Maatietopalvelu

Kyselyvastaus

**Asiakirjan tunnus:** KT891

**Päivämäärä**: 11.7.2024

**Julkisuus:** Julkinen

**Iran / Ulkomailla oleskelevat iranilaiset, viranomaisten harjoittama sosiaalisen median ja mielenosoitusten valvonta**

**Iran / Iranian abroad, monitoring of social media and demonstrations by the authorities**

Kysymykset

1. Onko Iranin viranomaisten raportoitu harjoittavan ulkomailla oleskelevien iranilaisten sosiaalisen median sisällön valvontaa?
2. Onko Iranin viranomaisten raportoitu harjoittavan ulkomailla hallinnon vastaisiin mielenosoituksiin osallistuvien valvontaa?

Questions

1. Is there reporting on authorities monitoring of social media content published by Iranians residing outside of Iran?
2. Is there reporting on authorities monitoring of Iranians residing outside of Iran and taking part of anti-government demonstrations?

# Onko Iranin viranomaisten raportoitu harjoittavan ulkomailla oleskelevien iranilaisten sosiaalisen median sisällön valvontaa?

Iranin turvallisuusjoukkojen toiminta Iranin ulkopuolella

Iranin ulkopuolella oleskelevat toisinajattelijat ovat olleet islamilaisen tasavallan aikana Iranin hallinnon ulkomaanoperaatioiden keskeisimpiä kohteita ja Iran on tehnyt jopa salamurhia aktivistien hiljentämiseksi. Iranin hallinto pitää monia ulkomailla oleskelevia iranilaisia uhkana sen turvallisuudelle ja olemassaololle.[[1]](#footnote-1) Turvallisuuspalvelut ovat kuitenkin sittemmin keskittäneet toimintaansa salamurhien sijaan piilotetumpaan toimintaan, kuten ulkomailla oleskelevien iranilaisten vakoiluun, sieppauksiin[[2]](#footnote-2) ja mustamaalaamiseen tai doksaamiseen[[3]](#footnote-3) [[4]](#footnote-4). Esimerkiksi Ruotsin turvallisuuspoliisi Säpon vuosia 2023–2024 koskevan vuosikertomuksen mukaan Iran toimii Ruotsissa useilla eri tavoilla hankkiakseen tietoa ja kyvykkyyksiä. Säpon mukaan Iranin tiedustelupalvelut keskittyvät maassa toimimaan Ruotsissa oleskelevaa iranilaisdiasporaa ja ‑oppositiota vastaan. Säpo huomauttaa, että Iran on käyttänyt myös Euroopassa väkivaltaa hiljentääkseen kritiikkiä ja kokemaansa uhkaa maan hallintoa vastaan.[[5]](#footnote-5)

United States Institute of Peace ‑tutkimuslaitoksen (USIP) julkaiseman Iranin tiedustelupalveluiden taktiikkaa käsittelevän artikkelin mukaan tiedustelupalvelut seuraavat Euroopassa ja muualla Iranin ulkopuolella oleskelevia toisinajattelijoita. Tiedustelupalveluiden kohteina ovat olleet eri oppositiotoimijat ja yksittäiset aktivistit ja toimittajat, erityisesti ne, jotka ovat osallistuneet niin kutsutun Vihreän liikkeen vuonna 2009 järjestämiin mielenosoituksiin tai myöhempiin vastaaviin. Tiedustelupalvelujen mielenkiinto kohdistuu erityisesti Iranin etnisiin vähemmistöihin ja arabi-, kurdi- ja belutsiseparatistiryhmiin. Erityisesti Iranin tiedusteluministeriö (MOI, *Ministry of Intelligence*, farsiksi *Vezarat-e ettelaat*) keskittyy Euroopassa toimivien opposition edustajien ja aktivistien valvontaan.[[6]](#footnote-6) Myös Iranin vallankumouskaartin tiedustelupalvelu toimii ulkomailla.[[7]](#footnote-7)

Internetissä ja sosiaalisessa mediassa tapahtuva valvonta

Useat tutkijat, medialähteet ja viranomaistoimijat toteavat Iranin viranomaisten harjoittavan ulkomailla oleskelevien iranilaisten sosiaalisessa mediassa tai laajemmin internetissä harjoittaman toiminnan ja julkaisujen valvontaa.[[8]](#footnote-8) Amsterdamin yliopiston tutkija Marcus Michaelsen kuvaa tieteellisessä Globalizations -lehdessä julkaistussa artikkelissaan, että Iran alkoi kehittää internetissä tapahtuvan toiminnan valvontaa vuonna 2009 Vihreän liikkeen aloittamien mielenosoitusten seurauksena.[[9]](#footnote-9) USIP- tutkimuslaitoksen mukaan Iranin tiedustelupalvelut käyttävät useita eri taktiikoita tiedon hankkimiseen. Ne pystyvät keräämään paljon tietoa verkossa tapahtuvasta toiminnasta, sieppaavat sähköistä viestintää ja seuraavat sosiaalista mediaa etsiäkseen Iranin hallitukseen kohdistuvaa kritiikkiä.[[10]](#footnote-10) Euroopan unionin turvapaikkaviraston Irania koskevaa maatietoraporttia varten haastatellun kurdeihin erikoistuneen Linné-yliopiston apulaisprofessori Barzoo Eliassin mukaan Iranin turvallisuusjoukkojen ”kyberjoukkojen” tehtävänä on seurata internetissä jaettuja [iranilaisten poliittisten aktivistien] mielipiteitä niin Iranissa kuin ulkomailla.[[11]](#footnote-11) Newlines Magazinen mukaan Iranin vallankumouskaartiin liitoksissa olevien Basij-joukkojen kyberjoukot ovat erikoistuneet sosiaalisen median seurantaan, hallinnon uhaksi katsomien henkilöiden tunnistamiseen ja näiden vastaisten hyökkäysten tekemiseen Iranissa ja sen ulkopuolella.[[12]](#footnote-12) Belgian maatietopalvelun Cedocan haastatteleman kyberturvallisuusasiantuntijan mukaan Iranin viranomaiset olisivat tehostaneet ulkomailla oleskelevien iranilaisten valvontaa vuonna 2022 käynnistyneiden mielenosoitusten seurauksena.[[13]](#footnote-13)

