Iran: Überwachung der sozialen Medien im Ausland

Themenpapier der SFH-Länderanalyse

Bern, 25. November 2023

Weyermannsstrasse 10
Postfach, CH-3001 Bern
T +41 31 370 75 75
F +41 31 370 75 00
info@fluechtlingshilfe.ch
www.fluechtlingshilfe.ch
Spendenkonto
PC 30-1085-7

Impressum

Herausgeberin
Schweizerische Flüchtlingshilfe (SFH)
Postfach, 3001 Bern
Tel. 031 370 75 75
Fax 031 370 75 00
E-Mail: info@fluechtlingshilfe.ch
Internet: www.fluechtlingshilfe.ch
Spendenkonto: PC 30-1085-7

Sprachversionen
Deutsch, Französisch

Inhaltsverzeichnis

Dieser Bericht basiert auf Auskünften von Expertinnen und Experten und auf eigenen Recherchen. Entsprechend den COI-Standards verwendet die SFH öffentlich zugängliche Quellen. Lassen sich im zeitlich begrenzten Rahmen der Recherche keine Informationen finden, werden Expertinnen und Experten beigezogen. Die SFH dokumentiert ihre Quellen transparent und nachvollziehbar. Aus Gründen des Quellenschutzes können Kontaktpersonen anonymisiert werden.

1 Einleitung

Einer Anfrage an die SFH-Länderanalyse sind die folgenden Fragen entnommen:

1. Werden (immer/regelmässig/im Einzelfall) Äusserungen iranischer Staatsangehöriger in sozialen Medien (Facebook, Instagram, Twitter, Telegram, etc.) überwacht?

2. Gibt es Erkenntnisse, ob für eventuelle staatliche Repressionsmassnahmen unterschieden wird,

    a. Welche Reichweite die Äusserung/Aktivität hat (z.B. wie viele Personen haben dies unmittelbar gesehen/gehört, erfolgte die Äusserung/Aktivität in einem öffentlichen Medium, wie viele Follower*innen nehmen die Aktivität in den sozialen Netzwerken wahr)?
    b. Ob es sich um eigene Äusserungen handelt oder z.B. in sozialen Netzwerken lediglich Äusserungen/Inhalte/Karikaturen Dritter geteilt oder weitergegeben werden?

Die Schweizerische Flüchtlingshilfe (SFH) beobachtet die Entwicklungen in Iran seit mehreren Jahren.[1] Aufgrund von Auskünften von Expert*innen und eigenen Recherchen nimmt die SFH zu den Fragen wie folgt Stellung:

2 Überwachung der sozialen Medien

Iran hat fortschrittliche Überwachungstechnologien aus anderen Staaten erworben. Iran hat nach Angaben von *Freedom House* Überwachungstechnologie von anderen autoritären Regierungen, darunter China und Russland, erworben. Im März 2023 berichtete das *Wall Street Journal*, dass die russische Regierung Iran Technologie verkauft hat, die Software zur «Kommunikationsüberwachung» umfasst.[2]

Massive Überwachung der Aktivitäten in sozialen Medien in Iran. Die Online-Sphäre in Iran wird nach Angaben von *Freedom House* vom iranischen Staat stark überwacht. Untersuchungen, die im Jahr 2022 von Intercept und Citizen Lab veröffentlicht wurden, ergaben, dass die Regierungsbehörden in der Lage sind, massenhaft Mobiltelefondaten von Nutzer*innen zu Überwachungszwecken abzufangen, zu speichern und zu analysieren. Der iranische Staat überwacht soziale Medien auf Aktivitäten, die er für illegal hält. *Deep Packet Inspection Tools*[3] ermöglichen es den Behörden, Online-Inhalte zu filtern und gleichzeitig den Browserverlauf und die Kommunikation zu analysieren. In der Vergangenheit hatten Behördenvertretende

1 https://www.fluechtlingshilfe.ch/publikationen/herkunftslaenderberichte.
2 Freedom House, Freedom on the Net 2023 - Iran, 4. Oktober 2023: https://freedomhouse.org/country/iran/freedom-net/2023.
3 Bei Deep Packet Inspection handelt es sich um eine fortschrittliche Methode zur Analyse, Überwachung, Filterung und Markierung der in einem Netzwerk übertragenen Datenpakete. In einigen Staaten wird DPI genutzt, um den Internetverkehr der Bürger*innen zu überwachen oder Inhalte zu zensieren. Security Insider, Was ist Deep Packet Inspection (DPI)? 23. Juni 2021: https://www.security-insider.de/was-ist-deep-packet-inspection-dpi-a-1052442/.

laut *Freedom House* zugegeben, die Online-Posts von Aktivist*innen und Demonstrant*innen zu überwachen.[4]

Überwachung von inländischen Anwendungen für soziale Medien und Kommunikation. In den letzten Jahren haben die Behörden gemäss *Freedom House* inländische Anwendungen für soziale Medien und Kommunikation gefördert, denen Verbindungen zu den iranischen Geheimdiensten nachgesagt wurden.[5] Verschiedene Quellen gehen davon aus, dass die Nutzung der inländischen Messaging-Apps die Überwachung durch die Behörden ermöglicht.[6] Im März 2022 kündigte der ICT-Minister an, dass es den Sicherheitskräften erlaubt sein soll, mit einem Durchsuchungsbefehl auf die Nutzer*innendaten dieser Apps zuzugreifen. Laut dem *Magazin New Lines* haben die Manager von Rubika, einer der inländischen Messaging-Apps im Iran, behauptet, dass sie künstliche Intelligenz (KI) einsetzen, um Inhalte, die als «unmoralisch» angesehen werden, zu identifizieren und aus der App zu entfernen.[7] Wenn Diaspora-Mitglieder diese iranischen Apps verwenden, sind sie für die Behörden laut *Kontaktperson H*[8] «einfache Ziele» und werden überwacht.[9]

