Trustwave Insights: Navigating the Cyber Front Line in the Israel-Iran Conflict

Trustwave®
SpiderLabs®

Table of Contents

Key Findings

- Israel and Iran are conducting stealthy cyberattacks against each other, with the results often becoming public only after visible effects emerge.
- Multiple cyber groups have already become actively involved in the cyberwarfare between Israel and Iran.
- Currently, a pro-Israeli group has carried out a disruption attack on Iran's banking and crypto systems. Many of these activities attempt to make a psychological impact on the population of other countries.
- Smaller hacktivist groups are often operating under umbrella identities like the Cyber Islamic Resistance or United Cyber Front for Palestine and Iran. These loosely affiliated "cyber unions" share resources and synchronize campaigns, amplifying their impact despite limited technical sophistication.
- One threat actor, DieNet, maintains a hybrid identity. While it operates under a pro-Iranian and pro-Hamas narrative, there is mounting evidence of its Russian-speaking members and technical connections to cyber communities in Eastern Europe.
- One of the most active pro-Israeli cybergroups is Gonjeshke Darande, translated as Predatory Sparrow. It is a highly sophisticated and widely believed to be affiliated with Israeli intelligence.
- Fake alert disinformation campaigns continue to evolve beyond infrastructure into the cognitive and emotional domains; these manipulative tactics underscore the growing threat of non-technical but highly impactful digital influence operations.
- Numerous cybergroups are conducting DDoS attacks against the opposition, making different services inaccessible to common citizens.

Israel-Iran Cyberwarfare

The cyber conflict between Iran and Israel is rooted in a broader geopolitical rivalry that spans decades .. Iran views Israel as an illegitimate presence in the Middle East and a close ally of its main adversary, the United States. Israel, in turn, perceives Iran's nuclear ambitions, support for proxy groups like Hezbollah and Hamas, and its influence operations across the region as existential threats. Against this volatile backdrop, cyber warfare has emerged as a critical front in their ongoing confrontation.

Cyber operations offer both states the ability to conduct deniable, cost-effective, and asymmetrical actions far beyond their borders. For Iran, whose conventional military capabilities are relatively limited compared to Israel's, cyberattacks provide a strategic equalizer, enabling it to project power and retaliate without triggering open war. Israel, known for its technological superiority and advanced intelligence services, has leveraged cyber capabilities to carry out precise, high-impact operations designed to delay Iran's nuclear progress and disrupt hostile infrastructure.

What sets the Israel–Iran cyber conflict apart is its persistence and intensity. Unlike conventional warfare, these digital clashes are ongoing, with attacks often unfolding silently, in parallel to diplomatic developments or covert operations. The line between cyber espionage and cyber sabotage is frequently blurred. While the most visible operations often come from hacktivist fronts or public defacement campaigns, it is important to note that both Israel and Iran are also conducting highly targeted, stealthy cyber operations behind the scenes. These state-level campaigns are typically more strategic, involve advanced capabilities, and rarely surface in open-source channels, making them harder to detect, attribute, or assess in real time.

We are continuously monitoring the situation, tracking shifts in tactics, new actors, and cross-regional alliances that may signal changes in the intensity or objectives of this cyber conflict. The cyber domain has become a central theater in the Israel–Iran cyberwarfare, serving both as a tool for strategic influence and as a battlefield for covert, high-stakes confrontation.

Hacktivist Coalitions and Cyber Group Alignments

The cyber warfare landscape between Iran and Israel is not limited to state actors, it has rapidly expanded into a crowded and volatile ecosystem of non-state hacktivist coalitions. The image reveals a stark asymmetry in group alignment, with 65 hacktivist groups supporting Iran, compared to 11 anti-Iran groups and only 6 pro-Israel cyber collectives. This imbalance reflects broader geopolitical sentiment in online spaces, where narratives opposing Israel tend to mobilize more hacktivist engagement, particularly from actors across the Middle East, South Asia, North Africa, and even parts of Latin America and Eastern Europe.