Cedocan haastatteleman kyberturvallisuusasiantuntijan mukaan viranomaiset kohdistavat seurantansa erityisesti vaikutusvaltaiseksi katsomiinsa henkilöihin, eikä kiinnostuksena ole niinkään yksittäiset kriittiset mielipiteet. Vaikka ei ole olemassa suoraa laskukaavaa siihen, mikä on viranomaisten mielestä kiinnostavaa, niin voidaan sanoa, että suuret määrät tilien seuraajia tai julkaisujen jakamisia ovat tässä suhteessa merkittäviä. Kun joku henkilö pystyy vaikuttamaan sosiaalisen median julkaisujen narratiiveihin, hänestä tulee kiinnostava. Myös toisen Cedocan haastatteleman kyberturvallisuusasiantuntijan mukaan varsinaiset hyökkäykset kohdistuvat ”korkean profiilin” toisinajattelijoihin ja henkilöihin, jotka johtavat jotain ryhmää tai joilla on vaikutusvaltaa. Toisaalta myös sellaisten ihmisten, joita ei voida sanoa korkean profiilin omaaviksi, tilien julkista sisältöä voidaan seurata tai tarkkailla, ketkä kuuluvat henkilön verkostoihin.[[14]](#footnote-14) Australian ulko- ja kauppaministeriön maatietoraportin mukaan myös Australiassa oleskelevien ”julkisen profiilin” omaavien iranilaisten sosiaalisten median toimintaa voidaan seurata Iranin viranomaisten toimesta. Ministeriön mukaan viranomaiset eivät kuitenkaan ”rutiininomaisesti” tee tutkintaa ulkomailla oleskelevien iranilaisten toiminnasta.[[15]](#footnote-15)

Kanadan maahanmuuttoviranomaisten haastattelema Yorkin yliopiston emeritusyliopistoprofessori huomauttaa myös, että joissain tapauksissa Iranin viranomaiset voivat käyttää muita ulkomailla oleskelevia iranilaisia, kuten opiskelijoita ja liikemiehiä, seuramaan viranomaisten näkökulmasta kiinnostavia maamiehiään.[[16]](#footnote-16)

Verkkohyökkäykset ulkomailla oleskelevia iranilaisia vastaan

Useiden tutkimuslaitosten, ihmisoikeusjärjestöjen, medialähteiden ja viranomaistoimijoiden mukaan Iranin viranomaiset ovat pystyneet hyökkäystarkoituksessa murtamaan ulkomailla oleskelevien iranilaisten sähköposti- ja sosiaalisen median käyttäjätilejä muun muassa phishing-verkkohyökkäyksillä[[17]](#footnote-17).[[18]](#footnote-18) Amsterdamin yliopiston tutkija Marcus Michaelsenin mukaan iranilaiset hakkeriryhmät, joilla on peiteltyjä yhteyksiä Iranin viranomaisiin, ovat tehneet verkkohyökkäyksiä useita kohteita vastaan Iranin ulkopuolella. Kohteina ovat olleet Lähi-idän ja sen ulkopuolisten maiden valtiolliset organisaatiot, yksityiset yritykset, kansainväliset tutkijat sekä poliittiset vastustajat ja kriitikot ulkomailla. Toiminnan luonteen vuoksi hyökkäyksiä on vaikeaa todistaa jonkun tietyn toimijan ja erityisesti valtiollisten toimijoiden tekemiksi tai tilaamiksi. Michaelsenin mukaan rikoksentekijöiden käyttämien ohjelmistojen ja haittaohjelmien tutkimisen perusteella voidaan kuitenkin päätellä, että nämä ovat työskennelleet Iranista käsin. Myös kohteiden valinta, erityisesti Iranin kansalaisyhteiskunnan ja diasporan toimijoiden joukosta, viittaa siihen, että niillä on pyritty ajamaan Iranin regiimin ja turvallisuusjoukkojen poliittisia ja strategisia etuja. Michaelsenin artikkelin mukaan ensimmäisen kerran vuonna 2015 paljastui, että Iranin viranomaiset pyrkivät murtamaan ulkomailla oleskelevien aktivistien käyttäjätilejä seuraamalla näiden toimintaa ja lähettämällä phishing-viestejä.[[19]](#footnote-19) Kanadan maahanmuuttoviranomaisten haastatteleman kyberturvallisuusanalyytikon mukaan Iranin viranomaiset käyttävät Kanadassa asuvien kansalaistensa valvomiseksi phishing-verkkohyökkäyksiä saadakseen tietoja valvontansa kohteena olevasta henkilöstä. Lähteen mukaan esimerkiksi oletetut Iranin viranomaiset olivat olleet häneen yhteydessä LinkedIn-palvelussa käyttämällä hakkeroitua ”erään tuttavan” tiliä ja lähettivät sitten analyytikolle linkin sivustolle, jonka avulla hakkeroitiin hänen sähköpostitilinsä ja päästiin käsiksi hänen salasanoihinsa.[[20]](#footnote-20)

