capabilities that enable the state to identify private user information, communications and contacts, which severely endangers the attacked account holders. The Islamic Republic arrests and imprisons dissidents based on online communications. The spyware can:

- Gather a list of existing files on the victim's computer.
- Take screenshots of the monitor at the attacker's discretion.
- Record keyboard impressions.

[52] IranWire, 'Iranians Furious at Identity Theft by IRGC's Instagram Ripoff', 16 August 2021
[53] Filterwatch, 'The Role of Domestic Messaging Apps in Iran's Information…', 30 November 2021
[54] Freedom House, 'Freedom on the Net 2021: Iran' (C5), 21 September 2021
[55] Atlantic Council, 'Iranian on #SocialMedia', 22 January 2022

- Enable remote access to the computer.'[56]

4.5.2 The CHRI added, 'Since CHRI first began investigating the cyberattacks in early 2018, at least 74 people in Iran, Europe and the United States have fallen victim to the spyware.'[57]

4.5.3 The USSD noted in its human rights report for 2020 that, 'In January, Certfa Lab reported a series of phishing attacks from an Iranian hacker group known as Charming Kitten, which was allegedly affiliated with Iran's intelligence services. According to the report, the phishing attacks targeted journalists as well as political and human rights activists.'[58]

4.5.4 The same report noted, 'In March [2020], Comparitech reported that data from 42 million Iranian Telegram accounts were leaked online. Telegram released a statement alleging the data came from the two unofficial Telegram apps Hotgram and Telegram Talaei, which became popular after the platform's ban in the country. There were reports the two client apps have ties to the government and Iranian hacker group Charming Kitten.'[59]

4.5.5 In February 2021, the cyber security firm, Check Point Research, reported on the use of malware, known as Domestic Kitten, linked to the Iranian government, to spy on its citizens[60]. The report stated:

'Starting in 2017, this operation, consisting of 10 unique campaigns, targeted over 1,200 individuals with more than 600 successful infections. It includes 4 currently active campaigns, the most recent of which began in November 2020. In these campaigns, victims are lured to install a malicious application by multiple vectors, including an Iranian blog site, Telegram channels, and even by SMS with a link to the malicious application.'[61]

4.5.6 Whilst the majority of Domestic Kitten victims were in Iran, Check Point Research also identified victims in the US, UK, Pakistan, Afghanistan, Turkey, and others[62].

See also Monitoring online activity abroad.

4.5.7 In June 2021, cybersecurity firm Kaspersky reported that it had uncovered a long-standing cyber-espionage campaign against Persian-speaking individuals in Iran. The report dubbed the malware 'Ferocious Kitten' and stated it had been active since 2015, adding that it, '… targets its victims with decoy documents containing malicious macros. These documents are disguised as images or videos that depict action against the Iranian regime (protests or footage from resistance camps). The initial messages within the decoy documents attempt to convince the target to enable the attached images or videos.'[63]

Back to Contents

[56] CHRI, 'Iranian State Malware Continues to Hack Online Accounts of Religious…', 20 May 2019
[57] CHRI, 'Iranian State Malware Continues to Hack Online Accounts of Religious…', 20 May 2019
[58] USSD, '2020 Country Reports on Human Rights Practices…' (section 1F), 30 March 2021
[59] USSD, '2020 Country Reports on Human Rights Practices…' (section 1F), 30 March 2021
[60] Check Point Research, 'Domestic Kitten – An Inside Look at the Iranian…', 8 February 2021
[61] Check Point Research, 'Domestic Kitten – An Inside Look at the Iranian…', 8 February 2021
[62] Check Point Research, 'Domestic Kitten – An Inside Look at the Iranian…', 8 February 2021
[63] Kaspersky, 'A 6-year cyberespionage campaign uncovered in the Middle East', 16 June 2021

4.6 Arrest, detention and convictions

4.6.1 Filterwatch reported that in October 2018, the head of FATA announced that nearly 75,000 people had been arrested for online activities in the previous eight years[64]. Referring to this announcement, the Freedom on the Net 2020 report noted, 'While some of those arrests may have been justified, many were for legitimate online activities, including criticism of the government.'[65]

4.6.2 In August 2019, the CHRI reported that, following investigations, it had found:

'… dozens of Iranians with large followings on Instagram – including athletes, fashion models and actors – were summoned by security officials in 2019 and in some cases charged with crimes for the content of their posts.

'Although most were ultimately released on bail, many were forced to hand over control of their Instagram accounts by revealing their passwords.

'Some of the targeted individuals, fearing jail time, ultimately suspended or severely limited their online posts as well as removed old posts that could be interpreted as "immoral" according to state dictates.'[66]

4.6.3 Referring to nationwide protests which took place in November 2019 against the hike in fuel prices, Amnesty International noted that many individuals were charged with 'criminal activity against nationality security' after undertaking peaceful activities including filming or sharing content of the protests including on social media and writing or sharing social media posts sympathetic to the protests or those who were killed[67].

4.6.4 The Atlantic Council January 2022 report on social media in Iran cited an email from the Human Rights Activists (HRA) in Iran group, who reported that between January 2017 and January 2021 at least 332 people were arrested for their online activities, 109 of whom were arrested for Instagram posts[68]. Referring to the arrests of Instagram users, a BBC News report dated January 2021 noted that the arrests followed a similar pattern and stated, 'Instagram personalities were harassed, arrested and prosecuted by Iranian authorities, which activists say pressured them to "confess" their alleged crimes, sometimes on state TV.'[69]

4.6.5 The HRA noted that the most common charges were for blasphemy (20.41%), followed jointly by insulting the Supreme Leader and colluding against national security (both 16.33%), and publishing vulgar content (14.29%)[70]. Insulting the authorities was the least common charge at 1%[71].

