Farsi Version

Download PDF .PDF

Accessibility

Text Size − 100% +

Related Articles

1. FATAwatch: April – June 2022
2. Hijab Legislation in Cyberspace: the Government Expands its Efforts to Suppress Personal Freedoms in Iran
3. The Rising Wave Of Impersonation
4. Increasing Control of Cyberspace to Repress Social Change
5. The Art of Deception:
6. A Cyber Power That Wasn't
7. Annual Report on The Impact of FATA Police on Citizen Rights in the Wake of the Women, Life, Freedom Movement
8. Iran Cyber Threat Intelligence Report: The Silent War Against Ethnic Minorities and Civil Society

Cyber Threat Reports

Wartime Cyber Crackdown and the Emergence of Mercenary Spyware Attacks

July 22, 2025 Filterwatch

Executive Summary

This report examines trends in cyberattacks, content management, digital rights violations, and arrests in the first six months of 2025, based on data from Miaan Group's Digital Security Helpdesk(DSH).

Digital repression in Iran has entered a new and unprecedented phase; a phase in which highly sophisticated technological tools have been employed for political and social repression. For the first time, Miaan Group has documented three Iranian individuals targeted by commercial-grade spyware comparable to Pegasus. This development indicates the government's shift from general surveillance to targeted and aggressive espionage.

During this same period, Israel's military attack brought a wave of widespread internet disruptions, user repression, and increased arrests. More than one-third of cases referred to the Digital Security Helpdesk after Israel's attack were related to disruptions in access to communication services, device seizures, or direct threats to user accounts.

Digital repression, particularly against women, ethnic minorities, and activists abroad, has intensified. Data shows that pressure on women, both in the form of account seizures under the pretext of "mandatory hijab" and in the form of

arrests and physical violence, has been on an upward trend. Furthermore, the share of users from Azerbaijan, Kurdistan, and other ethnic minorities in digital security cases has increased, and cyberattacks against Iranians abroad have expanded to new countries.

During this period, civil society organizations experienced the largest share of cyberattacks, and individual requests for help also saw an unprecedented increase; all of which are indicators of deepening repression across various layers of society.

Technically, the pattern of cyberattacks has become more advanced and organized, with phishing and impersonation, as well as exploitation of messaging platforms for infiltration and espionage, becoming widespread. Simultaneously, social coercion tactics such as SIM card seizures, threatening SMS messages, and cyber deception, aimed at controlling public behavior and cultural norms, have intensified.

This report indicates that ensuring digital security for civil society activists in Iran is no longer just a technical challenge, but has become a vital issue for their survival and the continuation of civil society activities.

During the twelve-day war of Israel against Iran, the security agencies of the Islamic Republic, took advantage of wartime conditions—using disinformation and deceptive tactics alongside targeted and complex cyberattacks—to carry out organized repression against ethnic minorities, civil society activists, and political opponents."

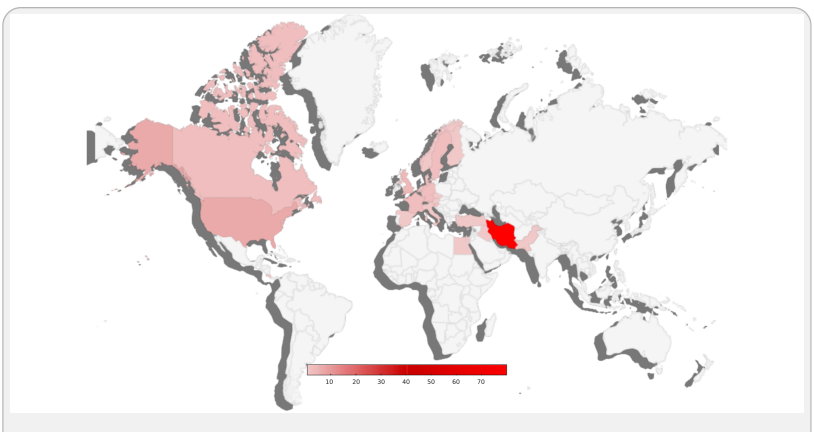
Key Findings

- **For the first time, three Iranian victims of mercenary spyware were identified:** In May 2025, Miaan's DSH identified three cyberattacks using such tools against Iranian users (two cases in Iran, one in Europe). This indicates the government's shift from general surveillance to targeted and advanced espionage.
- **A wave of digital repression during and after the 12-day war of Israel against Iran:** Following internet disruptions, phishing attacks, blocking access to communication services, and increased arrests, the Baha'i religious minority as well as artists were among the primary targets of security agencies.
- **Significant increase in digital repression against women:** Women accounted for over 46% of registered digital security cases, a figure that, along with documented arrests, torture, and harsh prison and death sentences, reflects an intensified focus by security and judicial agencies on repressing women.
- **Increased targeted repression of ethnic minorities, especially in West and East Azerbaijan:** The share of cases from these two provinces has reached over 12% — a five-fold increase compared to the previous six months.