Iraniin erikoistunut yhdysvaltalainen Miaan-ajatuspaja julkaisi vuonna 2020 raportin, jonka mukaan Antromedaa-niminen iranilainen yritys oli tehnyt vuosina 2018–2020 phishing-verkkohyökkäyksiä, joiden kohteina olivat muun muassa aktivistit ja Iranin etniset vähemmistöt. Hyökkäysten kohteina olivat iranilaiset Telegram-käyttäjät Iranissa sekä lukuisissa muissa maissa, myös Suomessa. Lisäksi yhtiö oli muun muassa luonut huijaussovelluksen, jonka kohteena olivat farsinkieliset henkilöt, jotka olivat hankkimassa ajokorttia Ruotsissa. Miaanin mukaan hyökkäysten kohteiden perusteella voidaan päätellä, että niiden taustalla on ollut valtiollista toimintaa.[[21]](#footnote-21)

Myös yhdysvaltalais-israelilainen kyberturvallisuusyhtiö Check Point julkaisi vuonna 2020 raportin, jonka mukaan iranilaiset tahot olivat jo vuodesta 2014 lähtien tehneet verkkovakoilua, jonka kohteena ovat olleet ulkomailla oleskelevat iranilaiset. Valtaosa seurannasta kohdistui Iranin vähemmistöihin kuuluviin aktivisteihin ja vastarintatoimijoihin, kuten Mujahedin-e Khalqiin (MEK), Azerbaijan National Resistance Organizationiin ja belutseihin. Myös Check Point oli havainnut phising-hyökkäysten ja huijaussovellusten käytön. Suuren osan hyökkäyksistä on toteuttanut Domestic Kitten -nimellä toimiva ryhmä.[[22]](#footnote-22)

Verkkohyökkäykset ovat jatkuneet syksyllä 2022 Iranissa alkaneiden mielenosoitusten jälkeen. Human Rights Watch raportoi joulukuussa 2022 Iranin hallintoon liitoksissa olevien hakkereiden käynnistäneen phishing-verkkohyökkäyksiin perustuvan vakoiluoperaation, jonka kohteena oli Human Rights Watchin työntekijöiden lisäksi muita ”korkean profiilin” aktivisteja, journalisteja, tutkijoita, diplomaatteja ja poliitikkoja, jotka työskentelevät Lähi-itää liittyvien asioiden kanssa. Operaation tarkoituksena oli päästä käsiksi uhrien sosiaalisten median ja muiden verkkopalveluiden yksityiseen sisältöön ja heidän yhteystietoluetteloihinsa. Ainakin yhdessä tapauksessa hyökkääjät olivat saaneet käyttöönsä kohteensa koko Google-palvelun historian, sisältäen muun muassa verkkohaut ja sijaintihistorian. Järjestö oli sen työntekijöihin kohdistuneen hyökkäyksen avulla pystynyt tunnistamaan 18 muuta tahoa, joihin hyökkäys oli mahdollisesti ja yhteydenoton jälkeen nämä tahot olivat pystyneet selvittämään hyökkäyksen kohteeksi joutumisensa.[[23]](#footnote-23)

Wired-verkkolehti uutisoi maaliskuussa 2023, että Iranin hallintoon liitettyjen tahojen tekemät phishing-verkkohyökkäykset olivat lisääntyneet tuolloin, mutta samanaikaisesti hyökkääjät ovat joutuneet kehittämään uusia tapoja ulkomailla oleskelevien iranilaisten seuraamiseksi, koska käyttäjät ovat tulleet tietoisemmiksi vakoiluyrityksistä. Wired mainitsee lisäksi Twitter‑palveluun luoduista, valesisältöä julkaisevista tileistä, joilla on julkaistu Iranin hallintoa kritisoivaa materiaalia tai sitä koskevaa valeuutisointia ja näin hallinto on pystynyt tunnistamaan sitä kritisoivia henkilöitä. Lisäksi oppositioryhmiä pyritään saamaan keskinäisiin kiistoihin tileillä julkaistun valeuutisoinnin avulla. Wired kuitenkin muistuttaa, että tilejä on vaikeaa suoraan yhdistää Iranin hallintoon, sillä iranilaiset ovat muutenkin usein anonyymeinä verkkopalveluissa.[[24]](#footnote-24) Newlines Magazinen artikkelin mukaan Iranin vallankumouskaartin alaiset tiedustelupalvelut ovat kohdistaneet uhkaksi katsomiinsa ulkomailla toimiviin iranilaisiin myös doksaus- eli mustamaalaamis- ja valeinformaatiohyökkäys. Operaatiot ovat keskittyneet poliittisiksi katsottuihin henkilöihin, ja niillä on pyritty haittaamaan poliittisesti aktiivisten henkilöiden mainetta levittämällä virheellisiä tai harhaanjohtavia tietoja näistä. Hyökkäysten kerrotaan lisääntyneen vuoden 2024 aikana.[[25]](#footnote-25)