Keine «harten Beweise» für automatisierte Massenüberwachung. Überwachung sozialer Medien besteht oft darin, dass versucht wird, Menschen auf verschiedene Weise ihre Passwörter zu entlocken, Aktivitäten in offenen sozialen Medien zu überwachen und gefälschte Konten in Gruppen im Internet und in sozialen Medien zu erstellen. Laut *Kontaktperson I*[10] ist nicht klar, ob die iranischen Behörden eine automatisierte Massenüberwachung der sozialen Medien durchführen können. Sie geht davon aus, dass sehr viel in der Masse überwacht werde. Dadurch erhöhe sich das Gefühl von Willkür und Unberechenbarkeit.[11] In gewisser Weise sei die digitale Überwachung nach Einschätzung von *Kontaktperson H* systematisch, aber nicht vergleichbar mit dem Vorgehen in Russland und China. *Kontaktperson H* wies darauf hin, dass die iranischen Behörden russische Überwachungstechnologie erhalten haben. Es sei offensichtlich, dass die Behörden Daten sammeln, aber es gebe keine «harten Beweise» für den Einsatz solcher Technologie für eine automatisierte Massenüberwachung.[12] *Kontaktperson G*[13] wies darauf hin, dass die iranischen Behörden nicht alle Nutzer*innen in sozialen Medien überwachen könnten, da dies enorme Ressourcen benötige.[14] *Article 19* gab im November 2019 an, dass die iranischen Geheimdienste versuchen, den Eindruck zu erwecken, das Internet und die sozialen Medien auf raffinierte Weise überwachen zu können. In der Praxis bestehe die Überwachung sozialer Medien oft darin, dass versucht wird, Menschen auf verschiedene Weise ihre Passwörter zu entlocken, Aktivitäten in offenen

4 Freedom House, Freedom on the Net 2023 - Iran, 4. Oktober 2023.
5 Ebenda.
6 Ebenda; Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
7 Freedom House, Freedom on the Net 2023 - Iran, 4. Oktober 2023.
8 Kontaktperson H ist eine auf den Iran spezialisierte Expertenperson für Cybersicherheit.
9 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
10 Kontaktperson I verfügt über Expertenwissen zu transnationaler Unterdrückung und digitaler Überwachung des iranischen Staats.
11 Telefon-Interview vom 15. September 2023 mit Kontaktperson I.
12 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
13 Kontaktperson G ist eine ausgewiesene Expertenperson für iranische Internetzensur, Cyberangriffe und digitale Sicherheit.
14 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.

sozialen Medien zu überwachen und gefälschte Konten in Gruppen im Internet und in sozialen Medien zu erstellen.[15]

Nachrichtendienstlichen Fähigkeiten des Irans beruhen auf grosser Zahl von Personen, die für sie Informationen über Online-Aktivitäten sammeln. Der *US-Organisation Atlantic Council* zufolge beruhen die nachrichtendienstlichen Fähigkeiten des Irans nicht in erster Linie auf fortschrittlicher Technologie, sondern auf der grossen Anzahl von Personen, die für sie arbeiten und Informationen über das, was sie online sehen, weitergeben.[16] *Kontaktperson H* wies darauf hin, dass die iranischen Nachrichtendienste aktuell viele Zudienende hätten, welche für sie Informationen sammeln.[17] Auch *Kontaktperson I* wies darauf hin, dass aus Äusserungen von iranischen Regierungsvertretenden zu schliessen sei, dass es genügend Personal gäbe, um umfassend Informationen zu sammeln und auf regierungskritische Posts in sozialen Medien zu reagieren. Wie koordiniert das gemacht und geheimdienstlich ausgewertet werde, sei laut *Kontaktperson I* schwer abzuschätzen.[18]

Es wurde dokumentiert, dass die iranischen Sicherheitsbehörden spezifische Themen in den sozialen Medien systematisch und umfassend analysierten. *Kontaktperson G* wies darauf hin, dass die iranischen Sicherheitsdienste ein spezielles Team einstellen können, wenn sie an einem bestimmten Thema in den sozialen Medien interessiert sind. Dieses Team würde das Thema, dann systematisch untersuchen.[19] Aus gehackten E-Mails der iranischen Behörden, welche *Miaan Group* analysiert hatte, wurde ersichtlich, dass die iranischen Behörden *LifeWeb*, eine iranische Analysegruppe für soziale Medien, beauftragt haben. Sie wurde angeheuert, um die Reaktionen der iranischen Nutzer*innen auf Twitter, Instagram und Telegram auf den Abschuss des ukrainischen Flugzeugs in Teheran im Januar 2020 zu analysieren. *LifeWeb* hatte für die iranischen Sicherheitsdienste einen sehr umfassenden Bericht dazu verfasst. *LifeWeb* ging dabei über die Analyse sozialer Netzwerke hinaus und beschäftigte sich auch mit politischer Inhaltsanalyse.[20]

Social Engineering und Entdeckung von Netzwerken. Die Überwachung wird oft in Form von digitaler Schadsoftware, zum Beispiel Malware[21] und Phishing-Angriffe[22], durchgeführt, die darauf abzielt, die empfangende Person zur Weitergabe von sensiblen Daten zu

---

15 Office of the Commissioner General for Refugees and Stateless Persons (Belgium), COI unit (CGRS-CEDOCA), Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 20: https://www.ecoi.net/en/file/local/2092670/coi_focus_iran._surveillance_van_de_diaspora_door_de_iraanse_autoriteiten_20230510.pdf.