4.6.6 Reporting on events in 2020, Amnesty International stated:

'Cyber police established a special task force to tackle "cyber rumours" and "fake news" related to COVID-19 on social media; and scores of journalists,

[64] Filterwatch, 'Filterwatch/October 2018', 27 November 2018
[65] Freedom House, 'Freedom on the Net 2020: Iran' (C3), 14 October 2020
[66] CHRI, 'Iran Cracks Down on Instagram Celebrities…', 16 August 2019
[67] Amnesty International, 'Iran: Trampling Humanity – Mass arrests…' (page 25), 2 September 2020
[68] Atlantic Council, 'Iranian on #SocialMedia', 22 January 2022
[69] BBC News, 'The Instagrammers who worry Iran', 17 January 2021
[70] Atlantic Council, 'Iranian on #SocialMedia', 22 January 2022
[71] Atlantic Council, 'Iranian on #SocialMedia', 22 January 2022

social media users, health care workers and others were arrested, summoned for questioning or given warnings. In April, Rahim Yousefpour, a doctor from Saqqez, Kurdistan province, was charged with "spreading propaganda against the system" and "disturbing public opinion" for his Instagram posts about COVID-19.'[72]

4.6.7 Also reporting on the task force to combat online rumours, the USSD human rights report for 2020 noted, 'In April a military spokesman said authorities had arrested 3,600 individuals for spreading COVID-19 "rumors" online, with no clear guidance on what authorities considered a "rumor."'[73]

4.6.8 As noted in the Freedom on the Net 2021 report, 'The authorities routinely arrest and impose harsh sentences on journalists and social media users for their online activities. Those affected in recent years have included prominent activists, Instagram celebrities, editors at independent news outlets, and citizen journalists associated with persecuted religious groups like the Gonabadi dervishes and Baha'is.'[74]

4.6.9 The report added, 'Extralegal intimidation and violence by state authorities is common in Iran. Journalists, bloggers, and activists who are serving prison sentences due to their online activities frequently experience maltreatment and even torture while in detention.'[75] The report provided examples of harsh sentences, torture and mistreatment in detention and also added, 'Harassment and intimidation short of imprisonment is common.'[76]

4.6.10 Filterwatch's FATAwatch, a series of quarterly reports, first published in April 2019, sought to scrutinise the operations of Iran's Cyber Police (FATA). In its first edition, covering the period January to March 2019 and based solely on reports published by FATA, Filterwatch identified the charges brought against persons detained by FATA, which it classified into 3 main groups:

- 'Illegal Products & Services – These charges include the sale of goods such as weapons and drugs, as well as services including gambling or prostitution.
- 'Financial Crimes – These are mostly linked to phishing, online scams, and other types of fraud.
- 'Moral Crimes – These charges include stalking, spreading rumours, revenge porn, or other crimes involving the publication of content deemed immoral or illegal. Some of these crimes will have had financial motives, but FATA has instead presented them as moral crimes.'[77]

4.6.11 The then UK Foreign and Commonwealth Office (FCO) noted in its Human Rights and Democracy Report for 2019 that at least 15 journalists, bloggers, or social media activists were arrested[78]. In 2020, the renamed Foreign, Commonwealth and Development Office (FCDO) reported, 'At least 19

[72] Amnesty International, 'Iran 2020', 17 April 2021
[73] USSD, '2020 Country Reports on Human Rights Practices…' (section 2A), 30 March 2021
[74] Freedom House, 'Freedom on the Net 2021: Iran' (C3), 21 September 2021
[75] Freedom House, 'Freedom on the Net 2021: Iran' (C7), 21 September 2021
[76] Freedom House, 'Freedom on the Net 2021: Iran' (C7), 21 September 2021
[77] Filterwatch, 'FATAwatch/01 – Iranian Cyber Police Monitoring', 19 April 2019
[78] FCO, 'Human Rights and Democracy: the 2019 Foreign and Commonwealth…', 16 July 2020

journalists, writers and social media users were arrested, with a sudden increase in detentions during November and December.'[79]

4.6.12 Between January and September 2019, 497 arrests were recorded by FATA, 208 of which were related to moral crimes, according to Filterwatch[80]. Province-wise, most arrests occurred in Tehran (68), followed by Hormozgan (47), Razivi Khorasan (44), Esfanan (44), and Kurdistan (38)[81].

4.6.13 The report of the UN Secretary General published on 14 May 2021 noted that, 'Between 1 June 2020 and 31 January 2021, more than 57 individuals were arrested and detained for online activities and postings on Instagram, Telegram and other social media platforms, including on charges of "insulting the Prophet of Islam", "connection with opposition groups" and "insulting the police".'[82]

4.6.14 In its Yearbook 1399, covering events between March 2020 and March 2021, Filterwatch reported on arrests relating to coverage of the COVID-19 pandemic:

'According to an announcement by the FATA Chief for Fars Province, Colonel Heshmat Soleimani, at least 24 people were arrested in the province for "spreading rumours" about COVID-19. The Head of FATA Police also commented that 118 people were arrested for spreading rumours online. According to a senior spokesperson for Iran's Armed Forces, both the Basij and Police had arrested up to 3,600 people by April 29 for spreading "false information or rumours" online.'[83]

4.6.15 The same report noted arrests for other online activity, particularly in relation to reported that 'moral' violations, which often targeted women, 'On 20 May, FATA Deputy for Social Affairs Colonel Pashaei stated that "over 320 people were arrested" in relation to their online activities. He reiterated that not wearing a hijab online constitutes "inappropriate behaviour" and will be considered a crime.'[84]

4.6.16 FATAwatch quarterly reports cited numerous arrests for online activities, including for posting 'false information', 'immoral content' and 'anti-government activities'.