- **Expansion of geographical repression in Iran:** A significant increase in cases in provinces such as Gilan, Isfahan, Razavi Khorasan, and Mazandaran, along with new cases recorded from provinces such as Golestan, Kermanshah, and Hormozgan.
- **Growth of cross-border attacks against Iranian activists abroad:** An increase in cases in the UK, France, Germany, Slovenia, and even countries like Austria and Egypt, indicates the global expansion of threats.
- **Civil society groups are the main target of cyberattacks by the Islamic Republic:** Organizational requests for digital support have increased by over 70%; in some areas such as minority and women's rights, the growth rate has exceeded 250%.
- **Significant increase in individual requests for digital security assistance:** A 720% growth in individual requests compared to the previous six months, indicating that repression extends beyond professional activists and threatens the entire civil society.
- **WhatsApp, Telegram, and Instagram platforms are the main targets of cyberattacks:** Phishing and social engineering attacks on these platforms have significantly increased, and attackers have used advanced techniques of impersonation, phishing traps, and account deletion.
- **Social and cultural repression has played a prominent role, particularly through censorship and pressure to conform to state-imposed norms:** Seizure of user accounts due to "non-observance of mandatory hijab" or "Islamic lifestyle," indicates the use of technology for cultural and social control.

Geographical Distribution

Digital repression in Iran has expanded not only in intensity but also in geographical spread. Tehran province remains at the top of the list for digital security violations, but data shows a significant increase in cases in provinces such as Gilan, Isfahan, Razavi Khorasan, and Mazandaran; an indication of the structural dispersion of repression and targeting of new areas. Also, for the first time, traces of similar repressive tactics have extended to provinces that were previously absent from statistics, such as Golestan, Hormozgan, and Qom.



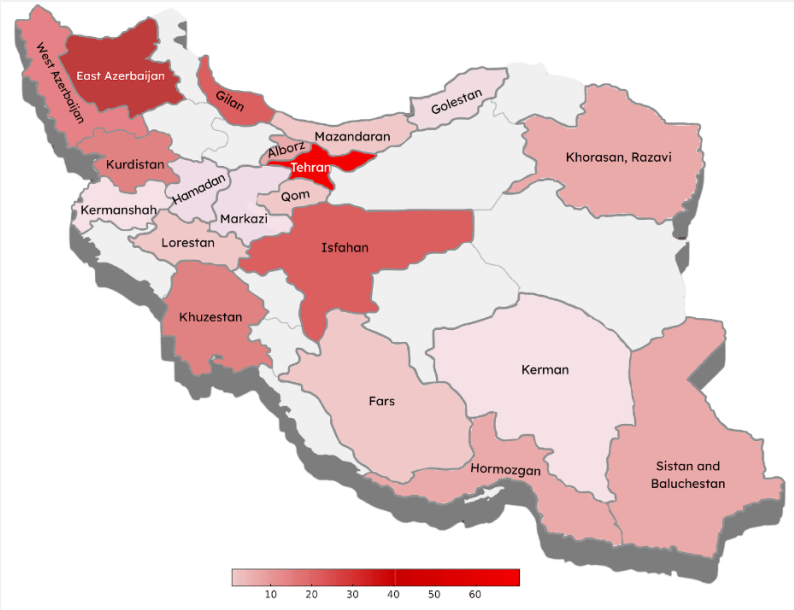
Worldwide Cyber Threat Landscape for Iran

Outside the country, despite a 9% decrease compared to the second half of 2024, the targeting of civil activists has expanded in European countries, with significant growth in countries like the UK, Germany, France, and even Slovenia. These developments indicate a comprehensive strategy by the Islamic Republic to expand the scope of digital repression both within and outside its borders.

Inside Iran

Tehran province, home to a high concentration of political institutions, parties, universities, and media outlets, remained the leading region for digital security violations. However, data from Miaan's DSH shows a nearly twofold increase in registered cases in winter and spring 2025 compared to the previous period.

Widespread arrests after a "Veterans" rally in protest of the political situation in February, the ongoing repression of students, political and civil activists, as well as pressures from security agencies under the pretext of wartime conditions after Israel's attack on Iran, indicate an intensification of systematic repression against opponents and the restriction of civil liberties under the shadow of regional and domestic developments.



Cyber Threat Landscape for Iran's Security Agencies Inside Iran

The pattern of digital repression in the first half of 2025 also shows another major change compared to the last six months of 2024: an increase in geographical spread.

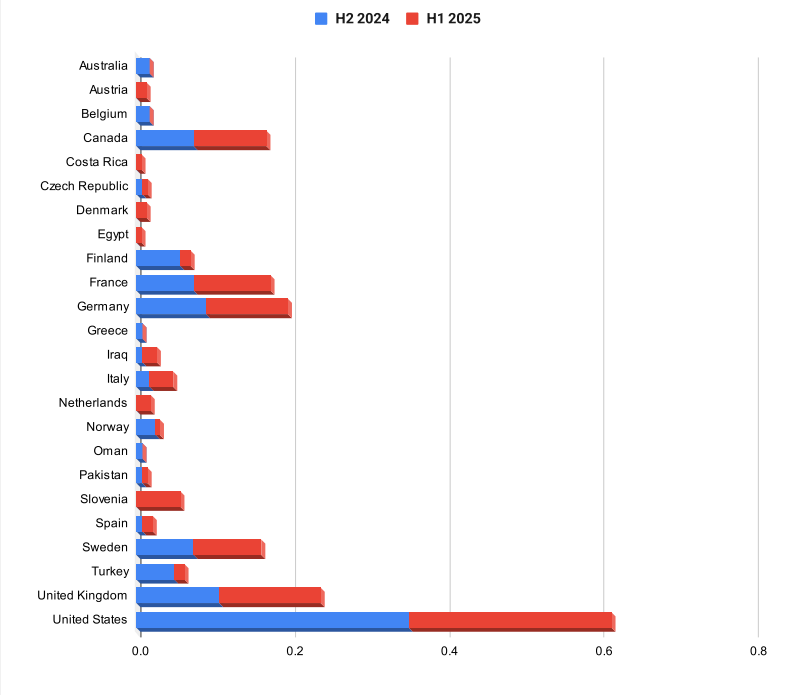
Cases registered in the past six months show an increase in digital repression with a growth rate of 175% in Gilan, 143% in Isfahan, 150% in Razavi Khorasan,

and 25% in Mazandaran province. These four provinces alone account for nearly 15% of the cases registered at Miaan's DSH.