16 Ebenda.

17 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.

18 Telefon-Interview vom 15. September 2023 mit Kontaktperson I.

19 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.

20 Ebenda; Miaan Group, Internet Oppressors: A Look at the Office of Iran's Attorney General and its Contractors, Unveiling the Involvement of Private Companies, Academic Institutions, Judicial Bodies, and Security Organizations in Iran's Internet Repression, Juli 2023, S. 44: https://filter.watch/en/wp-content/uploads/sites/2/2023/09/Internet-Oppressors-Report-2023.pdf.

21 Malware ist bösartige Software, die sich ohne Wissen der betroffenen Person durch das Anklicken eines Links oder Anhangs auf ihrem Gerät installiert.

22 Betroffene werden durch Phishing «gelockt» oder getäuscht und dazu gebracht, sich auf Websites anzumelden und ihre Daten preiszugeben. Oft werden gefälschte Konten oder Anwendungen dafür verwendet. Landinfo, Norwegian Country of Origin Information Centre, Iran; Reaksjoner mot iranere i eksil, 28. November 2022, S. 16: https://www.ecoi.net/en/file/local/2083379/Temanotat-Iran-Reaksjoner-mot-iranere-i-eksil-28112022.pdf

verleiten.[23] Nach aktuellen Erkenntnissen des *Bundesamtes für Verfassungsschutz* (BfV) ist von konkreten Ausspähversuchen der Gruppierung *Charming Kitten* gegen iranische Personen und Organisationen in Deutschland auszugehen. Hierzu verwendet die Gruppierung ein ausgefeiltes *Social Engineering* und entwickelt auf die Opfer zugeschnittene Online-Identitäten.[24] Unter *Social Engineering* verstehe man, dass ein Cyber-Angriff vorbereitet werde und eine Geschichte entwickelt werde, die das Opfer dazu verleite, eine gewisse Handlung vorzunehmen, zum Beispiel einen Anhang in einer E-Mail zu öffnen, in dem sich dann ein Schadprogramm befindet.[25] *Kontaktperson G* gab an, dass der iranische Geheimdienst in der Lage ist, anspruchsvolle und sehr gute OSINT-Recherchen (*Open Source Intelligence*) durchzuführen. In einem Fall, der von der *Miaan Group* dokumentiert wurde, fand eine Gruppe von Hacker*innen der iranischen Regierung viel über eine oppositionelle Person im Ausland heraus. Sie führten umfangreiche und ausgeklügelte Nachforschungen über diese Person durch. Sie fanden heraus, dass die Person einen Führerschein beantragen wollte und erstellten als Phishing-Angriff ein kostenloses Antragsformular für einen Führerschein für die Person im Ausland.[26] Laut *Cybersicherheitsexperte X* ist das Hauptziel der Überwachungsaktivitäten der iranischen Behörden im Ausland die Erstellung von Profilen der Zielpersonen und die Kartierung von Netzwerken. Dabei seien soziale und persönliche Informationen der Zielperson von Interesse, um Phishing-Angriffe durchführen. Das zweite Ziel sei es, Netzwerke der Zielperson und Kontakte zu entdecken, die durch die iranischen Behörden kompromittiert werden können.[27] *Kontaktperson H* wies darauf hin, dass iranische Hacker*innen Schwachstellen in Netzwerken finden und dadurch beispielsweise Zugang zu Mailkonten erhalten.[28] Staatliche Hacker*innen starten häufig Cyberangriffe gegen Aktivist*innen in der Diaspora.[29]

Einfache Identifikation von vielen «normalen» und unvorsichtigen Nutzer*innen. Viele Exil-Iraner*innen, die zuvor nicht politisch aktiv gewesen sind, haben sich in der Protestbewegung eingebracht. Da viele ihre Identität nicht genügend verbergen, ist ihre Überwachung für die iranischen Behörden einfacher.[30] Der *Präsident des Bundesamtes für Verfassungsschutz Thomas Haldenwang* warnte in diesem Zusammenhang vor Aktivitäten in den sozialen Medien, wodurch die Identität regimekritischer Menschen preisgegeben werden könnten. So hat der iranische Geheimdienst ein Interesse daran, die Teilnehmenden der grossen Solidaritätsdemonstrationen in Berlin zu identifizieren. Dass sich die Beteiligten gegenseitig bei der Demonstration fotografierten und filmten und die Bilder in den sozialen Netzwerken verbreiteten, machte es den iranischen Diensten laut *Haldenwang* noch einfacher. Schon seit einigen Jahren sei festzustellen, dass iranische Stellen ein Interesse an der Ausforschung dieser Menschen hätten.[31] Auch *Kontaktperson H* wies darauf hin, dass die iranischen Behörden in

---

23 Ebenda.

24 BfV, Cyber-Brief Nr. 01/2023, 10. August 2023, S. 1: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-01-bfv-cyber-brief-deutsch.pdf?__blob=publicationFile&v=5.