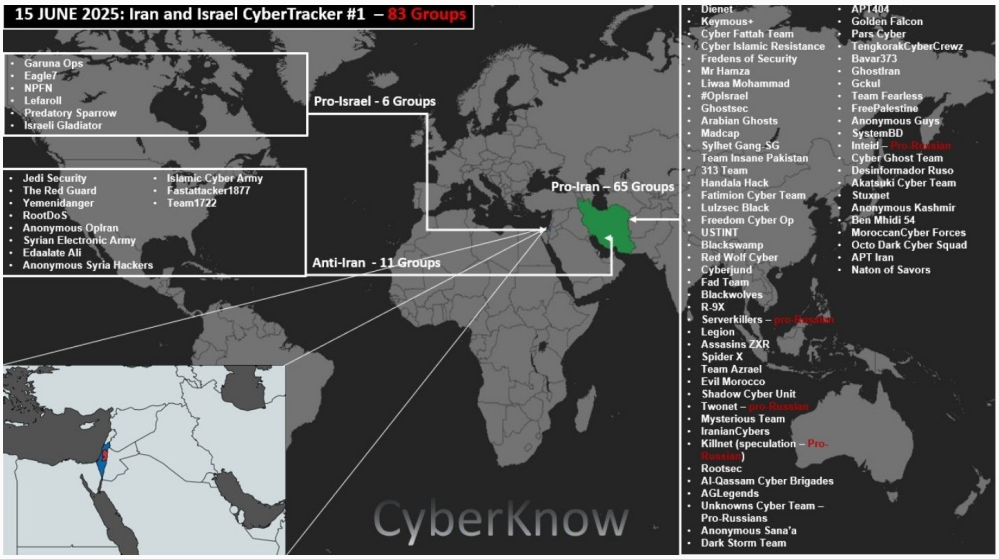


Figure 1: The Cyber groups spread in Israel-Irani cyberwarfare by Hacktivists Coalitions chart (https://x.com/Cyberknow20/status/1934258425590141193/photo/1)

Pro-Iran cyber coalitions include a mix of familiar names from past regional conflicts, APT404, Cyber Islamic Resistance, Al-Qassam Cyber Brigades, and Handala Hack, alongside dozens of lesser-known or newly emerged entities such as Evil_Byte, Fad Team, and SystemBD. Many of these groups previously appeared in the Hamas–Israel cyber conflict, demonstrating how cyber actors often recycle their branding and infrastructure across aligned ideological fronts. For instance, Al-Qassam Cyber Brigades and Cyber Fattah Team are active in both Hamas-linked operations and the broader Iranian cyber narrative, suggesting operational overlaps or even centralized coordination.

On the opposing side, the pro-Israel presence is notably small and more elite, featuring high-impact players like Predatory Sparrow, a group widely believed to be linked to Israeli intelligence operations, and Garuna Ops, known for surgical strikes against Iranian critical infrastructure. These groups appear more technically sophisticated but are fewer in number, operating more like specialized cyber units than crowd-sourced collectives.

The anti-Iran bloc, which may include Arab or neutral cyber groups, adds a unique layer to the conflict. Entities like Jedi Security and The Red Guard hint at broader opposition to the Iranian regime that extends beyond Israeli interests. Some of these actors previously targeted pro-Iran militias or operated during Arab Spring-related movements, showcasing the fluid allegiance and multi-conflict engagement of modern hacktivist entities.

This fragmented but ideologically charged coalition map echoes the cyber force alignments seen in the Russia–Ukraine conflict. Just as Ukraine benefited from loosely coordinated global support (e.g., Anonymous, IT Army of Ukraine), Israel finds backing in smaller but targeted cyber operations. Meanwhile, Iran's model resembles Russia's use of a broad, low-control cyber militia strategy, activating loosely affiliated actors like KillNet or NoName057(16) for widespread psychological and nuisance attacks, while keeping elite groups like Sandworm for high-impact intrusions.

In essence, the Israel-Iran cyber conflict reveals a hybrid threat model: a few state-linked actors embedded within a dense jungle of ideological, opportunistic, and proxy-driven cyber collectives. The recurring presence of familiar names across the Hamas–Israel and Israel-Iran conflicts underlines how cyber warfare has evolved into a networked ecosystem of reconfigurable threat actors, united more by shared enemies than by command structures. The blurring lines between patriotic hackers, ideological militants, and state proxies make attribution difficult, retaliation risky, and escalation more likely.