Reports of digital rights violations by users in Golestan, Hamadan, Hormozgan, Khuzestan, Kerman, Kermanshah, Lorestan, and Qom provinces were also recorded in the past six months, which, in addition to increasing the depth of penetration of Miaan's DSH compared to the past, indicates the extent of the spread of repression last winter and spring.

Global Targeting of Iranian Civil Society

Iranian civil activists residing in the United States, despite a 9% decrease compared to the second half of 2024, remain the primary target of the Islamic Republic's security agencies.

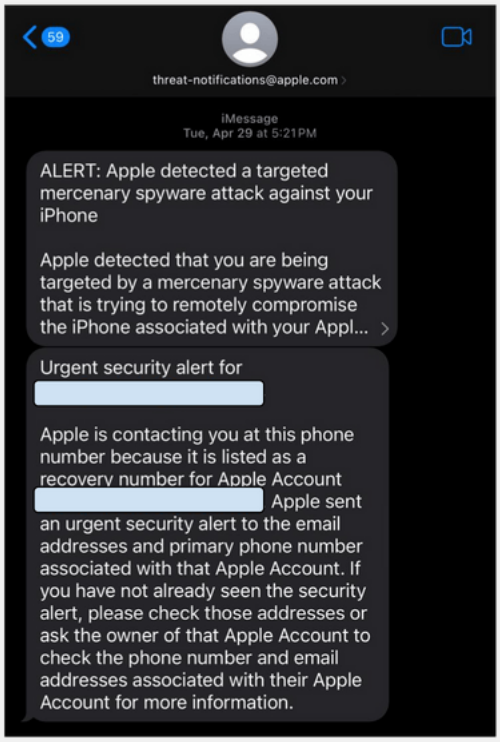


Comparison of the Geographical Distribution of Cyberattacks by the Islamic Republic's Security Agencies Against the Iranian Diaspora

The registered data also indicates an increase in the geographical targeting of Iranian diaspora civil society activists, with cases from Austria, Egypt, Denmark, the Czech Republic, Pakistan, and Costa Rica being recorded in winter and spring 2025.

Thematic Analyses

For the First Time: Mercenary Spyware Attacks Three Iranian Users



Screenshot of an Apple notification for an Iran-based user, revealing their device has been infected with mercenary malware

In May 2025, we identified three targeted cyberattacks using mercenary spyware against Iranian citizens (two cases in Iran and one in Europe), some of whom have a long history of political activism. Existing evidence suggests that there are more instances of this tool being used against Iranians. To protect the privacy of those targeted by this attack, we will refrain from providing further details about their identities.

This is the first time that documented evidence of the use of such highly advanced espionage tools, both inside Iran and against Iranians residing abroad, has been obtained.

Based on technical information and collected evidence, we believe that the identified cases may be linked to the recent **cyberattack** against European Parliament representative, Hannah Neumann. Investigations in this regard are ongoing; however, there are indications that these spyware tools may have been provided to Iranian entities through one of Iran's neighboring countries.

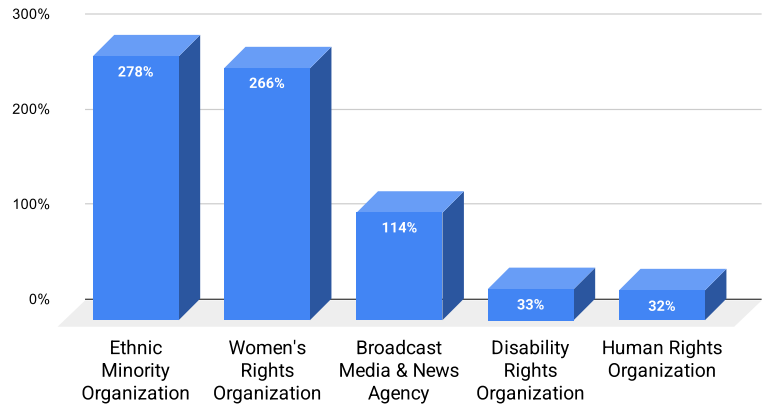
Mercenary spyware attacks, like those seen with tools such as Pegasus from NSO Group, are among the most advanced and expensive types of cyberattacks, usually carried out only by actors with extensive financial and technical resources and against specific targets. These attacks can give the attacker full control of the device, access to communications, sensitive data, location, and even activate the target's microphone and camera.

We anticipate that more instances of this type of tool being used against Iranian users, both inside and outside the country, will be identified. Therefore,

civil society, media, and digital rights advocacy organizations must react vigilantly and coordinately to the spread of this new threat.