25 Tagesschau, Wie das iranische Regime seine Kritiker hackt, 19. August 2023: https://www.tagesschau.de/ausland/asien/iran-cyberfalle-verfassungsschutz-100.html.

26 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.

27 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 21.

28 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.

29 Freedom House, Freedom on the Net 2023 - Iran, 4. Oktober 2023.

30 Landinfo, Iran: Overvåking av regimekritikere i utlandet som følge av «Kvinne, liv, frihet-protestene», 5. Juli 2023, S. 4: https://www.ecoi.net/en/file/local/2094929/Respons-Iran-Overvaking-av-regimekritikere-i-utlandet-som-folge-av-Kvinne-liv-frihet-protestene-05072023-1.pdf

31 Die Zeit, Verfassungsschutz warnt Menschen iranischer Herkunft vor Ausspähung, 1. Januar 2023: https://www.zeit.de/politik/deutschland/2023-01/verfassungschutz-ausforschung-iran-regimekritiker-deutschland.

den sozialen Medien aktive Diasporamitglieder zum Teil einfach identifizieren können. So würden viele Personen sehr unvorsichtig ihre persönlichen Daten offenlegen. Wenn die Personen Fotos von sich auf sozialen Medien veröffentlichen würden, würde das die Identifikation stark vereinfachen.[32]

Fokus auf Inhalte in persischer Sprache. Aber auch Inhalte in anderen Sprachen können überwacht werden. Der Fokus der Überwachung liege nach Angaben der *Kontaktpersonen G* und *E*[33] auf Beiträgen in persischer Sprache.[34] Auch Beiträge in verschiedenen Sprachen werden nach Einschätzung von *Kontaktperson C*[35] überwacht.[36]

Nutzer*innenverhalten gibt Ausschlag, welche sozialen Medien überwacht werden. Das Nutzer*innenverhalten in Iran gibt nach übereinstimmender Einschätzung der *Kontaktpersonen H* und *I* Ausschlag, welches soziales Medium von den Behörden stärker überwacht wird. Instagram, Telegram und Twitter (beziehungsweise «X»[37]) seien aktuell populärer als Facebook. Entsprechend liegt der Fokus stärker auf diesen Medien. Überwachung kann man aber grundsätzlich bei keinem sozialen Medium ausschliessen.[38] *Cybersicherheitsexperte X* gab ebenfalls an, dass Twitter, Instagram und Telegram wichtige soziale Medien seien, um ein iranisches Publikum zu erreichen. Twitter und Instagram seien die wichtigsten sozialen Medien für Iraner*innen.[39] Laut *Cybersicherheitsexperte X* und *Kontaktperson H* ist Twitter eine sehr politische Plattform, während es bei Instagram eher um Unterhaltung geht.[40] Laut *Kontaktperson H* wird Twitter sehr stark überwacht und es werden viele Leute wegen Äusserungen auf Twitter verhaftet. Telegram habe unter den Iraner*innen sehr hohe Nutzer*innenzahlen – fast die Hälfte der Bevölkerung Irans –und sei entsprechend ebenfalls sehr interessant für die iranischen Behörden. Die iranischen Behörden verfügen aufgrund verschiedener Leaks von Kontodaten in der Vergangenheit bereits über sehr viele Daten von iranischen Telegram-Nutzer*innen und würden aktiv mit gefälschten Anmeldeseiten oder mit Nachahmer-Apps die Daten von weiteren Iraner*innen erhalten.[41] Blogs und Facebook sind laut *Cybersicherheitsexperte X* in Iran nicht mehr populär und entsprechend für die iranischen Behörden weniger interessant.[42]

3 Risikogruppen

Prioritäten der iranischen Behörden für die überwachten Gruppen können sich ändern. Laut dem auf den Iran spezialisierten *Cybersicherheitsexperten X* überwachen die iranischen Behörden Aktivist*innen im Exil. Sie hätten aber nicht die Kapazität, alle Aktivist*innen im Exil zu überwachen. Dabei setze das Regime Prioritäten auf der Grundlage seiner Interessen, und diese Prioritäten könnten sich ändern.[43]

---

32 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
33 Die iranisch-deutsche Kontaktperson E verfügt über Expertenwissen zu Iran.
34 Telefon-Interviews vom 23. und 24. Oktober 2023 mit Kontaktperson G und E.
35 Kontaktperson C ist politische Aktivist*in und Mitglied der iranischen Diaspora.
36 Telefon-Interview vom 26. Oktober 2023 mit Kontaktperson C.
37 Twitter hat im Sommer 2023 seinen Namen in «X» geändert.
38 Telefon-Interviews vom 27. Oktober und 15. September 2023 mit Kontaktpersonen H und I.
39 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 21-22.
40 Ebenda; Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
41 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
42 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 21-22.
43 Ebenda, S. 21.