Pro-Israeli Cyber Activities

One of the most active Pro-Israeli cybergroups is Gonjeshke Darande, translated as Predatory Sparrow. It is a highly sophisticated and likely state-aligned cybergroup widely believed to be affiliated with Israeli intelligence. The group emerged publicly in 2021 and has since been linked to a series of precise, high impact cyberattacks against Iranian infrastructure, including fuel distribution systems, steel plants, and railway networks. Known for its advanced operational security, custom toolsets, and psychological messaging, Predatory Sparrow often accompanies its attacks with public statements in Persian and English, signaling both technical capability and narrative control. Its operations reflect a strategic focus on disruption, deterrence, and symbolic retaliation within the Israel-Iran cyberwarfare.

Data Exfiltration and Sharing

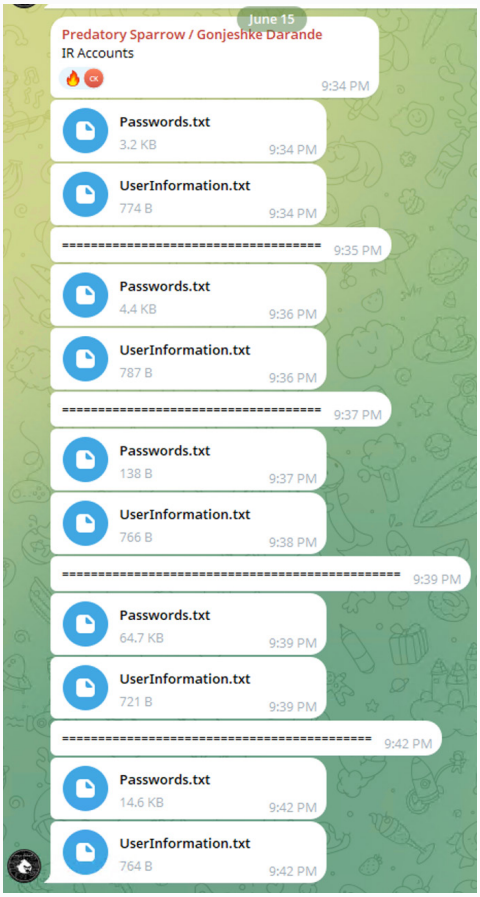
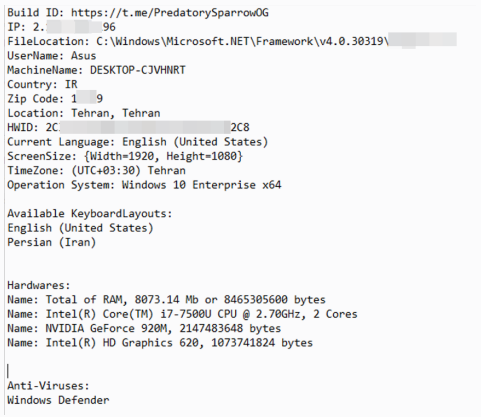


Figure 2: Predatory Sparrow (Gonjeshke Darande) introduces user data dumps in its Telegram channel

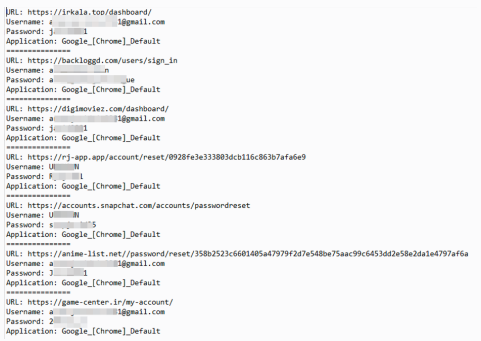
On June 15, the cybergroup Predatory Sparrow publicly released a series of data dumps allegedly exfiltrated from hacked Iranian users. The leak was shared in multiple parts, with each entry comprising two corresponding files: one detailing system-level user information, and the other containing browser credential data.



```
Build ID: https://t.me/PredatorySparrowOG
IP: 2.[redacted]96
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\[redacted]
UserName: Asus
MachineName: DESKTOP-CJVHNRT
Country: IR
Zip Code: 1[redacted]9
Location: Tehran, Tehran
HWID: 2C[redacted]2C8
Current Language: English (United States)
ScreenSize: {Width=1920, Height=1080}
TimeZone: (UTC+03:30) Tehran
Operation System: Windows 10 Enterprise x64

Available KeyboardLayouts:
English (United States)
Persian (Iran)


Hardwares:
Name: Total of RAM, 8073.14 Mb or 8465305600 bytes
Name: Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, 2 Cores
Name: NVIDIA GeForce 920M, 2147483648 bytes
Name: Intel(R) HD Graphics 620, 1073741824 bytes

Anti-Viruses:
Windows Defender
```