Amsterdamin yliopiston tutkija Marcus Michaelsen huomauttaa alankomaalaisen Hivos-kehitysyhteistyöjärjestön vuonna 2020 julkaisemassa raportissa, että phishing-hyökkäykset harvoin kohdistuvat vain yhteen tiettyyn henkilöön, vaan ne keskittyvät eri ihmisten välisiin yhteyksiin ja näin pyrkivät hyökkäämään kokonaisia ryhmiä tai verkostoja vastaan. Yhden henkilön yksityisiä tietoja voidaan käyttää muiden tähän liitoksissa olevien tietojen paljastamiseen.[[26]](#footnote-26) Myös Wiredin haastatteleman kyberturvallisuusasiantuntijan mukaan Iraniin liitoksissa olevat hyökkääjät ovat alkaneet käyttää ”dominotaktiikkaa”, jossa ensin pyritään hakkeroitumaan ”matalan profiilin omaavien” kohteiden tileille. Tämän jälkeen uhrien tilejä käytetään luottamuksen luomiseen heidän “korkeaprofiilisten” yhteyksiensä kanssa, jotta näiden tilit voitaisiin myöhemmin murtaa. Wiredin haastattelema iranilainen ihmisoikeusaktivisti kertoo joutuneensa tällaisen hyökkäyksen uhriksi.[[27]](#footnote-27) Myös Belgian maatietopalvelun Cedocan haastatteleman kyberturvallisuusasiantuntijan mukaan Iranin viranomaiset saattavat käyttää muita sosiaalisen median käyttäjiä hyväkseen pystyäkseen hyökkäämään varsinaista kohdettaan vastaan.[[28]](#footnote-28)

Sosiaalisessa mediassa toimiviin ulkomailla oleskeleviin iranilaisiin kohdistuneet oikeudenloukkaukset

Michaelsenin haastattelemat aktivistit näkevät digitaaliset uhat ja hyökkäykset heidän viestintäjärjestelmiinsä ensisijaisesti Iranin turvallisuusviranomaisten viestinä siitä, että heitä seurataan. Vaikka hyökkäyksillä on harvoin suoria vaikutuksia, ne luovat painetta ja lisäkustannuksia, koska aktivistien on pakko miettiä verkkokäyttäytymistään ja suojella viestintäänsä.[[29]](#footnote-29)

Murtoyritysten lisäksi sosiaalisessa mediassa toimiville aktivisteille on lähetetty suoria uhkauksia. Ulkomailla toimiville aktivisteille on lähetetty myös haasteita oikeuteen vastaamaan syytteisiin heidän kotiosoitteisiinsa Iranissa.[[30]](#footnote-30) Myös Kanadan maahanmuuttoviranomaisten haastattelemien lähteiden mukaan Iranin viranomaiset ovat uhkailleet ulkomailla aktivisteina toimineita henkilöitä, muun muassa sosiaalisessa mediassa.Kanadan maahanmuuttoviranomaisten haastatteleman julkista valtaa tutkivan Macdonald-Laurier Instituten juristin mukaan järjestöllä oli tiedossa tapauksia, joissa epäiltiin Iranin viranomaisten seuraavan fyysisesti Kanadassa oleskelevia iranilaisia. Kanadan maahanmuuttoviranomaisilla oli myös tiedossa tapauksia, joissa Iranin viranomaiset olivat vierailleet Kanadassa oleskelevien iranilaisaktivistien perheiden luona tuoden ilmi, että he ovat tietoisia perheenjäsenen toiminnasta ulkomailla. Yhden haastatellun mukaan myös perheenjäseniä oli pidätetty ja kuulusteltu.[[31]](#footnote-31) Tunnetuin Iranin turvallisuusjoukkojen toteuttama sosiaalisen median käyttäjiin kohdistunut ulkomaanoperaatio on ollut Ruhollah Zahin sieppaus vuonna 2019. Ranskassa oleskellut Zam ylläpiti Telegram-kanavaa, jossa arvosteltiin Iranin hallintoa. skotaan, että Iranin viranomaiset saivat huijausviestejä käyttämällä Zahin matkustamaan Irakiin tapaamaan uskonnollista johtajaa, missä hänet siepattiin ja vietiin Iraniin. Zah sai kuolemantuomion toiminnastaan ja hänet teloitettiin joulukuussa 2020.[[32]](#footnote-32)