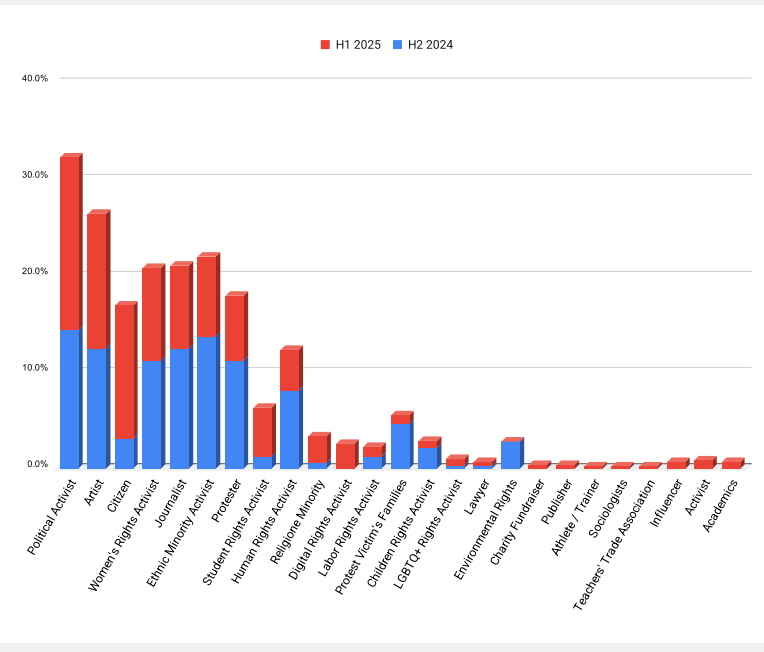
Civil Society Organizations are the Main Target of Security Agencies

Data shows that the number of individual requests for digital support in the first half of 2025 has seen an unprecedented growth—over 720%. This alarming jump indicates that cyber threats are no longer limited to well-known activists and that the scope of repression has extended to wider layers of society.



Cyberattacks Against Organizations.svg

Among those seeking support, political opponents had the largest share at 18%, followed by artists and women's rights activists (14% each), journalists (9%), and ethnic minority rights activists (8%). Other groups, including students, human rights defenders, religious minorities, digital rights activists, and workers, constituted between 1% and 3%. These statistics illustrate the expanding dimensions of digital threats and systematic repression at various levels of Iranian civil society.



Comparison of the Number of Individual Requests in the Second Half of 2024 and the First Half of 2025, Categorized by Field of Activity

Intensification of Repression Under the Pretext of War

The twelve-day war between Iran and Israel was not just a geopolitical crisis, but a turning point in the intensification of cyber threats, privacy violations, and the structural vulnerability of Iran's digital space. During this period, severe internet disruption, blockage of international communication tools, and widespread filtering severely weakened the digital security of users.

- **Threatening Internet Users and Followers of Accounts Attributed to Israel**

Internet users received SMS messages warning them against following or subscribing to social media pages or accounts associated with Israel—such as those belonging to media outlets, journalists, or official institutions. These actions aim to instill fear and promote self-censorship, restrict free access to information, and label independent journalists or government critics as security threats. This tactic is part of the broader effort by the Iranian authorities to control the flow of information and limit users' engagement with international sources.

- **Infrastructural Blockage and Secondary Effects on Account Security**

The cutting of international traffic ingress, blocking of foreign calls and SMS, and disruption of VoIP tools effectively rendered many users unable to receive identity verification codes (OTP and two-factor authentication). These disruptions were not merely technical dissatisfactions, but acted as targeted disruptions in the authentication process. Based on available data, nearly 12% of registered cases in this period are related to loss of access to social accounts due to not receiving these codes.

On the other hand, in a situation where installing and using secure messengers like Signal requires receiving an activation code, intentional disruption in sending OTP codes practically amounted to depriving users of secure and encrypted communications. This situation forced users to use virtual numbers or insecure non-native tools, increasing the level of threat.

- **Widespread Use of VPNs and Increased Risk**

With the intensification of internet restrictions, the need for VPNs increased significantly. Over 32% of visitors during this period requested VPNs. This surge not only underscores the collapse of free access to information, but also heightens the risk of users unknowingly relying on compromised VPNs—many of which may be fake, infected, or controlled by security agencies, as documented in previous cyber campaigns linked to the Islamic Republic.

- **Digital Repression Concurrent with Physical Pressure**

As military operations subsided and a ceasefire approached, digital threats against civil society intensified. More than 22% of war-related cases involved direct targeting of user accounts, including arrests, summons, or the seizure of devices used for digital activity.This trend indicates that digital threats, contrary to popular belief, do not decrease after the end of the physical phase of the war, but continue with greater focus and more precise tools.

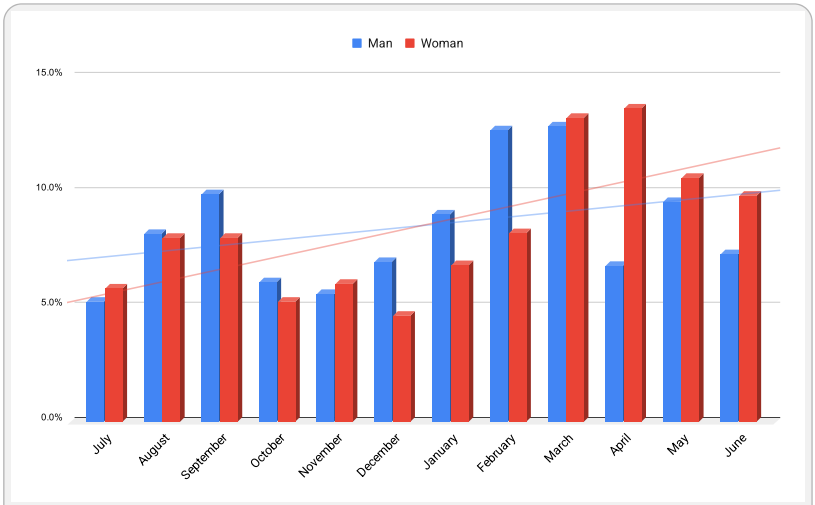
- **Selective Targeting of Minorities and Artists**

Among social groups, the Baha'i minority has accounted for the largest share of threats to user accounts. 12% of cases were related to this group, and in half of them, seizure of personal devices (phone, laptop, or computer) was reported. This issue is not only a violation of the right to privacy but also indicates systematic digital surveillance of religious minorities under the guise of national crises.