Back to Contents

Section 5 updated: 11 March 2022

5. Social media usage in Iran

5.1 Social media platforms

5.1.1 The Freedom House Freedom on the Net 2021 report noted:

'A number of social media and messaging platforms are blocked in Iran... The messaging app Signal was blocked in January 2021. Its website became inaccessible a few days prior to its blocking, and it was removed

[79] FCDO, 'Human Rights and Democracy: 2020 Foreign, Commonwealth and…', 8 July 2021
[80] Filterwatch, 'FATAwatch and the Judiciary Monitor', 18 March 2020
[81] Filterwatch, 'FATAwatch and the Judiciary Monitor', 18 March 2020
[82] UNHRC, 'Situation of human rights in the Islamic Republic of Iran…', 14 May 2021
[83] Filterwatch, 'Filterwatch Yearbook 1399 (March 2020 – March 2021)' (page 23), 11 June 2021
[84] Filterwatch, 'Filterwatch Yearbook 1399 (March 2020 – March 2021)' (page 24), 11 June 2021

from Iranian app stores in accordance with orders from the Committee to Determine Instances of Criminal Content (CDICC). Signal was previously blocked and unblocked in December 2017. Iranian officials did not explain or take responsibility for either incident. Signal has since added a transport layer security (TLS) proxy that can be set up as an "interim solution" in order to "bypass the network block."

'Twitter, Facebook, Telegram, and YouTube are all blocked or filtered, as are major blog-hosting platforms like Wix, WordPress, Blogspot, and Blogger. Conservative leaders have repeatedly exerted pressure on the CDICC – a government body headed by the prosecutor general that consists of representatives from 12 state institutions – to block other prominent social media platforms.'[85]

5.1.2 A 2015 report by Small Media, a London-based digital rights organisation, referred to Iran's 'copycat' social media platforms, which included Cloob.com and Facenama (both similar to Facebook), Aparat (similar to You Tube) and Lenzor (similar to Instagram), and listed the terms and conditions for using them[86].

5.1.3 The Atlantic Council January 2022 report on social media in Iran stated, 'To counter Telegram, Iran released its domestic version known as Soroush (and later other apps, including: Bale, Gap, iGap, and Rubika). The move prompted many privacy and security concerns, with some Iranians resorting to humor to highlight the Big Brother aspect of such apps.'[87]

5.1.4 Filterwatch also analysed 6 of the most popular domestic social media app 'alternatives' to Telegram, including Soroush, Gap, iGap, Bale, Bisphone and Wispi[88]. Filterwatch noted that the leading domestic messenger apps '… all have close ties with government entities.'[89]

5.1.5 Iran International reported in September 2021 that, 'The government has spent tens of millions of dollars to create domestic messaging apps to help reduce the use of foreign platforms it cannot control, but people weary of government eavesdropping have refused to migrate to its apps.'[90]

5.1.6 Some domestic social media platforms were accessible from outside Iran, according to Similarweb data, which analysed the geographic location of a site's core audience over the last month[91].

5.1.7 The Freedom on the Net 2021 report noted, 'Instagram and WhatsApp were among the few international platforms still available in Iran at the end of the coverage period [1 June 2020 to 31 May 2021]... In April 2021, the audio discussion app Clubhouse, which had quickly gained popularity among Iranian journalists, politicians, state elites, and activists, was blocked by the leading Iranian providers.'[92]

---

[85] Freedom House, 'Freedom on the Net 2021: Iran' (A3 and B1), 21 September 2021
[86] Small Media, 'IIIP/October 2015', 15 November 2015
[87] Atlantic Council, 'Iranian on #SocialMedia', 22 January 2022
[88] Small Media, 'Filterwatch/January 2018', 23 February 2018
[89] Filterwatch, 'The Role of Domestic Messaging Apps in Iran's Information…', 30 November 2021
[90] Iran International, 'Foreign Social Media Apps Remain Highly Popular In…', 18 September 2021
[91] Similarweb, (website), no date
[92] Freedom House, 'Freedom on the Net 2021: Iran' (B1), 21 September 2021

5.1.8 An article by Layla M. Hashemi, a researcher and data analyst at the Terrorism, Transnational Crime and Corruption Center (TraCCC), noted in an article dated 24 November 2021 on Iran's threats to block Instagram, that, 'Ironically, prominent Iranian officials are active users of the same services they condemn and disparage; former President Hassan Rouhani has over 2.2 million Instagram and Twitter followers and the Supreme Leader's account @khameini_ir has over 3.6 million followers.'[93]

Back to Contents

5.2 Number of users

5.2.1 According to DataReportal's Digital 2021 Report, Iran had 36 million active social media users as of January 2021, which had increased by 3 million between January 2020 and January 2021, equivalent to 42.6% of the country's total population[94]. The Statistical Center of Iran (SCI) reported on 18 September 2021 that 55 million people (65% of the population) in Iran used social media[95].

5.2.2 Citing the SCI statistics, Iran International, a privately-owned UK-based news site, stated that Telegram, the most popular messaging app in Iran even though it was blocked by the government, had 45 million registered users, with 15 billion messages sent via the app each day[96]. The report added that, '… Whatsapp and Instagram are also very popular with 88.5 and 68 percent of [social media] users respectively having accounts on these two platforms.'[97]

5.2.3 As of 6 September 2021, Iran's domestic social media platform Facenama received over 97,000 unique visitors a day[98] and, as of 31 January 2022, Aparat received nearly 33 million[99], according to data obtained on W3 Snoop, which provides reports on websites and domain names[100].

5.2.4 Filterwatch reported that, 'Etemaad Online estimates that fewer than 8 million Iranians use the top 5 domestic messaging applications, including Soroush and iGap.'[101] Filterwatch also noted:

'According to a poll by the Iranian Students Polling Agency (ISPA) on 31 August [2021], 48.4% of 1,570 respondents declared that they only use international social media and messaging platforms such as Telegram and Instagram while 27% of respondents stated that they did not use either domestic or international platforms. 22.8% of respondents stated they used both domestic and international platforms, however only 1.8% stated that they only use domestic platforms such as Soroush, Rubika, and Gap.'[102]