Figure 3: One of UserInformation files shared by the Predatory Sparrow cybergroup

The first file in each pair, labeled “UserInformation,” included technical metadata extracted from infected machines. This data featured IP addresses, hardware specifications, operating system details, screen resolutions, and other configuration markers, likely used for profiling or targeting purposes.



```
URL: https://irkala.top/dashboard/
Username: a[redacted]1@gmail.com
Password: j[redacted]1
Application: Google_[Chrome]_Default
==========
URL: https://backloggd.com/users/sign_in
Username: a[redacted]n
Password: a[redacted]ue
Application: Google_[Chrome]_Default
==========
URL: https://digimoviez.com/dashboard/
Username: a[redacted]1@gmail.com
Password: j[redacted]1
Application: Google_[Chrome]_Default
==========
URL: https://rj-app.app/account/reset/0928fe3e333803dcb116c863b7afa6e9
Username: U[redacted]N
Password: j[redacted]1
Application: Google_[Chrome]_Default
==========
URL: https://accounts.snapchat.com/accounts/passwordreset
Username: U[redacted]N
Password: s[redacted]5
Application: Google_[Chrome]_Default
==========
URL: https://anime-list.net//password/reset/358b2523c6601405a47979f2d7e548be75aac99c6453dd2e58e2da1e4797af6a
Username: a[redacted]1@gmail.com
Password: J[redacted]1
Application: Google_[Chrome]_Default
==========
URL: https://game-center.ir/my-account/
Username: a[redacted]1@gmail.com
Password: 2[redacted]
Application: Google_[Chrome]_Default
```

Figure 4: User credentials file shared by the cybergroup on its Telegram channel

The second file contained structured credential logs resembling output from common information-stealer malware. These files listed usernames, passwords, URLs of accessed services, and browser-specific parameters, strongly suggesting that the data was gathered via a credential stealer deployed on Iranian networks.

Similarly, the cybergroup released information about an individual they identified as a terrorist, referred to as Sunny Rise.

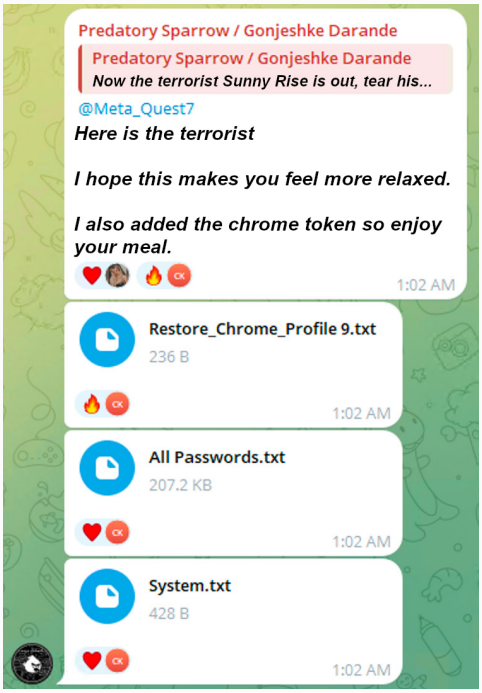


Figure 5: The Predatory Sparrow cybergroup shared user information including credentials and computer information on June 17

In the early hours of June 17, 2025, Predatory Sparrow released a new data dump on their Telegram channel, claiming it originated directly from Iran's Ministry of Communications. The group stated that, unlike previous leaks focused on social networks, this collection contains sensitive data tied to mobile infrastructure.