Artists, with 11% of all cases, are considered the second target group during the war. Data shows that photographers and documentary filmmakers, especially those active in the protest movement, faced more threats than others. These attacks indicate the intersection between controlling visual information, suppressing independent narrative-building, and restricting the circulation of visual information in wartime conditions.

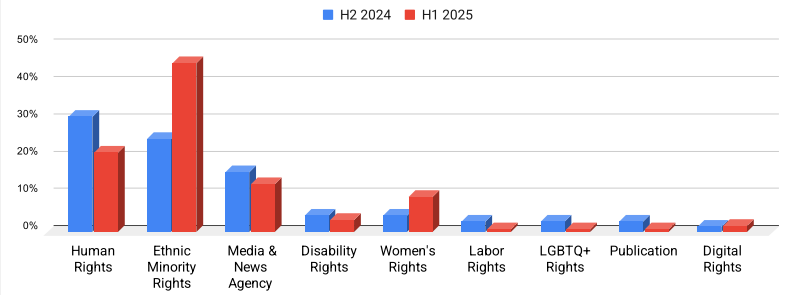
Harsher Repression of Women

Based on our data, repression of women increased in the first half of 2025. During this period, cases reported by women increased by 2.73%. In the second half of 2024, women accounted for approximately 44% of digital rights violation cases, compared to nearly 55% involving men. By early 2025, the proportion of cases reported by women rose significantly to over 46%, signaling a growing focus by authorities on targeting women in the digital space."



Increase in Digital Repression of Women Compared to Men Over the Past 12 Months

This data aligns with reports of intensified repression against women in the first half of 2025. During this period, approximately 60 female activists were arrested. Authorities also issued at least 12 death sentences and 19 prison sentences in April alone, followed by a total of 29 years and 4 months of imprisonment handed down in May. Amnesty International has confirmed that arbitrary arrests, sexual violence, and acts of torture—including shootings and instances of paralysis—were carried out against women involved in protests.



Comparison of the Number of Organizational Requests in the Second Half of 2024, Categorized by Field of Activity

Ethnic Minorities in Iran Still Under Cyber Attack

Ethnic minorities in Iran continue to be subjected to cyberattacks by the Islamic Republic's security agencies, but in the first half of 2025, the pattern of these attacks has undergone significant changes.

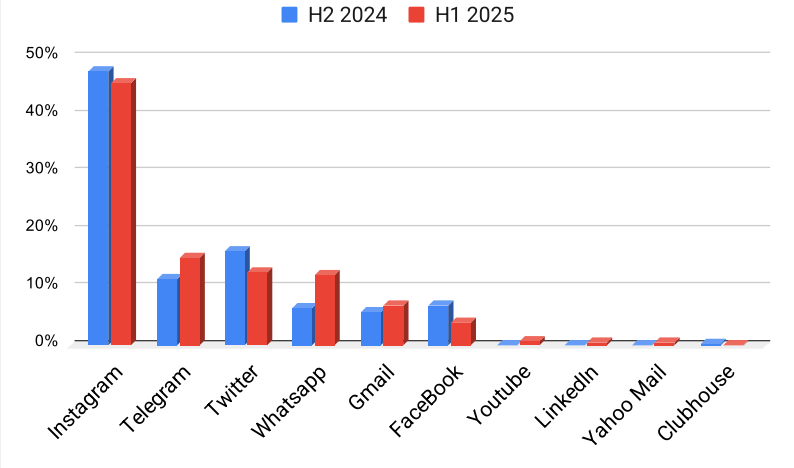
In winter and spring 2025, security pressures on the Turkic minority increased, and East and West Azerbaijan provinces have become new centers of cyber repression. Over 12% of registered cases were related to users in these two provinces, while this figure was only 2.5% in the second half of 2024. This spike coincided with identity-based Nowruz celebrations and gatherings of Tractor football club supporters, both of which were met with violent and widespread crackdowns. Human rights media such as Hengaw, Iran Human Rights Organization, and Kurdpa have repeatedly warned about increased repression in these areas.

In contrast, cyberattacks against the Baloch minority have decreased. While in the second half of 2024, over 9% of reports were related to Baloch users, this figure decreased to 2.5% in the first half of 2025.

Also, the focus of security agencies on the structured repression of civil organizations defending the rights of ethnic minorities has increased. In this period, 45% of support requests were registered by organizations and only 8% by individuals active in this field. This is while in summer and autumn 2024, the ratio of individuals to organizations was reversed (20% individuals, 13% organizations). This shift indicates a new focus of security agencies on weakening collective and institutional infrastructures for supporting minority rights.