Michaelsenin toteaa Hivos-kehitysyhteistyöjärjestön vuonna 2020 julkaisemassa raportissa, että ulkomailla toimivia aktivisteja on paitsi uhkailtu mutta heihin on kohdistunut myös väkivaltaa, salamurhia ja pidätyksiä, jos he ovat palanneet Iraniin. Vastaavia uhkauksia on kohdistunut henkilöiden perheenjäseniin Iranissa.[[33]](#footnote-33) Myös Kanadan maahanmuuttoviranomaisten haastattelema julkista valtaa tutkivan Macdonald-Laurier Instituten juristin mukaan ”jotkut Iraniin palaavat iranilaiset”, joiden toimintaa on seurattu ulkomailla, joutuvat viranomaisten puhuteltaviksi maahan palatessa. ”Jotkut maahan palaavat” joutuvat myös luovuttamaan juristin mukaan passinsa viranomaisille ja heitä ohjeistetaan toisesta, myöhemmästä kuulustelusta.[[34]](#footnote-34) Myös Euroopan unionin turvapaikkaviraston Irania koskevaa maatietoraporttia varten haastatellun Barzoo Eliassin mukaan Iranin viranomaisten saatua ilmoituksen jonkin ulkomailla oleskelleen iranilaisen toiminnasta, tämä joutuu kuulusteltavaksi Iraniin paluun yhteydessä.[[35]](#footnote-35)

# Onko Iranin viranomaisten raportoitu harjoittavan ulkomailla hallinnon vastaisiin protesteihin osallistuvien valvontaa?

Amsterdamin yliopiston tutkija Marcus Michaelsen toteaa Hivos-kehitysyhteistyöjärjestön vuonna 2020 julkaisemassa Iranin, Syyrian ja Egyptin valtioiden harjoittamaa transnationaalista sortoa käsittelevässä raportissa, että kyseisten maiden suurlähetystöjen henkilökunta käyttää asemaansa hyväksi vakoillakseen ja häiritäkseen asemamaissaan oleskelevan diasporan poliittista toimintaa. Lähetystöjen henkilökunta osallistuu julkisiin tapahtumiin, jotka käsittelevät poliittista toimintaa ja saattavat myös häiritä näitä.[[36]](#footnote-36) Belgian maatietopalvelu Cedocan haastattelemien lähteiden mukaan Iranin viranomaiset tallentavat kuvia ja videoita henkilöistä, jotka osallistuvat mielenosoituksiin ulkomailla. Haastatellun ihmisoikeusasiantuntijan mukaan Iranin ulkomaanedustustojen valvontakameroiden kuvanlaatu on kehittynyt ja nämä voivat käyttää kasvojentunnistusteknologiaa. Haastatellulla kyberturvallisuusasiantuntijalla ei ollut todisteita siitä, että viranomaiset etsisivät mielenosoituksiin osallistuneita henkilöitä myöhemmin. Ihmisoikeusasiantuntijan mukaan vuoden 2009 yhteydessä ulkomailla mielenosoituksiin osallistuneilta on estetty saamasta konsulipalveluja Iranin edustustoissa mutta vuonna 2022 käynnistyneiden mielenosoitusten yhteydessä ei ollut tuolloin tietoja vastaavasta toiminnasta.[[37]](#footnote-37)

Myös Kanadan maahanmuuttoviranomaisten haastatteleman julkista valtaa tutkivan Macdonald-Laurier Instituten juristin mukaan Iranin viranomaiset valvovat kansalaistensa osallistumista tapahtumiin tai mielenosoituksiin Kanadassa. Viranomaiset seuraavat myös kansalaistensa "televisio- ja verkkotoimintaa" ulkomailla. Lähteen mukaan ”joidenkin Kanadassa asuvien iranilaisten” Iranissa asuvien perheenjäsenten luona on vieraillut viranomaisia sen jälkeen, kun he ovat osallistuneet televisio- tai verkkohaastatteluihin ja lähteen mukaan näin oli tapahtunut hänen omille sukulaisillensa. Lähteen mukaan Iranin viranomaisten valvovat henkilöitä, jotka ovat poliittisesti ”hyvin aktiivisia", mutta näiden lisäksi myös ”tavallisia ihmisiä”, jotka saattavat osallistua poliittiseen toimintaan vain ajoittain.[[38]](#footnote-38)