Back to Contents

[93] Hashemi L, 'Threats to Iranian Instagram: Analyzing Iran's Internet Landscape', 24 November 2021
[94] DataReportal, 'Digital 2021 – Iran', 11 February 2021
[95] Iran International, 'Foreign Social Media Apps Remain Highly Popular In…', 18 September 2021
[96] Iran International, 'Foreign Social Media Apps Remain Highly Popular In…', 18 September 2021
[97] Iran International, 'Foreign Social Media Apps Remain Highly Popular In …', 18 September 2021
[98] W3 Snoop, 'Facenama.com', 16 September 2021
[99] W3 Snoop, 'Aparat.com', 31 January 2022
[100] W3 Snoop, 'About', no date
[101] Filterwatch, 'Filterwatch Yearbook 1398 (March 2019 – March 2020)' (page 35), 10 June 2021
[102] Filterwatch, 'Policy Monitor – August 2021', 15 September 2021

6. Surveillance outside Iran

6.1 Targeting citizens abroad

6.1.1 In 2018 the Washington Institute for Near East Policy published a report by Senior Fellow, Mehdi Khalaji, on Iran's targeting of dissidents in Europe as well as the arrests of dual nationals. Khalaji cited past targets including the assassinations of the shah's former prime minister, Shapour Bakhtiar in Paris and several Kurdish opposition leaders in Berlin in the early 1990s, the killing of GEM TV owner Saeed Karimian and his Kuwaiti business partner in Istanbul in 2017, and in 2018 the assassination plot against an exiled leader of the Arab Struggle Movement for the Liberation of Ahvaz (ASMLA) in Denmark[103]. Dual Swedish national and former leader of ASMLA, Habib Chaab, went missing in Turkey in October 2020 after apparently being lured there by Iranian intelligence agents. He later appeared on Iranian state television and was charged with terrorism[104].

6.1.2 Indicating Iran's capacity for targeting its citizens abroad, Khalaji noted that, in the wake of mass protests launched by the Green Movement against the 2009 rigged presidential election, in November 2009, '… senior military official Gen. Masoud Jazayeri promised that Iran would "identify the dissidents, whether inside or outside the country, and crack down on them at the proper time," explicitly noting the potential for operations on foreign soil: "If the Islamic Republic sees it as inevitable, it can go after the coup supporters even beyond the border".'[105] Following an IRGC missile attack on the Iraqi headquarters of the Kurdistan Democratic Party-Iran (KDP-I) in September 2018, 'Gen. Yahya Rahim Safavi, the Supreme Leader's military advisor and former IRGC commander-in-chief, reiterated Jazayeri's 2009 threat about striking abroad: "If necessary, the IRGC will hunt and crack down on dissidents and enemies beyond borders and seas".'[106]

6.1.3 Noting Iran's strategies to carry out such operations, Khalaji stated:

'… the regime uses a wide network of intelligence organs. Beside the main Intelligence Ministry and the Qods Force, the IRGC special forces wing responsible for extraterritorial operations, the Supreme Leader directly supervises several agencies capable of taking action against dissidents, including intelligence bureaus within the IRGC, the police, the regular army, the judiciary, the office of the president, and the Interior Ministry. For instance, many Iranian dual nationals have been arrested by IRGC intelligence (e.g., British citizen Nazanin Zaghari-Ratcliffe, detained since 2016).'[107]

6.1.4 In his concluding comments Khalaji said, '… thousands of Iranians work abroad in academia, NGOs, Persian-language media, and other institutions. Iran's hardline regime casts the bulk of these citizens as major security threats and has shown signs of expanding its efforts to crack down on them

[103] Washington Institute, 'Iran Intensifying Its Crackdown on Citizens Abroad', 2 November 2018
[104] RFERL, 'Iranian-Swedish Former Leader Of Arab Separatist Group Goes…', 18 January 2022
[105] Washington Institute, 'Iran Intensifying Its Crackdown on Citizens Abroad', 2 November 2018
[106] Washington Institute, 'Iran Intensifying Its Crackdown on Citizens Abroad', 2 November 2018
[107] Washington Institute, 'Iran Intensifying Its Crackdown on Citizens Abroad', 2 November 2018

wherever they are – whether by conducting acts of terror on European soil, preventing dual nationals from entering Iran, or arresting those who hold European, Canadian, or American citizenship.'[108]

6.1.5 A 2020 report by the Swedish Security Service highlighted the threats to Sweden posed by Iran, noting:

'Iran is mainly involved in industrial espionage and intelligence activities targeting refugees.

'Iran's intelligence activities targeting refugees are mainly geared towards minority groups considered by the Iranian regime to pose a threat. The Iranian regime uses its intelligence services to carry out security-threatening activities in Sweden. This involves monitoring regime critics and targets in Sweden linked to opposition groups considered by Iran as being or potentially being destabilising or potentially destabilising to the regime.

'The primary goal of the Iranian regime is to secure its own survival by countering internal and external threats wherever identified, including in Sweden. Exiled opposition groups are considered an internal threat located outside the country's borders. Such groups and individuals exist in Sweden.'[109]

6.1.6 BBC News reported on 16 July 2020 on an announcement made by Iran's judiciary in June 2020 that '… Ruhollah Zam, a dissident journalist and founder of the influential Telegram account AmadNews, had been sentenced to death for "spreading corruption on earth". One of the accusations he faced was encouraging people to participate in anti-government protests in 2017 and 2018. Zam was based in Paris, but he was lured to Iraq by the Iranian Revolutionary Guards' intelligence service and then kidnapped and taken back to Iran.'[110]

6.1.7 Following what Amnesty International described as a 'grossly unfair trial' by Branch 15 of the Revolutionary Court in Tehran, Zam's sentence was upheld by the Supreme Court on 8 December 2020 and he was executed on 12 December 2020[111].