Diaspora-Netzwerke und jede Form politischer Organisation im Fokus der iranischen Behörden. *Kontaktperson I*[44] gab der SFH an, dass jegliche Form von politischer Organisation in der Diaspora in den Fokus der iranischen Behörden fällt. Diaspora-Netzwerke würden sicherlich überwacht. Sobald es um Diaspora-Organisationen und -Netzwerke geht, die sich im Internet bilden, muss laut *Kontaktperson I* auf jeden Fall davon ausgegangen werden, dass die iranischen Behörden die Aktivitäten auf sozialen Medien überwachen.[45]

Landinfo weist darauf hin, dass Überwachung und Cyberangriffe eine breite Gruppe von Iraner*innen im Exil betreffen können.[46] Im Folgenden werden verschiedene Profile aufgeführt, die in Quellen genannt werden:

- **Opfer von Cyber-Attacken sind Regime-Gegner*innen des Iran.** Laut *Jadran Mesic, dem Leiter des Bereichs Cyberabwehr vom Bundesamt für Verfassungsschutz* werden in Deutschland «offensichtlich» Regime-Gegner*innen des Iran, die diese Meinung ganz offen kommunizieren und deshalb den iranischen Behörden Iran bekannt sind, Opfer von Cyber-Attacken. Darüber hinaus würden auch «enge Anbindungen an entsprechende Organisationen, die sich zum Beispiel für Menschenrechte im Iran einsetzen», bestehen.[47] Auch *Shiva Mahbobi, Sprecherin der Campaign to Free Political Prisoners in Iran* geht davon aus, dass regierungskritische Aktivist*innen überwacht werden.[48]
- **Journalist*innen.** Verschiedene Quellen berichten, dass Journalist*innen, auch solche, die für reformorientierte Medien oder ausländische Medien arbeiten, zum Ziel von Cyberangriffen oder Überwachung werden können.[49]
- **Gonabadi-Derwische**, **aserbaidschanische Dissident*innen**, **Frauenrechts- und Studentenaktivist*innen.** Zu den Opfern von Malware-Angriffen mit dem Ziel, bestimmte Gruppen innerhalb und ausserhalb des Landes anzugreifen und private Informationen zu sammeln, gehören auch Gonabadi-Derwische, aserbaidschanische Dissident*innen, Frauenrechts- und Studentenaktivist*innen.[50]
- **Dissidentenorganisationen**, **Jurist*innen und Menschenrechtsaktivist*innen.** Im Jahr 2022 berichteten mehrere IT-Sicherheitsdienstleister über die Gruppierung *Charming Kitten*, die an der Ausforschung von iranischen Oppositionellen und Exil-Iraner*innen beteiligt sein soll. Die Cyberangriffe richteten sich vor allem gegen Dissidentenorganisationen und Einzelpersonen wie Jurist*innen oder Menschenrechtsaktivist*innen innerhalb und ausserhalb des Iran.[51] Laut *Kontaktperson G* können Personen, die Informationen über Menschenrechtsverletzungen in Iran sammeln, zum Ziel der digitalen Überwachung werden.[52]

---

44 Kontaktperson I verfügt über Expertenwissen zu transnationaler Unterdrückung und digitaler Überwachung des iranischen Staats.
45 Telefon-Interview vom 15. September 2023 mit Kontaktperson I.
46 Landinfo, Iran; Reaksjoner mot iranere i eksil, 28. November 2022, S. 23.
47 Tagesschau, Wie das iranische Regime seine Kritiker hackt, 19. August 2023: https://www.tagesschau.de/ausland/asien/iran-cyberfalle-verfassungsschutz-100.html.
48 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 23.
49 Ebenda, S. 21; Telefon-Interviews vom 23. Oktober und 15. September 2023 mit Kontaktpersonen G und I; BfV, Cyber-Brief Nr. 01/2023, 10. August 2023, S. 1; Landinfo, Iran; Reaksjoner mot iranere i eksil, 28. November 2022, S. 23.
50 Freedom House, Freedom on the Net 2023 - Iran, 4. Oktober 2023.
51 BfV, Cyber-Brief Nr. 01/2023, 10. August 2023, S. 1.
52 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.

- **Aktivist*innen ethnischer Minderheiten und Umweltaktivist*innen**. Der *Cybersicherheitsexperte X* gab Cedoca an, dass unter anderem Aktivist*innen ethnischer Minderheiten und Umweltaktivist*innen Opfer von Hackerangriffen werden. [53]
- **Iranische Regierungsbeamte und «reformorientierte» Politiker*innen**, wie Mitglieder der Regierung des ehemaligen Präsidenten Hassan Rohani und Mahmud Ahmadineschād.[54]
- **Religiöse Minderheiten**, darunter Mitglieder des Baha'i-Glaubens, aber auch christliche, jüdische, zoroastrische oder sunnitisch muslimische Einzelpersonen und Institutionen.[55]
- **Kulturelle Persönlichkeiten** wie Künstler*innen, Musiker*innen, Karikaturist*innen und Satiriker*innen.[56]
- **Oppositionsgruppen, terroristische Organisationen, ethnische Separatistengruppen und ausländische Organisationen der Zivilgesellschaft**.[57]

Personen aus dem sozialen Umfeld der Zielpersonen. Datenangriffe, die versuchen, an die Anmeldedaten der Opfer für E-Mail- und Social-Media-Konten zu gelangen, zielen häufig auf grössere Gruppen oder Netzwerke von Einzelpersonen ab. Dies erhöhe die Wahrscheinlichkeit, dass sie an mindestens einem Ort erfolgreich sind und somit Zugang erhalten, um das gesamte Netzwerk zu gefährden.[58] Der iranische Geheimdienst kann auch an allen Formen von Informationen interessiert sein, die dazu verwendet werden können, Druck auf Einzelpersonen auszuüben, wie Informationen über Alkoholkonsum oder sexuelle Beziehungen.[59] Dies bedeutet, dass auch Personen aus dem sozialen Umfeld der Zielpersonen von den Geheimdiensten überwacht werden können.[60]