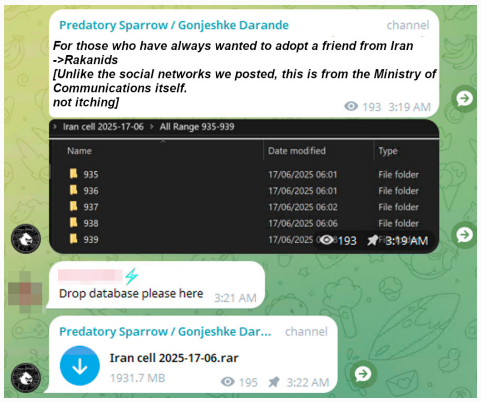


Figure 6: On June 17, Predatory Sparrow shared a database claimed to be obtained from the Iranian Ministry of Communications

The leaked archive, titled "Iran cell 2025-17-06.rar", is nearly 2 GB in size and includes five directories labeled numerically from 935 to 939, likely referencing Iranian mobile operator number ranges. A screenshot posted by the group shows the file structure and timestamps confirming recent extraction. While the contents have not been independently verified at the time of writing, the implication is clear: this leak may include telecommunications data, subscriber records, or metadata tied to Iranian cellular services.

Banking Disruption

On June 17, 2025, the cyber group Predatory Sparrow escalated its campaign against Iranian institutions by announcing a targeted cyberattack on Bank Sepah, one of Iran's oldest and most strategically important banks. Sepah Bank is allegedly associated with the Islamic Revolutionary Guard Corps (IRGC).

Figure 7: Predatory Sparrow's statement about the attack against Bank Sepah

In its public statement, the group claimed responsibility for disrupting the bank's operations, framing the action as a direct blow against what they described as a financial engine used by the Iranian government to fund terrorism, missile, and nuclear programs.

Unlike their earlier leaks focused on personal data or user device logs, this operation marked a clear shift toward strategic financial disruption.

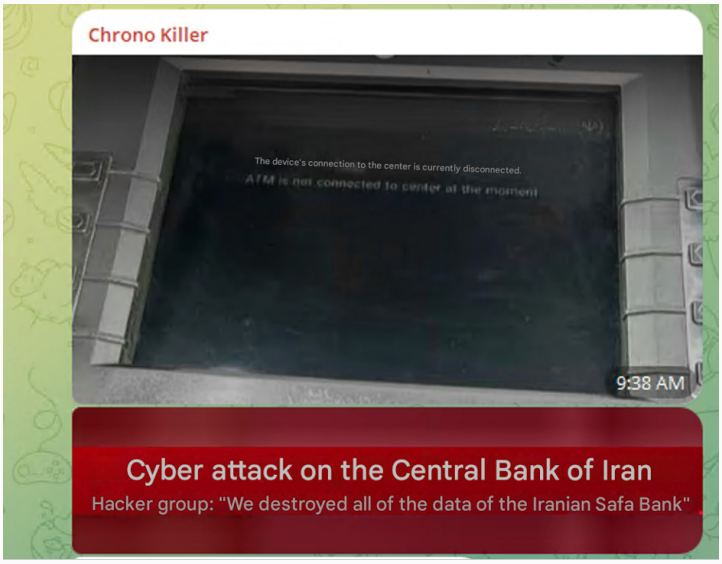


Figure 8: A screenshot of ATMs not operating in Iran (messages translated to English) from Predatory Sparrow's Telegram channel

Shortly after the group's post, Iranian users on social media began reporting widespread issues, including ATM outages, failed transactions, and inaccessible online banking services. Several independent media sources and Telegram channels confirmed that Bank Sepah's digital infrastructure was experiencing severe interruptions, affecting both personal and commercial users.

Breach of An Iranian Crypto-exchange

On June 18, the cyber group Predatory Sparrow (Gonjeshke Darande) issued a high-profile threat claiming responsibility for an attack on Nobitex, Iran's largest cryptocurrency exchange. In a statement shared, the group warned that it would release Nobitex's source code and internal data within 24 hours, placing all assets on the platform "at risk." The message emphasized that Nobitex is not just a civilian exchange, but a critical tool in the Iranian regime's alleged efforts to bypass sanctions and finance global terrorism.

Figure 9: Translated cybergroup statement claiming attack against Iranian cryptocurrency exchange

According to the group, Nobitex openly assists users in evading international sanctions and is treated by the regime as a key asset, so much so that working there is reportedly considered a valid substitute for military service. This rhetoric mirrors the group's earlier operation against Bank Sepah and makes clear that Predatory Sparrow is now systematically targeting what it sees as the financial backbone of Iran's regime, from traditional banks to decentralized crypto infrastructure.