6.1.8 A September 2020 article in The Iran Primer published a timeline of Iran's assassinations and plots, noting that since the 1979 revolution to September 2020, Iran '… had reportedly assassinated at least 21 opponents abroad and killed hundreds in bombings of foreign military, diplomatic, and cultural facilities.' According to the report, during period there were 59 'attacks or plots', including 20 that 'targeted Iranian dissidents.'[112]

6.1.9 A special report by Freedom House dated February 2021 noted:

'The Iranian regime's expansive definition of who constitutes a threat to the Islamic Republic contributes to the breadth and intensity of its transnational repression campaign. The authorities frequently label the targeted dissidents and journalists as terrorists, using the term as a blanket justification for

[108] Washington Institute, 'Iran Intensifying Its Crackdown on Citizens Abroad', 2 November 2018
[109] Swedish Security Service, 'Yearbook 2020' (page 25), 2020
[110] BBC News, 'Iran judiciary may halt protesters' executions after social media storm', 16 July 2020
[111] Amnesty International, 'Iran: Execution of journalist Rouhollah Zam…'12 December 2020
[112] The Iran Primer, 'Timeline: Iran's Assassinations and Plots', 16 September 2020

violence and disregard for due process. The campaign incorporates the full spectrum of transnational repression tactics, including assassinations, renditions, detentions, unlawful deportations, Interpol abuse, digital intimidation, spyware, coercion by proxy, and mobility controls. These tools have been deployed against Iranians in at least nine countries in Europe, the Middle East, and North America.

'The Iranian campaign is distinguished by the total commitment it receives from the state, the level of violence that it employs, and its sophisticated application of diverse methods against a similarly diverse set of targets. The result is intense intimidation of the Iranian diaspora, from which even those who avoid physical consequences ultimately suffer. As an Iranian activist told Freedom House, "They drain you emotionally, financially, in every way."'[113]

6.1.10 In February 2021, a query response by the Research Directorate of the Immigration Refugee Board of Canada (IRB) referred to overseas monitoring capabilities of Iran and cited a telephone interview with an Assistant Professor of political science at the University of Tennessee at Chattanooga, who studies authoritarian regimes with a focus on the Middle East and North Africa and has written about Iran, who '… indicated that Iranian authorities "focus on political opponents abroad" and that there have been cases of activists being kidnapped and returned to Iran (Assistant Professor 23 Jan. 2021). The same source noted that the authorities "will try to kidnap" "high-ranking activists" (Assistant Professor 23 Jan. 2021).'

Back to Contents

6.2 Monitoring citizens abroad

6.2.1 The February 2021 IRB query response also cited a telephone interview with a retired professor at York University, who has published books and articles in English and Persian on the leftist movement in Iran, religious fundamentalism, secularism, multiculturalism and the diaspora:

'When asked whether Iran monitors overseas anti-government activities, the retired Professor responded that Iran's government "sends people as agents to other countries" (Retired Professor 25 Jan. 2021). The Assistant Professor [of political science at the University of Tennessee] indicated that the government "will try to find [anti-government activists] inside and outside of the country" and that the intelligence agency will help gather information (Assistant Professor 23 Jan. 2021). The same source noted that Iran uses refugees to monitor other refugees outside of the country (Assistant Professor 23 Jan. 2021).'[114]

6.2.2 The IRB went on to cite a 2019 article by the Associated Press, which noted, '… in December 2019 an Iraqi man was charged with spying and was sentenced to two and a half years in prison for collecting information about Iranian refugees in Sweden, Denmark, Belgium, and the Netherlands…'[115]

6.2.3 The IRB response continued:

[113] Freedom House, 'Iran Case Study | Understanding Transnational Repression', February 2021
[114] IRB, 'Iran: Treatment by the authorities of anti-government activists…', 22 February 2021
[115] IRB, 'Iran: Treatment by the authorities of anti-government activists…', 22 February 2021

'The Assistant Professor also noted that Iran's government monitors political opponents abroad to find out about their activities (Assistant Professor 23 Jan. 2021). The same source noted that the authorities "usually focus on important people, but they are interested in any information that they can use to put pressure on people," such as information about a person's consumption of alcohol or romantic relationships (Assistant Professor 23 Jan. 2021). The retired Professor indicated that Iran's government spies on the opposition and Iranians abroad (Retired Professor 25 Jan. 2021). The same source stated that Iranian authorities "will threaten people" to induce them to cease their activities abroad and that Iran's government has "tried to" assassinate Iranians abroad (Retired Professor 25 Jan. 2021).'[116]

See also Targeting citizens abroad.

Back to Contents

6.3 Sur place activity

6.3.1 Whilst numerous demonstrations occurred in the UK against the Iranian government, as well as for Kurdish rights, the extent to which the Iranian authorities monitored such events was unclear. Some examples of protests held in London are provided below.

6.3.2 In March 2018, 4 people were arrested by police after climbing to a first-floor balcony of the Iranian Embassy, London, in an apparent protest against the Iranian government[117] [118].

6.3.3 The Evening Standard reported on a demonstration outside the Iranian Embassy, London, in September 2018, led by Kurdish protesters following missile attacks on KDPI offices in the KRI and the execution of 3 Kurdish prisoners[119]. A short film of the protest was tweeted by Mutlu Civiroglu, described as a Kurdish Affairs Analyst. The tweet had been viewed just over 3,500 times[120]. According to the Evening Standard, 3 arrests were made by police after disorder broke out at the protest[121].

6.3.4 On 9 May 2019, the 9th anniversary of the execution of Kurdish activists in Iran, 'Britain's Kurds led by PJAK [Kurdistan Free Life Party] movement in the United Kingdom participated in a protest in front of the Iranian embassy in London to condemn the hanging execution of Kurdish activists', where the protesters '… chanted the slogans in Kurdish and English and condemned the Iranian policies against political and social activists', reported Rojhelat.info, a site which reported on news in Iranian Kurdistan and Kurdish human rights[122].