Cyber-Attacken eher gegen Dissident*innen mit hohem Profil, Überwachung aber auch gegen Personen mit niedrigem Profil. Laut dem auf *Cybersicherheit spezialisierten iranischen Experten Y* hängt die Art und Weise, wie iranische Behörden Iraner*innen im Ausland überwachen, vom Ziel ab. Die iranischen Behörden zielten mit Malware auf einige Dissident*innen in der Diaspora mit hohem Profil ab. Das Regime könnte hochrangige politische Aktivist*innen als Bedrohung ansehen und ausgeklügelte Cybersicherheitsangriffe gegen sie starten. Es sei laut *Experte Y* eher unwahrscheinlich, dass die iranischen Behörden Personen, die lediglich an Demonstrationen im Ausland teilnehmen, als hochrangige Ziele für solche ausgeklügelte Cybersicherheitsangriffe betrachten.[61] Auch *Kontaktperson H* wies darauf hin, dass die iranischen Behörden es bei Operationen wie Phishing und Hacking von Mails nur auf Personen mit niedrigem Profil abgesehen hätten, wenn diese Teil eines grösseren Netzwerks seien.[62] Es ist aber laut *Experte Y* gut möglich, dass die Social-Media-Profile von Personen, die keine hochrangigen Dissident*innen sind, überwacht werden. So können die iranischen Behörden beispielsweise lesen, worüber jemand twittert, oder sehen, wer im Netzwerk

53 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 21.
54 Landinfo, Iran; Reaksjoner mot iranere i eksil, 28. November 2022, S. 23.
55 Ebenda.
56 Ebenda.
57 Ebenda.
58 Ebenda.
59 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, 22. Februar 2021: https://www.ecoi.net/de/dokument/2047908.html.
60 Landinfo, Iran; Reaksjoner mot iranere i eksil, 28. November 2022, S. 23.
61 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 22.
62 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.

einer Person ist. *Experte Y* stellte klar, dass die iranischen Behörden hierfür öffentlich zugängliche Informationen verwenden und nicht private Konten überwachen würden.[63]

3.1 Anführen einer Gruppe

Behörden fokussieren eher auf Anführende und politische Aktivist*innen. *Kontaktperson G* gab der SFH an, dass die Intensität der Überwachung der Aktivitäten auf sozialen Medien davon abhänge, wer die Zielperson sei. Wenn die Regierung die betroffene Person als Zielperson einschätzt, werde sie möglicherweise überwacht. Wenn sie nur eine einfache Teilnehmende an einer Demonstration im Ausland sei und von den iranischen Behörden nicht als einflussreich wahrgenommen werde, würde die Regierung vermutlich ihre Aktivitäten in den sozialen Medien nicht überwachen. Nach Einschätzung von *Kontaktperson G* gehen die iranischen Behörden eher gegen Menschen vor, die Proteste anführen oder oppositionelle Aktivist*innen sind.[64] Der auf *Cybersicherheit spezialisierte iranische Experte Y* gab an, dass es die iranischen Behörden bei der Überwachung der iranischen Diaspora auf Führungspersönlichkeiten und Organisator*innen abgesehen haben, das heisst auf Personen, die eine Gruppe oder Partei anführen oder auf Personen, deren Aktivitäten von einer Gruppe von Menschen wahrgenommen werden.[65]

Es sind Ausnahmen möglich und unbekannte Personen können zufällig oder fälschlicherweise ins Visier geraten. *Kontaktperson G* betonte aber, dass es Ausnahmen geben könne, je nachdem, was die Person in den sozialen Medien oder anderweitig gemacht habe. *Kontaktperson G* wies darauf hin, dass die iranischen Sicherheitsdienste sich beispielsweise in ihrer Einschätzung irren könnten. So könnten sie eine Person fälschlicherweise für eine Anführerin halten, und sie ins Visier nehmen. *Kontaktperson G* wies als Beispiel auf den Fall einer iranischen Studentin in den USA hin. Sie sei in keiner Hinsicht eine relevante Oppositionsfigur gewesen, aber sie sei im Zusammenhang mit den jüngsten Diaspora-Protesten zu einer Fernsehsendung von *Iran International* eingeladen worden. Danach sei sie zum Ziel der iranischen Sicherheitsdienste geworden.[66] *Kontaktperson H* gab an, dass die iranischen Nachrichtendienste es gelegentlich auf unbekannte Personen abgesehen haben: «Niemand, weiss, wer sie sind, aber, aus welchen Gründen auch immer, haben die iranischen Behörden ein Interesse daran, sie zu verfolgen».[67] Die Behörden können zudem eine Person zufällig entdecken, weil sie an einer Diskussion teilgenommen hat, die bereits im Fokus der Behörden war.[68]