Uutislähteiden mukaan vuosina 2022–2024 on ollut tapauksia, joissa ulkomailla Iranin hallintoa kritisoiviin mielenosoituksiin osallistuneisiin on kohdistunut väkivaltaa tai uhkailua ja lähteet arvioivat näiden toimien taustalla olleen mahdollisesti Iranin hallinnon vaikuttamista.[[39]](#footnote-39) Iran International ‑uutissivuston mukaan toukokuussa 2024, Iranin presidentin Ebrahim Raisin kuoleman jälkeen, Lontoossa Iranin suurlähetystön edustalla järjestettyä opposition mielenosoitusta järjestänyttä ryhmää vastaan hyökättiin. Uutisen mukaan hyökkääjät olivat “Iranin islamilaisen tasavallan tukijoita” ja useiden haastateltujen asiantuntijoiden mukaan näiden taustalla on täytynyt olla Iranin hallinnon vaikuttamista. Lontoon poliisi ei kuitenkaan tuolloin kommentoinut hyökkääjien taustaa.[[40]](#footnote-40) Vastaavanlainen välikohtaus tapahtui Berliinissä lokakuussa 2022 Iranin suurlähetystön edustalla. Paikalle ilmestyi kolme henkilöä, jotka repivät mielenosoittajien käyttämästä ajoneuvosta heidän kiinnittämänsä Iranin demokraattista kehitystä tukevat kyltit pois ja tämän jälkeen pahoinpitelivät neljä ajoneuvossa ollutta mielenosoittajaa. Käytettävissä olevissa lähteistä ei löytynyt tarkempaa tietoa hyökkääjien taustoista.[[41]](#footnote-41) Vastaavasti CNN uutisoi maaliskuussa 2023 Ranskassa toimivasta mielenosoituksiin osallistuneesta iranilaisaktivistista, joka oli saanut uhkauspuheluita Iranin tiedusteluviranomaisilta ja lisäksi hänen Iranissa olevia sukulaisiaan oli uhkailtu ja kuulusteltu.[[42]](#footnote-42)

Australian kansallinen uutistoimisto AAP (Australian Associated Press) uutisoi syyskuussa 2023, että Australiassa toimivat iranilaiset aktivistit, mielenosoittajat ja oppositiotoimijat ovat kertoneet heihin kohdistuneesta häirinnästä ja väkivallasta useiden vuosien ajalta. Haastatellut mielenosoittajat ja heidän sukulaisensa ovat saaneet uhkauksia australialaisilta moottoripyöräjengeiltä ja aktivistit epäilevät, että Iranin hallinto on ostanut moottoripyöräjengiläisiä seuraamaan heidän toimintaansa. Lisäksi aktivistit epäilevät, että Iranin suurlähetystön työntekijät seuraavat heitä. Australian poliisi ei pystynyt vahvistamaan, että moottoripyöräjengiläiset kohdistaisivat toimiaan erityisesti iranilaisiin mutta Australian sisäministeri oli aiemmin kertonut, että tiedossa on Australiassa oleskeleviin iranilaisiin kohdistuvaa seurantaa, tarkkailua ja valokuvaamista.[[43]](#footnote-43)

## Lähteet

AAP (Australian Associated Press) 16.9.2023. *Iranians pledge strength amid spying, bikie threats*. Saatavilla Factiva-uutistietokannasta (<https://www.factiva.com>) [edellyttää kirjautumista] (käyty 8.7.2024).

CGVS/CGRA (Belgia: Commissariaat-generaal voor de Vluchtelingen en de Staatlozen/ Commissariat général aux réfugiés et aux apatrides) 10.5.2023. *Iran: Surveillance van de diaspora door de Iraanse autoriteiten*. [https://www.cgrs.be/sites/default/files/
rapporten/coi\_focus\_iran.\_surveillance\_van\_de\_diaspora\_door\_de\_iraanse\_autoriteiten\_20230510.pdf](https://www.cgrs.be/sites/default/files/rapporten/coi_focus_iran._surveillance_van_de_diaspora_door_de_iraanse_autoriteiten_20230510.pdf) (käyty 8.7.2024).

AP (Associated Press) 30.10.2022. *Police: Men attack pro-democracy vigil near Iranian embassy*. <https://apnews.com/article/iran-europe-middle-east-berlin-70729eb872f533b227c8e6c6052e9c37> (käyty 8.7.2024).

Australia: DFAT (Department of Foreign Affairs and Trade) 24.7.2023. *DFAT Country Information Report: Iran*. <https://www.dfat.gov.au/sites/default/files/country-information-report-iran.pdf> (käyty 8.7.2024).

Check Point Research 18.9.2020. *Rampant Kitten – an Iranian espionage Campaign.* <https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/> (käyty 8.7.2024).

CNN/Abdelaziz, Salma 21.4.2023. *These Iranian activists fled for freedom. The regime still managed to find them.* <https://edition.cnn.com/2023/04/21/europe/iran-paris-dissidents-mime-intl/index.html> (käyty 8.7.2024).

EUAA (European Union Agency for Asylum) 6/2024. *Iran – Country Focus*. <https://coi.euaa.europa.eu/administration/easo/PLib/2024_06_EUAA_COI_Report_Iran_Country_Focus.pdf> (käyty 8.7.2024).

The Guardian/Oltermann, Philip 31.10.2022. *Protesters attacked near Iranian embassy in Berlin*. <https://www.theguardian.com/world/2022/oct/31/protesters-attacked-near-iranian-embassy-in-berlin> (käyty 8.7.2024).

Hivos/Michaelsen, Marcus 2020. *Silencing across borders: Transnational repression and digital threats against exiled activists from Egypt, Syria, and Iran*. <https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf> (käyty 8.7.2024).

HRW (Human Rights Watch) 5.12.2022. *Iran: State-Backed Hacking of Activists, Journalists, Politicians*. <https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians> (käyty 8.7.2024).

Iran International/Mojtahedi, Negar 24.5.2024. *Islamic Republic's Loyalists Attack Iranian Protesters in London*. <https://www.iranintl.com/en/202405240084> (käyty 8.7.2024).