6.3.5 Arab News, a daily English language newspaper, published in Saudi Arabia, reported on 30 July 2019, 'Thousands of exiled Iranian dissidents rallied in Trafalgar Square in London on [27 July 2019] to demand regime change in Tehran… The event organized by the National Council of Resistance of Iran

[116] IRB, 'Iran: Treatment by the authorities of anti-government activists…', 22 February 2021
[117] Reuters, 'Four arrested after balcony protest at Iranian embassy in London', 9 March 2018
[118] Arab News, 'Protesters held after scaling Iran embassy in London: police', 10 March 2018
[119] Evening Standard, 'Three arrests after disorder breaks out during Iranian…', 10 September 2018
[120] Mutlu Civiroglu @mutludc, 'Kurds in London, UK protest outside the…', 10 September 2018
[121] Evening Standard, 'Three arrests after disorder breaks out during Iranian…', 10 September 2018
[122] Rojhelat.info, 'Kurds in Britain condemned the Iranian Regime on the anniversary…', 12 May 2019

came amid tension between London and Tehran over the seizure of a British oil tanker in the Strait of Hormuz.'[123]

6.3.6 Middle East Monitor (MEMO), a London based media monitoring organisation, published a photo of demonstrators outside the Iranian Embassy in London as they protested against the execution of Iranian wrestler, Navid Afkari, on 12 September 2020[124].

6.3.7 In March 2021, the family members of Nazanin Zaghari-Ratcliffe (a dual British- Iranian national) protested outside the Iranian Embassy in London, alongside Amnesty International UK officials, demanding her release from Iran, where she was arrested and imprisoned for spying in 2016. Nazanin's husband, Richard Ratcliffe, attempted to deliver a 160,000 signature petition to the authorities but officials refused to meet him[125] [126].

6.3.8 On 10 October 2021 protests took place in central London demanding the release of Kurdistan Workers Party (PKK) leader Abdullah Ocalan[127].

6.3.9 See also Search | Amnesty International UK and Search Results London — Rojhelat.info for other examples of protests held in London and/or outside the Iranian Embassy.

Back to Contents

6.4 Monitoring online activity abroad

6.4.1 In regard to surveying foreign social media platforms compared to those hosted in Iran, the Freedom on the Net 2021 report said:

'It remains unclear how thoroughly Iranian authorities can monitor the content of messages on foreign social media platforms, 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 platforms do not guarantee the kind of user protection offered by some of their international counterparts, which may explain their lack of popularity.'[128]

6.4.2 The same source also reported:

'In 2020, the South African telecommunications company MTN released its first transparency report, indicating that in 2019 it had received 77,109 requests for location data and numbers identifying specific mobile devices, 77,400 data requests pursuant to criminal investigations, and 69,730 data requests pursuant to service suspension or restriction orders from Iran's judiciary – some of the highest figures for any country covered in the report. MTN has been operating in Iran since 2006 in a joint venture with Irancell, and has about 46.8 million subscribers in the country.'[129]

6.4.3 Facebook produced transparency reports showing the number of government requests for user data. Between January 2017 and June 2021,

[123] Arab News, 'Iranian exiles rally in London to demand regime change in Tehran', 30 July 2019
[124] MEMO, 'Iranian wrestler executed despite international outcry', 13 September 2020
[125] The National, 'Family of Nazanin Zaghari-Ratcliffe protest outside Iranian…', 8 March 2021
[126] Independent, 'Nazanin Zaghari-Ratcliffe's husband and daughter protest…', 8 March 2021
[127] Rojhelat.info, 'Today In London! The Activity With The Slogan…', 10 October 2021
[128] Freedom House, 'Freedom on the Net 2021: Iran' (C6), 21 September 2021
[129] Freedom House, 'Freedom on the Net 2021: Iran' (C6), 21 September 2021

Facebook received a total of 18 requests from the Iranian authorities, relating to 29 users/accounts. Facebook noted 'Each and every request we receive is carefully reviewed for legal sufficiency and we may reject or require greater specificity on requests that appear overly broad or vague.'[130] The report also cited the percentage of requests where Facebook produced some data. No detail on the nature of requests or data produced was provided[131].

6.4.4 Freedom on the Net 2021 also indicated, 'State hackers often launch cyberattacks against activists and campaigners, including those in the diaspora. Due to growing tensions among the governments of Iran, neighboring countries, and the United States, there has been a notable rise in reported hacking campaigns and cyberattacks affecting Iranians.'[132]

6.4.5 The report cited examples of cyberattacks, including 'In February 2021, it was reported that the security company Bitdefender and the radio program Argos had identified a server in a Dutch data center that was being used by the Iranian regime to "spy on political opponents" in countries such as Germany, the Netherlands, India, and Sweden. The server was said to have been a command-and-control unit that could be used to steal and manipulate data from computers infected with malware.'[133]

6.4.6 The IRB response dated February 2021 noted, 'The Assistant Professor stated that the authorities will "hack" for information on a "mid-rank" activist and will monitor "an ordinary Iranian," "because any information is useful" (Assistant Professor 23 Jan. 2021).'[134]

6.4.7 On 18 November 2021, IranWire reported on death threats received by Iranian human rights activists on their social media feeds, citing Twitter and Instagram. The report added:

'At a protest in Whitehall, London last week, they [the activists] were photographed and filmed extensively as they held up placards calling for an end to impunity in the Islamic Republic. The activists knew well what the pictures could mean for them.

"I am one of the victims," says Shadi Amin, co-founder of Justice for Iran, whose supporters were also present at the protest. "We live with the threats and with the fake news they spread about us [inside Iran] They make threats against our families in Iran.'[135]

Back to Contents

[130] Meta (Facebook), 'Government requests for user data – Iran', January 2017 to June 2021
[131] Meta (Facebook), 'Government requests for user data – Iran', January 2017 to June 2021
[132] Freedom House, 'Freedom on the Net 2021: Iran' (C8), 21 September 2021
[133] Freedom House, 'Freedom on the Net 2021: Iran' (C8), 21 September 2021
[134] IRB, 'Iran: Treatment by the authorities of anti-government activists…', 22 February 2021
[135] IranWire, 'Transnational Repression: How Iran Haunts and Kills its Critics…', 18 November 2021

Terms of Reference

A 'Terms of Reference' (ToR) is a broad outline of what the CPIN seeks to cover. They form the basis for the country information section. The Home Office's Country Policy and Information Team uses some standardised ToR, depending on the subject, and these are then adapted depending on the country concerned.