The implications of these attacks are significant. Unlike temporary DDoS outages or limited data leaks, the compromise of financial infrastructure, especially one involved in sanction evasion and international crypto transactions, has the potential for far-reaching geopolitical and economic consequences. It raises the stakes of cyberwarfare into the realm of financial warfare, targeting systems that enable the Iran resilience amid global isolation.

Pro-Iranian Cyber Activities

Pro-Iranian cyber groups have emerged as a powerful and persistent force in the digital battlegrounds of the Middle East and beyond. Operating under a mix of ideological, political, and strategic motivations, these actors form a diverse ecosystem of state-aligned APTs, proxy militias, and hacktivist collectives. While some operate with clear connections to Iranian intelligence or military structures, others act independently but align closely with Tehran's geopolitical agenda, particularly in its confrontations with Israel, the United States, and Sunni-aligned regimes.

Figure 10: Cybergroup BD Anonymous made a statement highlighting that they support Iran in thisThis cyberwarfare

These groups engage in a wide range of cyber activities, including espionage, sabotage, disinformation, and psychological operations. Their campaigns frequently target critical infrastructure, private companies, government networks, and civilian services, aiming to destabilize, retaliate, or assert influence. Notably, many of these actors appear repeatedly in regional conflicts such as the Hamas–Israel war or wider anti-Western campaigns, leveraging shared infrastructure, malware tools, and ideological messaging to amplify Iran's strategic reach in cyberspace.

Handala's Hacking Claims

On June 14, following a dramatic escalation in Israeli airstrikes against Iranian facilities, the pro-Palestinian, pro-Iranian hacktivist collective Handala re-emerged, asserting a series of high-value cyber intrusions.

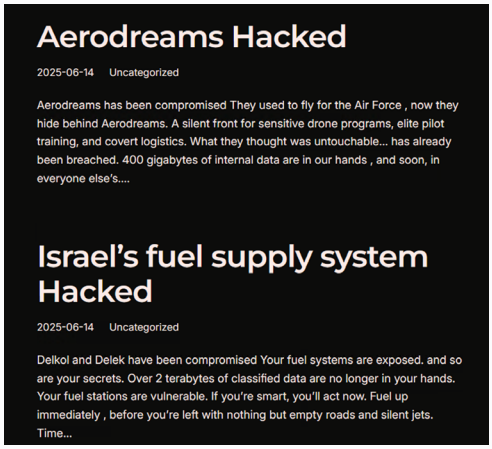


Figure 11: Handala's claims from June 14th

Handala claimed it exfiltrated over 2 TB of data from Israeli firms between of June 14–15. Notable alleged victims included the Delek Group and its subsidiary Delkol, with Handala purporting to have stolen sensitive information involving the company's military partnerships. Notable alleged victims included the oil provider Delek Group and its subsidiary Delkol, with Handala purporting to have stolen sensitive information involving the company's military partnerships. The group also asserted breaches of Y.G. New Idan, 099 Telecommunications, and AeroDreams, an Argentinian drone firm linked by Handala to the Israeli Air Force.

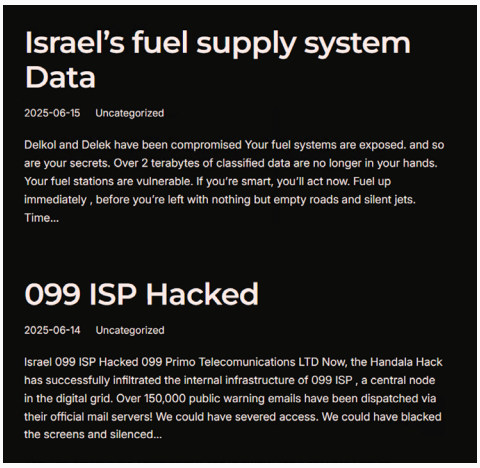


Figure 12: Handala claims hack into 099 Telecommunication provider and again to the already mentioned victim Delek

As proof, Handala released multiple archived files, though only "a dozen" 4 GB archives were made publicly available.

Victim responses and verification, at the time of this report's posting:

- Delek Group / Delkol: No public acknowledgment has been issued by the companies. According to some sources, the information was recycled from older breaches.
- Y.G. New Idan, 099 Primo Communications, and AeroDreams: None of these organizations have released any statements or regulatory disclosures concerning breaches or data compromise.
- Israeli Cyber Directorate / Security Establishment: As of the time of posting, no official confirmation or denial regarding these June claims has been made public.