IRB Canada (Immigration and Refugee Board Canada) 2.3.2023. *Iran: Monitoring of Iranian citizens outside of Iran, including political opponents and Christians, by Iranian authorities; monitoring of Iranian citizens in Canada; consequences upon return to Iran (2021–March 2023)*. <https://irb.gc.ca/en/country-information/rir/Pages/index.aspx?doc=458777&pls=1> (käyty 8.7.2024).

Jansson, K. & von Solms, R. 2011. ”Phishing for phishing awareness”, *Behaviour & Information Technology*. Saatavilla: [https://www.tandfonline.com/doi/abs/10.1080/
0144929X.2011.632650](https://www.tandfonline.com/doi/abs/10.1080/0144929X.2011.632650) (käyty 8.7.2024).

Khoshnood, A. M. & Khoshnood, A. 2024. “The Islamic Republic of Iran’s Use of Diplomats in Its Intelligence and Terrorist Operations against Dissidents: The Case of Assadollah Assadi”, julkaisussa *International Journal of Intelligence and CounterIntelligence*, *37*(3). Saatavilla: <https://doi.org/10.1080/08850607.2023.2295205> (käyty 8.7.2024).

Miaan Group 2020. *Spiraling Attacks: Iranian Hacking Campaign.* <https://miaan.org/wp-content/uploads/2020/09/Spiraling-Attacks_Iranian-Hacking-Campaign.pdf> (käyty 8.7.2024).

Michaelsen, Marcus 2018. “Exit and voice in a digital age: Iran’s exiled activists and the authoritarian state”, *Globalizations 15(2)*. Saatavilla: <https://doi.org/10.1080/14747731.2016.1263078> (käyty 8.7.2024).

Microsoft [päiväämätön]. *Protect yourself from phishing*. <https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44> (käyty 8.7.2024).

Newlines Magazine/Golgar, Saeid & Aarabi, Kasra 18.3.2024. *Iran’s Dissenting Voices Are Being Targeted Online*. <https://newlinesmag.com/spotlight/irans-dissenting-voices-are-being-targeted-online/> (käyty 8.7.2024).

Säpo (Ruotsi: Säkerhetspolisen) 2024. *Säkerhetspolisen 2023/2024*. <https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf> (käyty 8.7.2024).

UC Berkeley (University of California Berkeley) [päiväämätön]. *Protect yourself from "Doxxing"*. <https://ethics.berkeley.edu/privacy/resources/protect-yourself-doxxing> (käyty 8.7.2024).

USIP (United States Institute for Peace)/Katzman, Kenneth 17.2.2023. *Explainer: Tactics of Iranian Intelligence*. <https://iranprimer.usip.org/blog/2023/feb/17/explainer-how-iran%E2%80%99s-intelligence-agencies-work> (käyty 8.7.2024).

Wired 21.3.2023. *The Scorched-Earth Tactics of Iran’s Cyber Army*. <https://www.wired.com/story/iran-cyber-army-protests-disinformation/> (käyty 8.7.2024).

Tietoja vastauksesta

Maahanmuuttoviraston maatietopalvelun kyselyvastaus on laadittu noudattaen Euroopan unionin yhteisiä suuntaviivoja lähtömaatiedon tuottamisesta (2008). Vastaus perustuu huolellisesti valittuihin lähteisiin, joista kaikki on listattu vastauksen lähdeluetteloon. Ilmeisiä ja kiistattomia tosiasioita lukuun ottamatta kaikki esitetty tieto on tarkastettu useammasta lähteestä, ellei muuta erikseen mainita. Vastauksessa esitetyt tiedot on hankittu, arvioitu ja käsitelty huolellisesti, vastausajan ollessa rajattu. Vastaus ei kuitenkaan pyri olemaan kaikenkattava, eikä sitä tule pitää yksinään minkään oleskeluluvan, pakolaisaseman tai turvapaikkahakemuksen perusteena. Vaikka jotain tapahtumaa, henkilöä tai organisaatiota ei olisi mainittu vastauksessa, se ei tarkoita, etteikö kyseistä tapahtumaa olisi tapahtunut tai kyseistä henkilöä tai organisaatiota olisi olemassa. Vastaus ei välttämättä edusta Maahanmuuttoviraston virallista kantaa, eikä se ole poliittinen kannanotto tai oikeudellinen arvio.

Information on the response

This response has been compiled by the Country Information Service of the Finnish Immigration Service in accordance with the common EU guidelines for processing country of origin information (2008). The response is based on carefully selected sources of information. All sources used are referenced. With the exception of obvious and indisputable facts, all information presented has been cross-checked from several sources unless stated otherwise. The information provided in the response has been obtained, evaluated and processed carefully within the limited time frame given. However, the response does not aim to be exhaustive, and it should not be considered conclusive as to the merit of any particular claim to a residence permit, refugee status or asylum. Even if a certain event, person or organization is not mentioned in the response, this does not mean that the event has not taken place or that the person or organization does not exist. The response does not necessarily reflect the opinion of the Finnish Immigration Service, and it is not a political statement or a judicial evaluation.