How User Accounts Are Targeted on Major Platforms

In the first half of 2025, Instagram, Telegram, and Twitter were the most heavily targeted platforms. This data indicates that messaging and social networks remain the main communication tools for users and have aroused the most security sensitivity. A comparison between the data registered in the second half of 2024 and the first half of 2025 shows a significant growth rate of cyberattacks on various platforms.

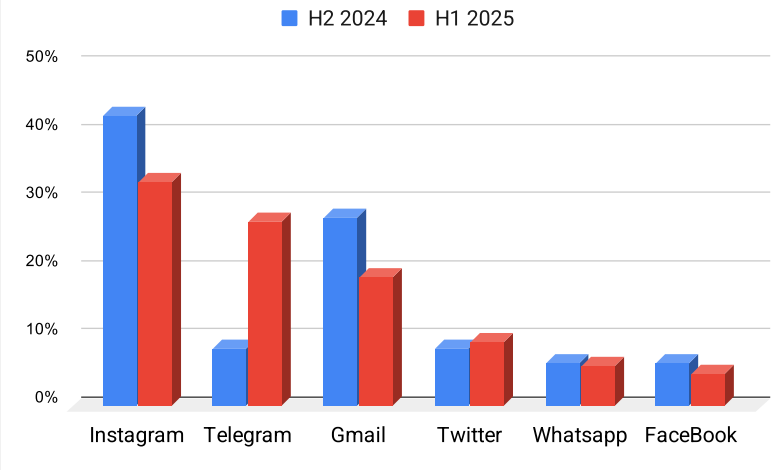


Comparison of Account Attacks Across Different Platforms

The increase in cyberattacks on user Gmail accounts indicates a greater focus on email accounts, perhaps for social engineering, infiltration, or surveillance. The inclusion of platforms such as YouTube, LinkedIn, and Yahoo in the list of targets of security agencies also indicates an expansion of the targeting scope.

Cyber Attacks

Cyberattacks by security agencies aimed at digital repression accounted for the largest share of threats and have seen significant growth compared to the second half of 2024. Based on the analysis of registered cases in winter and spring 2025, cyberattacks increased by 2.3%.



Comparison of Cyberattacks by Security Agencies Across Different Platforms

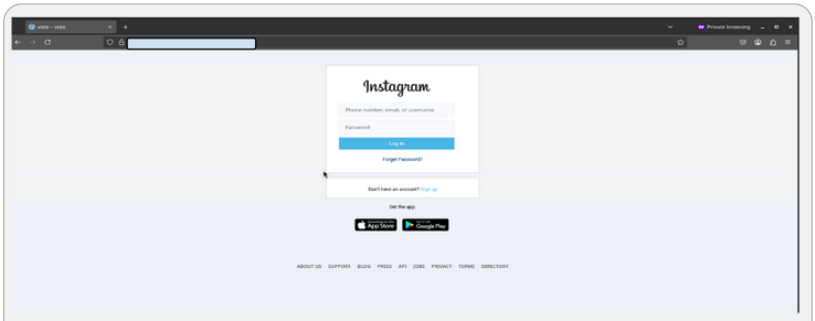
Examples of Cyber Attacks

We have received a total of 80 reports related to cyberattacks. Most of these involved a combination of phishing and impersonation techniques, where attackers used social engineering to gain the target's trust and lure them into clicking an infected link.

An examination of attack patterns shows that attackers have moved beyond classic phishing techniques and resorted to fabricating social trust structures, mimicking personal and professional tones, and exploiting platform vulnerabilities. The goal of these attacks goes beyond simple account infiltration; the perpetrators of these attacks seek access to communication networks, confidential information, and ultimately to create a climate of fear to restrict digital activism.

Organized Attacks on Artists

Attacks against artists were not only a means of accessing wider audiences but also part of the security-information strategy of government agencies aimed at cultural isolation and silencing symbols of public dissent. By targeting artists to infiltrate wider networks, these attacks reveal a calculated, chain-based approach in their design.



An image of a phishing website used to compromise the Instagram accounts of several artists.

Infiltration and Information Gathering from Human Rights and Women's Rights Activists

This category of attacks shows that attackers have turned to active and networked espionage and are not content with merely hacking accounts, but rather seek to reconstruct communication maps, identify collective structures, and disrupt human rights activities.

An image of a fake message in which a hacker attempted to impersonate an Oxford University student to deceive a women's rights activist and gain access to her account.

In one case, the victim's silence allowed the attackers to expand their infiltration, underscoring the critical need for rapid response and immediate security support.

Impersonation of International Bodies and Media

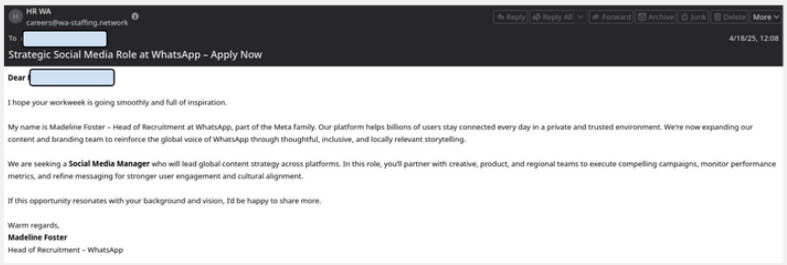
These patterns indicate more advanced and planned attacks. The precise impersonation of tone, signature, and even content shows that the attacker has acted with precise foreknowledge of the victim's background, professional position, and interests, and intends to infiltrate their digital assets through a gradual and targeted attack.