For this particular CPIN, the following topics were identified prior to drafting as relevant and on which research was undertaken:

- Legal context
- Access to social media in Iran
    - Number of users
    - Social media platforms
- Cyber surveillance
    - Cyber police
    - Control and monitoring of online activity
    - Arrest and detentions
- Surveillance outside Iran
    - Targeting citizens abroad
    - Monitoring online activity abroad
    - Monitoring citizens abroad and sur place activity

Back to Contents

Bibliography

Sources cited

Al Jazeera, 'Iran: Controversial internet control bill passes committee stage', 22 February 2022. Last accessed: 11 March 2022

Al Monitor, 'Iran pushes ahead with internet "protection" bill', 23 February 2022. Last accessed: 11 March 2022

Amnesty International,

'Iran: Execution of journalist Rouhollah Zam a "deadly blow" to freedom of expression', 12 December 2020. Last accessed: 10 February 2022

'Iran: Trampling Humanity – Mass arrests, disappearances and torture since Iran's 2019 November protests', 2 September 2020. Last accessed: 14 February 2022

'Report 2020/21, The State of the World's Human Rights, Iran 2020', 17 April 2020. Last accessed: 10 February 2022

Arab News,

'Iranian exiles rally in London to demand regime change in Tehran', 30 July 2019. Last accessed: 14 February 2022

'Protesters held after scaling Iran embassy in London: police', 10 March 2018. Last accessed: 14 February 2022

Article 19,

'Iran: Tightening the Net 2020, After Blood and Shutdowns', September 2020. Last accessed: 3 February 2022

'Islamic Republic of Iran: Computer Crimes Law', 5 April 2012. Last accessed: 3 February 2022

'Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran', 3 February 2017. Last accessed: 4 February 2022

Atlantic Council, 'Iranian on #SocialMedia', 22 January 2022. Last accessed: 3 February 2022

Australian Government, Department of Foreign Affairs and Trade (DFAT), 'Country Information Report Iran', 14 April 2020. Last accessed: 10 February 2022

BBC News,

'The Instagrammers who worry Iran', 17 January 2021. Last accessed: 15 February 2022

'Iran judiciary may halt protesters' executions after social media storm', 16 July 2020. Last accessed: 10 February 2022

Carnegie Endowment for International Peace (CEIP), 'Iran's Cyber Threat: Espionage, Sabotage, and Revenge', 4 January 2018. Last accessed: 14 February 2022

Center for Human Rights in Iran (CHRI),

'Iran Cracks Down on Instagram Celebrities as It Tightens Noose on Freedom of Speech and Expression', 16 August 2019. Last accessed: 10 February 2022

'Iranian State Malware Continues to Hack Online Accounts of Religious Minority Groups', 20 May 2019. Last accessed: 7 February 2022

'Iranians Looking Abroad to Escape State-Controlled Internet', 14 March 2016. Last accessed: 14 February 2022

Check Point Research, 'Domestic Kitten – An Inside Look at the Iranian Surveillance Operations', 8 February 2021. Last accessed: 7 February 2022

Committee to Protect Journalists (CPJ), 'Iran's parliament moves forward with troubling bill to further restrict internet', 1 November 2021. Last accessed: 3 February 2022

Danish Immigration Service,

'Iran: November 2019 Protests', July 2020. Last accessed: 14 February 2022

'Iranian Kurds: Consequences of political activities in Iran and KRIs', February 2020. Last accessed: 10 February 2022

DataReportal, 'Digital 2021 – Iran', 11 February 2021. Last accessed: 27 January 2022

Evening Standard, 'Three arrests after disorder breaks out during Iranian Embassy protest', 10 September 2018. Last accessed: 14 February 2022

Filterwatch,

'FATAwatch/01 – Iranian Cyber Police Monitoring', 19 April 2019. Last accessed: 7 February 2022

'FATAwatch and the Judiciary Monitor', 18 March 2020. Last accessed: 7 February 2022

'Filterwatch/October 2018', 27 November 2018. Last accessed: 14 February 2022

'Filterwatch Yearbook 1398 (March 2019 – March 2020)', 10 June 2021. Last accessed: 7 February 2022

'Filterwatch Yearbook 1399 (March 2020 – March 2021)', 11 June 2021. Last accessed: 7 February 2022

'Policy Monitor – August 2021', 15 September 2021. Last accessed: 7 February 2022

'The Role of Domestic Messaging Apps in Iran's Information Controls', 30 November 2021. Last accessed: 7 February 2022

Foreign and Commonwealth Office (FCO), 'Human Rights and Democracy: the 2019 Foreign and Commonwealth Office report', 16 July 2020. Last accessed: 10 February 2022

Foreign, Commonwealth and Development Office (FCDO), 'Human Rights and Democracy: 2020 Foreign, Commonwealth and Development Office report', 8 July 2021. Last accessed: 10 February 2022

Freedom House,

‘Freedom on the Net 2020: Iran’, 14 October 2020. Last accessed: 14 February 2022

‘Freedom on the Net 2021: Iran’, 21 September 2021. Last accessed: 27 January 2022

Hashemi L, ‘Threats to Iranian Instagram: Analyzing Iran’s Internet Landscape’, 24 November 2021. Last accessed: 31 January 2022

Immigration and Refugee Board of Canada (IRB), ‘Iran: Treatment by the authorities of anti-government activists, including those returning from abroad; overseas monitoring capabilities of the government (2019–February 2021) [IRN200457.E]’, 22 February 2021. Last accessed: 11 February 2022

Independent, ‘Nazanin Zaghari-Ratcliffe’s husband and daughter protest outside Iranian embassy as case reaches “endgame”’, 8 March 2021. Last accessed: 14 February 2022

Iran International, ‘Foreign Social Media Apps Remain Highly Popular In Iran Despite Blocking’, 18 September 2021. Last accessed: 27 January 2022

The Iran Primer,

‘New “Protection” Bill on Internet Freedom’, 14 October 2021. Last accessed: 4 February 2022