1. Khoshnood & Khoshnood 2024. [↑](#footnote-ref-1)
2. Khoshnood & Khoshnood 2024. [↑](#footnote-ref-2)
3. Doksaamisella (*doxxing)* tarkoitetaan henkilöön liittyvien tietojen keräämistä eri verkkoalustoilta (kuten sosiaalisesta mediasta) ja tämän tiedon levittämistä henkilön mustamaalaamistarkoituksessa. Tietoa voidaan hankkia julkisista tietokannoista, hakkeroimalla tai sosiaalisen manipuloinnin avulla. (UC Berkeley [päiväämätön].) [↑](#footnote-ref-3)
4. Khoshnood & Khoshnood 2024; Newlines Magazine/Golgar & Aarabi 18.3.2024. [↑](#footnote-ref-4)
5. Säpo 2024, s. 31, 35. [↑](#footnote-ref-5)
6. USIP/Katzman 17.2.2023. [↑](#footnote-ref-6)
7. USIP/Katzman 17.2.2023; Newlines Magazine/Golgar & Aarabi 18.3.2024. [↑](#footnote-ref-7)
8. Michaelsen 2018; USIP 17.2.2023; CGVS/CGRA 10.5.2023, s. 21–22; Australia: DFAT 24.7.2023; Newlines Magazine/Golgar & Aarabi 18.3.2024; EUAA 6/2024, s. 63. [↑](#footnote-ref-8)
9. Michaelsen 2018. [↑](#footnote-ref-9)
10. USIP/Katzman 17.2.2023. [↑](#footnote-ref-10)
11. EUAA 6/2024, s. 63. [↑](#footnote-ref-11)
12. Newlines Magazine/Golgar & Aarabi 18.3.2024. [↑](#footnote-ref-12)
13. CGVS/CGRA 10.5.2023, s. 21–22. [↑](#footnote-ref-13)
14. CGVS/CGRA 10.5.2023, s. 21–22. [↑](#footnote-ref-14)
15. Australia: DFAT 24.7.2023, s. 28, 40. [↑](#footnote-ref-15)
16. IRB Canada 2.3.2023. [↑](#footnote-ref-16)
17. *Phishing* eli tietojenkalastelu on sosiaaliseen manipulointiin (engl. *social engineering*) perustuva verkkohyökkäysten muoto, jossa valheellisesti esittämällä jotain oikeaa henkilöä tai palvelua pyritään saamaan käyttäjä paljastamaan henkilökohtaiset tietonsa (esim. salasana) oikeudettomasti. Tietoja käytetään tämän jälkeen murtautumiseen käyttäjän tietoihin verkkopalveluissa. (Microsoft [päiväämätön]; Jansson & von Solms 2011.) [↑](#footnote-ref-17)
18. Michaelsen 2018; Miaan Group 2020, s. 2, 4-5, 10; Check Point Research 18.9.2020; HRW 5.12.2022; IRB Canada 2.3.2023; Wired 21.3.2023. [↑](#footnote-ref-18)
19. Michaelsen 2018. [↑](#footnote-ref-19)
20. IRB Canada 2.3.2023. [↑](#footnote-ref-20)
21. Miaan Group 2020, s. 2, 4-5, 10. [↑](#footnote-ref-21)
22. Check Point Research 18.9.2020. [↑](#footnote-ref-22)
23. HRW 5.12.2022. [↑](#footnote-ref-23)
24. Wired 21.3.2023. [↑](#footnote-ref-24)
25. Newlines Magazine/Golgar & Aarabi 18.3.2024. [↑](#footnote-ref-25)
26. Hivos/Michaelsen 2020, s. 19. [↑](#footnote-ref-26)
27. Wired 21.3.2023. [↑](#footnote-ref-27)
28. CGVS/CGRA 10.5.2023, s. 21–22. [↑](#footnote-ref-28)
29. Michaelsen 2018. [↑](#footnote-ref-29)
30. Michaelsen 2018. [↑](#footnote-ref-30)
31. IRB Canada 2.3.2023. [↑](#footnote-ref-31)
32. Khoshnood & Khoshnood 2024. [↑](#footnote-ref-32)
33. Hivos/Michaelsen 2020, s. 20–21. [↑](#footnote-ref-33)
34. IRB Canada 2.3.2023. [↑](#footnote-ref-34)
35. EUAA 6/2024, s. 63. [↑](#footnote-ref-35)
36. Hivos/Michaelsen 2020, s. 21. [↑](#footnote-ref-36)
37. CGVS/CGRA 10.5.2023, s. 22–23. [↑](#footnote-ref-37)
38. IRB Canada 2.3.2023. [↑](#footnote-ref-38)
39. Iran International/Mojtahedi 24.5.2024; AAP 16.9.2023 CNN/Abdelaziz 21.4.2023; AP 30.10.2022; The Guardian/Oltermann 31.10.2022. [↑](#footnote-ref-39)
40. Iran International/Mojtahedi 24.5.2024. [↑](#footnote-ref-40)
41. AP 30.10.2022; The Guardian/Oltermann 31.10.2022. [↑](#footnote-ref-41)
42. CNN/Abdelaziz 21.4.2023. [↑](#footnote-ref-42)
43. AAP 16.9.2023. [↑](#footnote-ref-43)