Personen, die Gruppen von beispielsweise fünf Menschen anführen, können bereits ins Visier der Behörden geraten. Es müssen keine «wichtigen Anführer*innen sein. *Kontaktperson G* wies auf Recherchen der *Miaan Group* hin, welche Fälle von digitaler Überwachung dokumentiert hatte. Die Personen, die ins Visier der iranischen Geheimdienste gerieten, führten dabei eine Gruppe an, die nicht gross sein muss. Fünf Personen waren so zum Beispiel ausreichend, um in den Fokus der Behörden zu geraten. *Kontaktperson G* betonte, dass es sich um keine «wichtigen Anführer*innen» handeln müsse. Die Zielpersonen können auch

63 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 22.
64 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.
65 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 22.
66 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.
67 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
68 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.

beliebige Personen in den sozialen Medien sein, die nur durch Zufall in den Fokus der Behördengeraten sind. Grundsätzlich könne man aber davon ausgehen, dass eine Person mit vielen Follower*innen in den sozialen Medien eher zum Ziel werde.[69]

Personen mit «grossem Bekanntheitsgrad», Anführende einer Gruppe und Personen mit Einfluss werden systematisch überwacht. *Kontaktperson G* wies darauf hin, dass eine Person, welche in den sozialen Medien einen «grossen Bekanntheitsgrad» habe, überwacht wird. Dabei spiele es keine Rolle, ob die verbreiteten Inhalte einen grossen Wahrheitsgehalt hätten. Es gebe Leute, die «Müll veröffentlichen» und verfolgt werden, weil die Leute sich für diese Themen interessieren und sie automatisch zu einer Person mit Einfluss werden. Es spiele keine Rolle, was man sage und mache. Wenn man sich nicht im Interesse des Irans verhalte, könne man zum Ziel werden. Wenn eine Person einen «grossen Bekanntheitsgrad» habe, eine Gruppe anführe oder eine Person mit Einfluss sei, werde sie rund um die Uhr und systematisch überwacht.[70]

3.2 Reichweite

Einfluss definiert sich aus iranischer Sicht nicht nur durch die Anzahl Follower*innen, sondern, ob eine Person einen Trend oder eine Debatte auslösen könnte. *Kontaktperson H* wies darauf hin, dass die iranischen Behörden in der Regel Jagd auf Menschen machen, die aus ihrer Sicht Einfluss haben. Zu beachten sei aber, dass in Iran die Definition des Begriffs *Influencer*in* völlig anders sei als in den USA oder in Europa. *Influencer*in* bedeute in Iran nicht, dass man 10'000 Follower*innen habe. Stattdessen sei relevant, dass die Person einen Trend oder eine Debatte über ein bestimmtes Thema auslösen könne. Wenn eine Person in diese Kategorie falle, werden die iranischen Behörden versuchen, die Person aufzuspüren.[71] Auch *Cybersicherheitsexperte X* weist darauf hin, dass der Einfluss, den eine Person habe, entscheidend sei, ob diese das Interesse der iranischen Behörden wecke. Dies könne beispielsweise eine Person sein, die auf Fernsehsendern wie *Iran International* oder VOA zu sehen ist. *Cybersicherheitsexperte X* geht im Gegensatz zu *Kontaktperson H* davon aus, das der beste Massstab, um den Einfluss zu messen, die Zahl der Follower*innen sein könne. Allerdings gebe es keine einfache Formel, um den Einfluss zu messen. So könnten in einem Fall 10’000 Follower*innen nicht viel sein, 50'000 oder 100'000 dagegen schon. Man müsse dabei auch bedenken, dass Follower*innen gekauft werden können. Wenn eine Person nur wenige Follower*innen habe, aber ein Beitrag von 500 Personen retweetet werde, sei das bedeutend. Wenn alle Tweets einer Person 100-mal retweetet werden, dann sei die Person beispielsweise ein*e *Influencer*in*. Wenn die Person die Berichterstattung beeinflussen könne, werde sie für die iranischen Behörden interessant. Es gehe darum, wie man ein Narrativ vorantreiben kann, das sei der wichtige Faktor. Die iranischen Behörden verfolgten Personen, deren «Stimme gehört werde».[72] *Kontaktperson H* wies zudem darauf hin, dass die Zahl der Aufrufe eines Beitrags ein wichtiger Faktor sein könne, um die Aufmerksamkeit der Behörden zu wecken. Auch wenn eine weitere Person einen Diskurs teile und verstärke, werden die Behörden diese Person laut *Kontaktperson H* bemerken und ins Visier nehmen.[73]

---

69 Ebenda.
70 Ebenda.
71 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
72 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 21.
73 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.

Mehr Reichweite führt vermutlich zu mehr Repression. Laut *Kontaktperson I* wird gegen Leute, die mehr öffentliche Reichweite haben, strikter vorgegangen, da sie als sichtbare Feinde wahrgenommen werden. Diese werden online bedroht, auch ihre Familien in Iran werden bedroht.[74] Auch *Kontaktperson G* geht davon aus, dass die Behörden repressiver vorgehen, wenn eine betroffene Person mehr Follower*innen hat. [75]

Neben Reichweite und Anführen einer Gruppe kann eine Verbindung oder Kommunikation zu einer Gruppe ein Faktor sein. Neben den Hauptelementen Reichweite und Anführen einer Gruppe, die zu einer Überwachung führen können, würden die weiteren Kriterien laut *Kontaktperson G* vom jeweiligen Fall abhängen. Dabei gehe es darum, ob die Person mit einer anderen Gruppe in Verbindung stehe oder ob sie mit einer anderen Gruppe kommuniziere. Die Behörden würden zudem weitere Recherchen durchführen, um herausfinden zu können, ob sie eine Person ins Visier nehmen wollen.[76]