In one documented case, the identity of a senior BBC Persian reporter was impersonated to deceive the manager of Iran International news network through direct contact and gain access to their accounts. This attack occurred in a context that has long been accompanied by repeated threats against Persian-language media reporters. It is worth noting that Iran International network, which has been labeled a "terrorist network" by the Iranian government, has confirmed that it has been subjected to cyberattacks at least twice in the recent period.

These cases show that attackers not only operate with precise information about the relationships between media organizations and key individuals but also use targeted cognitive warfare to weaken the psychological and operational security of independent news organizations.

Exploiting Economic Conditions for Job Phishing

Attacks with job promises indicate the attackers' adaptation to the psychological-social contexts of the victims. This method combines social engineering and cognitive deception, turning economic vulnerability into an entry point for attack.


HR WA
careers@wa-staffing.network
Reply Reply All Forward Archive Junk Delete More
To [redacted]
4/18/25, 12:08
Strategic Social Media Role at WhatsApp – Apply Now
Dear [redacted]
I hope your workweek is going smoothly and full of inspiration.
My name is Madeline Foster – Head of Recruitment at WhatsApp, part of the Meta family. Our platform helps billions of users stay connected every day in a private and trusted environment. We're now expanding our content and branding team to reinforce the global voice of WhatsApp through thoughtful, inclusive, and locally relevant storytelling.
We are seeking a **Social Media Manager** who will lead global content strategy across platforms. In this role, you'll partner with creative, product, and regional teams to execute compelling campaigns, monitor performance metrics, and refine messaging for stronger user engagement and cultural alignment.
If this opportunity resonates with your background and vision, I'd be happy to share more.
Warm regards,
Madeline Foster
Head of Recruitment – WhatsApp

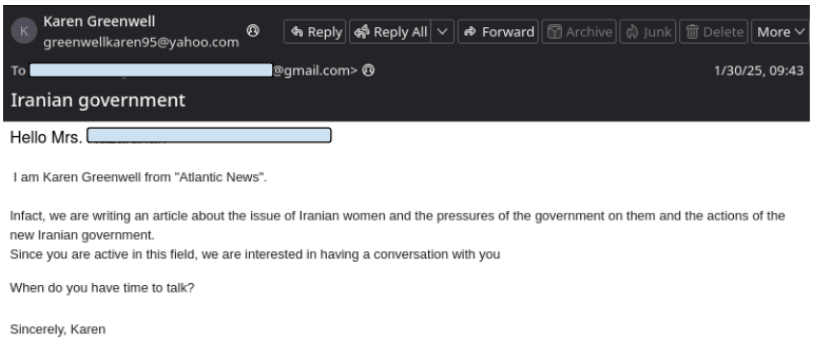
An image of a fake email attempting to impersonate the WhatsApp recruitment team at Meta.

Algorithmic Manipulation and Restriction of Active Accounts

These attacks are based on exploiting platform architectures. Without the need for direct infiltration, attackers can use coordinated operations to turn automated system behaviors against activists. This is a type of digital repression at the algorithmic level.

Hate Speech, Direct Threats, and Media Fabrications

At this stage, cyber threats have moved beyond technical infiltration and entered the realm of information operations and psychological warfare. The goal of these attacks is no longer merely to cause disruption, but to destroy social reputation, eliminate influential symbols, and create a climate of fear and distrust among civil society.

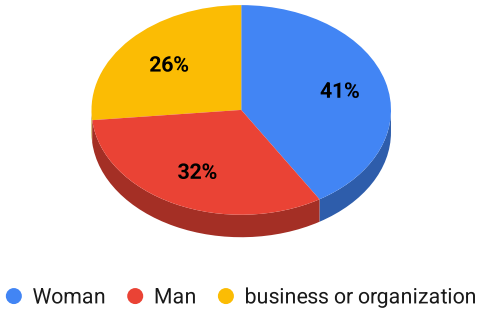

Karen Greenwell
greenwellkaren95@yahoo.com
Reply Reply All Forward Archive Junk Delete More
To [redacted]@gmail.com>
1/30/25, 09:43
Iranian government
Hello Mrs. [redacted]
I am Karen Greenwell from "Atlantic News".
Infact, we are writing an article about the issue of Iranian women and the pressures of the government on them and the actions of the new Iranian government.
Since you are active in this field, we are interested in having a conversation with you
When do you have time to talk?
Sincerely, Karen

One sign of this change is the significant increase in cases related to "content management," which now accounts for 39% of all reports. These attacks are often aimed at controlling user accounts and exploiting them to spread false

information, distort narratives, or engage in character assassination. The largest share of these threats belongs to Instagram with 53%, followed by Twitter (X) with 32%, and then Telegram with 14%. These figures show that major social platforms have become battlegrounds for psychological warfare against civil society.

Social Norms Threats

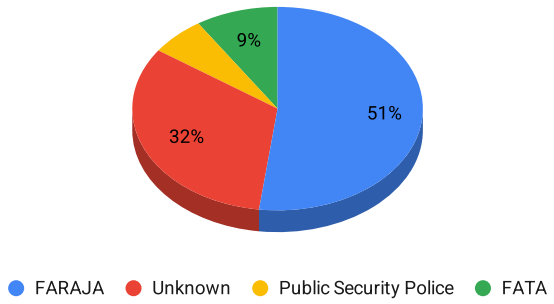
Social norms threats, one of the less technical but deeply repressive aspects of the Islamic Republic's cyber warfare, are a set of targeted actions to control citizens and impose specific lifestyle patterns. These actions include seizing user accounts on social networks, sending threatening SMS messages to unveiled women, seizing SIM cards, cyber deception, and psychological pressures against users for publishing content contrary to government norms. The main focus of these repressions has been on women and social minorities, which has severely violated not only their freedom of expression but also their privacy.