‘Timeline: Iran's Assassinations and Plots’, 16 September 2020, updated 21 September 2020. Last accessed: 11 February 2022

IranWire,

‘About us’, no date. Last accessed: 2 February 2022

‘Iranians Furious at Identity Theft by IRGC's Instagram Ripoff’, 16 August 2021. Last accessed: 4 February 2022

‘Police crackdown on live Instagrams’, 26 June 2020. Last accessed: 11 February 2022

‘Transnational Repression: How Iran Haunts and Kills its Critics Around the World’, 18 November 2021. Last accessed: 7 February 2022

Kaspersky, ‘A 6-year cyberespionage campaign uncovered in the Middle East’, 16 June 2021. Last accessed: 10 February 2022

Landinfo – Norwegian Country of Origin Information Centre, CGRS-CEDOCA – Office of the Commissioner General for Refugees and Stateless Persons (Belgium), COI unit, SEM – State Secretariat for Migration, ‘Iran; Criminal procedures and documents’, December 2021. Last accessed: 27 January 2022

Meta (Facebook), ‘Government requests for user data – Iran’, January 2017 to June 2021. Last accessed: 4 February 2022

Middle East Monitor (MEMO), ‘Iranian wrestler executed despite international outcry’, 13 September 2020. Last accessed: 14 February 2022

Mutlu Civiroglu @mutludc, ‘Kurds in London, UK protest outside the Iranian embassy against the execution of 3 Kurdish political prisoners and missle attacks against

KDPI offices in Iraqi Kurdistan region @Hevallo', 10 September 2018. Last accessed: 14 February 2022

The National, 'Family of Nazanin Zaghari-Ratcliffe protest outside Iranian embassy in London', 8 March 2021. Last accessed: 14 February 2022

The Organization for World Peace (OWP), 'Iran's "Protection Bill" To Enhance Internet Clampdown', 6 March 2022. Last accessed: 11 March 2022

Radio Free Europe/Radio Liberty (RFERL), 'Iranian-Swedish Former Leader Of Arab Separatist Group Goes On Trial In Iran', 18 January 2022. Last accessed: 11 February 2022

Reuters, 'Four arrested after balcony protest at Iranian embassy in London', 9 March 2018. Last accessed: 14 February 2022

Rojhelat.info,

'Kurds in Britain condemned the Iranian Regime on the anniversary of the execution of political activists', 12 May 2019. Last accessed: 14 February 2022

'Today In London! The Activity With The Slogan "The Time Is The Freedom Time For Ocalan!" Has Been Performed In London!', 10 October 2021. Last accessed: 14 February 2022

Sharing Electronic Resources and Laws on Crime (SHERLOC), UN Office on Drugs and Crime (UNODC), 'Iran Computer Crimes Act', no date. Last accessed: 14 February 2022

Similarweb, (website), no date. Last accessed: 31 January 2022

Small Media,

'Filterwatch/January 2018', 23 February 2018. Last accessed: 7 February 2022

'IIIP/October 2015', 15 November 2015. Last accessed: 7 February 2022

Swedish Security Service, 'Yearbook 2020', 2020. Last accessed: 2 February 2022

UN Human Rights Council (UNHRC), 'Situation of human rights in the Islamic Republic of Iran; Report of the Secretary-General [A/HRC/47/22]', 14 May 2021. Last accessed: 14 February 2022

US Department of State (USSD), '2020 Country Reports on Human Rights Practices: Islamic Republic of Iran', 30 March 2021. Last accessed: 11 February 2022

W3 Snoop,

'About', no date. Last accessed: 31 January 2022

'Aparat.com', 31 January 2022. Last accessed: 31 January 2022

'Facenama.com', 16 September 2021. Last accessed: 31 January 2022

Washington Institute for Near East Policy, 'Iran Intensifying Its Crackdown on Citizens Abroad', 2 November 2018. Last accessed: 10 February 2022

Back to Contents

Sources consulted but not cited

Article 19,

> 'Computer Crimes in Iran: Risky Online Behaviour', 2 July 2015. Last accessed: 4 February 2022
>
> 'Tightening the net: Online openings and closings in Iran', 11 December 2017. Last accessed: 4 February 2022Last accessed: 4 February 2022

The Begin-Sadat Center for Strategic Studies, 'The Ever-Growing Iranian Cyber Threat', 26 September 2021. Last accessed: 10 February 2022

Center for Human Rights in Iran (CHRI), 'Iranian State Hackers Launched Attacks on Same Day Supreme Leader Issued Fatwa Forbidding Privacy Violations', 11 April 2018. Last accessed: 4 February 2022

Facebook, Facebook Help Center, no date. Last accessed: 4 February 2022

Guarnieri C and Anderson C, 'Iran and the Soft War for Internet Dominance', August 2016. Last accessed: 4 February 2022

Human Rights Watch, 'Iran: Targeting of Dual Citizens, Foreigners', 26 September 2018. Last accessed: 11 February 2022

IranWire, '"What Else Can they Do?": Rage and Resignation in Iran Over Internet Filtering Bill', 29 July 2021. Last accessed: 4 February 2022

Iran Threats, 'Fictitious Profiles and Webrtc's Privacy Leaks used to Identify Iranian Activists', 11 November 2016. Last accessed: 4 February 2022

Security Boulevard, Demboski M, 'Analysis of the Iranian cyber attack landscape', 29 April 2021. Last accessed: 10 February 2022

Techwalla, 'How to Retrieve a Deleted Facebook Account', 16 October 2020. Last accessed: 4 February 2022

US Department of State, 'Sanctioning Iranian Intelligence Affiliates for Targeting Dissidents Abroad', 3 September 2021. Last accessed: 11 February 2022

Back to Contents

Version control

Clearance

Below is information on when this note was cleared:

- version **1.0**
- valid from **March 2022**

Official – sensitive: Start of section

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: End of section

Changes from last version of this note

First version of CPIN to reflect the country guidance case XX (PJAK – sur place activities - Facebook) Iran CG [2022] UKUT 23 (IAC).

Back to Contents