3.3 Äusserungen

«Rote Linien» der Inhalte können jederzeit ändern. *Marcus Michaelsen* hat in einer Studie zahlreiche Diaspora-Aktivist*innen zur digitalen Überwachung autoritärer Staaten befragt. In den Interviews mit den Befragten wurden einige der Grenzen aufgezeigt, deren Überschreitung eine Reaktion der staatlichen Stellen hervorrufen könnte. Zu den Themen gehörten Persönlichkeiten des Regimes, Sicherheitsorgane, politische Gefangene, Folter, Korruption, wirtschaftliche Probleme sowie ethnische und religiöse Minderheiten. Mehrere Befragte wiesen darauf hin, dass «alles eine rote Linie» sein könne und es besser wäre, «sich gar nicht zu äussern». Bemerkenswert war laut *Michaelsen*, dass sich diese «roten Linien» je nach Situation und Kontext jederzeit ändern konnten. Diese willkürliche Machtausübung sei ein inhärentes Merkmal autoritärer Herrschaft und fördere Angst und Selbstzensur unter den Bürger*innen auch über die Grenzen hinweg.[77]

Häufung der Kritik vermutlich kein wesentlicher Faktor. Laut *Cybersicherheitsexperte X* sei die Quantität an Kritik, die eine Person am Regime übt, kein wesentlicher Faktor, der das Risiko für eine Überwachung erhöhe. Stattdessen sei der «Einfluss» der betroffenen Person ausschlaggebend.[78]

Vermutlich nicht relevant, ob eigene Äusserungen oder Beiträge Dritter geteilt werden. Nach Einschätzung der *Kontaktpersonen H* und *I* sei es nicht relevant, ob eine Person eigene Äusserungen oder Inhalte Dritter teile.[79] Im Zweifelsfall können die iranischen Behörden alles gegen die Person verwenden. Entsprechend sei schwierig einzuschätzen, was bei Behörden Aufmerksamkeit erregt. Wenn eine Person etwas geteilt habe, könne dies gegen sie verwendet werden, um sie unter Druck zu setzen, für die Geheimdienste zu arbeiten.[80] Laut *Kontaktperson G* lässt sich nicht mit uneingeschränkter Gewissheit sagen, ob die Repressionsmassnahmen Irans sich unterscheiden, wenn eine Person eigene Beiträge oder Inhalte Dritter teilt.

---

74 Telefon-Interview vom 15. September 2023 mit Kontaktperson I.
75 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.
76 Ebenda.
77 Michaelsen, Marcus, Silencing Across Borders, Transnational Repression and Digital Threats against Exiled Activists from Egypt, Syria, and Iran, 2020, S. 13.
78 CGRS-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10. Mai 2023, S. 21.
79 Telefon-Interviews vom 27. Oktober und 15. September 2023 mit Kontaktpersonen H und I.
80 Telefon-Interview vom 15. September 2023 mit Kontaktperson I.

Nach den Erfahrungen der Organisation von *Kontaktperson G* und den ihnen vorliegenden Informationen führe das blosse Teilen einer Äusserung in der Regel nicht dazu, dass man ins Visier der iranischen Sicherheitsdienste gerät. *Kontaktperson G* gab aber an, dass dies nicht mit abschliessender Sicherheit zu bestimmen sei.[81] Laut *Kontaktperson H* sei vermutlich entscheidender, ob die Person ein*e *Influencer*in* nach iranischer Definition sei.[82] *Kontaktperson G* betonte jedoch, dass auch eine Person, die nicht als *Influencer*in* gelte und nur einen Inhalt Dritter teilt, trotzdem ins Visier des iranischen Geheimdienstes geraten könne.[83]

Iranische Behörden gehen zum Teil unvorhersehbar vor und auch eine unbekannte Person kann bei Rückkehr verhaftet werden. *Kontaktperson G* wies darauf hin, dass es nicht davon abhängen müsse, welche Äusserung eine Person in einem sozialen Medium teilt. Es sei sehr schwierig vorherzusagen, ob und wann eine Person zur Zielscheibe werde.[84] *Kontaktperson H* wies darauf hin, dass das Vorgehen der iranischen Behörden nicht immer logisch sei. So könne alles auf ein hohes Risiko hindeuten, aber es könne sein, dass bei einer Rückkehr nichts passiert. *Kontaktperson H* kenne aber auch einige anders gelagerte Fälle. Dabei wurde ein zufälliger Beitrag in den sozialen Medien veröffentlicht und die Personen gerieten deswegen in Gefahr. Auch wenn eine Person kein «grosser Fisch» sei und nur einige hochrangige Mitglieder der Diaspora oder einige kritische Äusserungen in sozialen Medien *geliked* habe, könne es sein, dass die Behörden die Person verhaften, wenn sie zurückkehrt. Die iranischen Behörden könnten auch einen Fall «erfinden», um eine Person strafrechtlich zu belangen.[85]

81 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.
82 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.
83 Telefon-Interview vom 23. Oktober 2023 mit Kontaktperson G.
84 Ebenda
85 Telefon-Interview vom 27. Oktober 2023 mit Kontaktperson H.