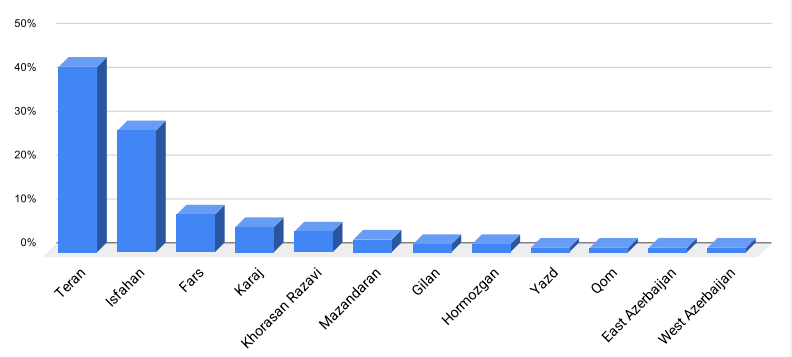
We have recorded an unprecedented increase in the seizure of Instagram accounts, with women being the primary target. The predominant reasons for these seizures were non-observance of "mandatory hijab" (57%) and "non-observance of Islamic lifestyle" (15%). Sexual and political content each constituted only 4%, indicating a strong focus of threats on cultural and gender control.

In the documented cases, the widespread seizure of accounts belonging to female singers, especially after the release of the "Caravanserai" concert by Parastoo Ahmadi in winter 2024, is noteworthy; nearly 12% of all seized accounts in this period belonged to female singers. The scope of seizures, however, was not limited to individuals, and organizations, brands, companies, and event organizers focused on women were also targeted. Companies such as "Seh Nan," "My Lady," and the organizers of the "National Architecture Awards" were seized or forced to hand over control of their accounts to security agencies due to the publication of images of unveiled women. Also, the creators of "Blind Date" videos and related activists were targeted with account seizures on Instagram and YouTube after the arrest of figures such as "Vini."

Based on the collected data, "FARAJA" (Law Enforcement Force of the Islamic Republic of Iran) had the largest role in account seizures with 51%, while in 32% of cases, the responsible entity was not specified, and FATA Police (Cyber Police) and Public Security Police were responsible for 9% and 6% of the actions, respectively.



Simultaneously, the sending of threatening SMS messages to unveiled women, which began in 2023, intensified in winter 2024 and spread from Isfahan to other cities. An examination of data from Mian Group's Digital Security Helpdesk in collaboration with the United for Iran organization shows that these actions are carried out using advanced surveillance technologies such as IMSI-Catcher. These tools, by identifying the location and characteristics of users, cause temporary disruption in mobile internet before sending SMS messages. 6% of survey respondents confirmed such a disruption.



Geographical Distribution of Mandatory Hijab SMS Notifications

Tehran with 42%, Isfahan with 29%, and Shiraz with 9% accounted for the largest share of threatening SMS messages registered in spring 2025. The highest frequency of SMS messages was in May. Although the government announced in June, coinciding with Israel's attack on Iran, that this process would stop, data indicates the continuation of pressures. In some cases, SMS messages were not limited to threats, and 12% of recipients were referred to judicial authorities.

This set of data indicates that the Islamic Republic is attempting to bring the lifestyle, privacy, and cultural space of society under complete control by utilizing cyber, surveillance, and police tools; and among them, women are most directly exposed to threats. Although after Israel's attack on Iran, the

sending of threatening SMS messages to women due to their attire was stopped.

Indicators of Compromise

URLs:

https://votescontests[dot]tranoclassic.com/

https://cvote[dot]famlagstrom.se

https://telrgram[dot]chat/

https://telvgram[dot]life/

https://shorten[dot]ee/@help_center_6639

https://teleok[dot]org

https://teleomm[dot]sbs/dist/

https://teinfo[dot]vip/

https://telrgram[dot]chat

https://joining-hosts-room[dot]online

https://www.mediafire[dot]com/folder/x5ctohdrdibok/Files

IPs:

185.151.30.222

77.238.179.82

104.21.16.1

104.21.45.73

198.54.127.78

209.85.220.41

104.21.16.1

103.42.179.60

103.42.179.60

92.118.147.35

91.195.240.19

185.201.18.55

Emails:

help11223311[at]outlook.com

fxyfgg[at]gmail10p.com

owieoi[at]oegmail.com

isaaceboh70[at]gmail.com

emailvote337[at]gmail.com

richardjohn8673[at]gmail.com

cavallariopgn614120[at]hotmail.com

greenwellkaren95[at]yahoo.com

karen[at]msmagazine.co

careers[at]wa-staffing.network

brett[at]beardesigns.com.au

Files:

kitchen.exe,
2fe9ecdbd7c97bd732ad81b5fd3e4961ea6f25d3fd04b5ed881c436118cce3b9

Tags Cyber Attacks on Civil Society
Cyber Repression Ethnic Minorities Iran
Iran Cyber Threats
Israel Iran Cyberwa
Mercenary Spyware
Phishing Attacks Iran 2025

فارسی
filter.v