Handala's latest claims align with a recognizable pattern: high-volume data exfiltration assertions followed by limited proof, often involving partial archives rather than comprehensive datasets.

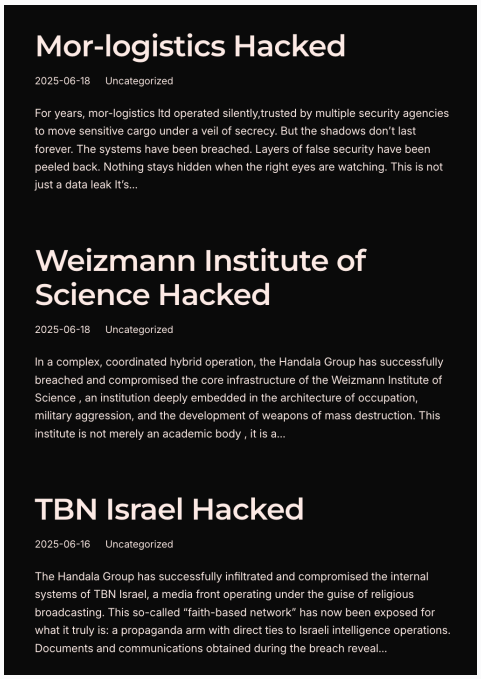


Figure 13: Handala's latest postspost on itsit page by the time of writing this blog

At present, the absence of authoritative confirmation, neither from companies, Israeli authorities, nor independent cybersecurity firms, indicates that these claims remain unverified. Yet they effectively amplify psychological impact and thrust Handala into the public narrative, sustaining its relevance during a peak phase of the Israel–Iran cyber escalation. Probably what they want to achieve.

While the technical substance of Handala's June declarations remains uncorroborated, the timing and thematic resonance are consistent with both real cyberattacks and influence-based operations. In the current environment, separating technical truth from strategic theater is increasingly complex, and Handala appears to be adept at navigating both.

DDoS Attacks

In the Israel-Iran cyber conflict, DDoS attacks have become a central tactic used by pro-Iranian groups to create disruption and psychological pressure, particularly when timed with political or military escalations. Since 2024, waves of such attacks have targeted Israeli government sites, banks, hospitals, and media platforms.

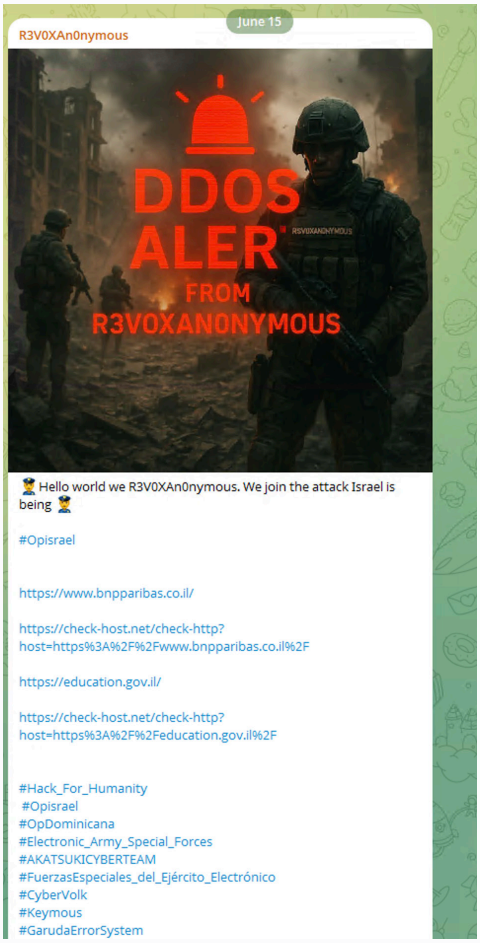


Figure 14: Pro-Iranian cybergroup joins DDoS attacks against Israel, listing other members of the joint operations

A key evolution in this phase is the coordination among smaller hacktivist groups, which now operate under umbrella identities like the Cyber Islamic Resistance or United Cyber Front for Palestine and Iran. These loosely affiliated "cyber unions" share resources and synchronize campaigns, amplifying their impact despite limited technical sophistication.

This trend mirrors the Hamas–Israel and Russia–Ukraine conflicts, where decentralized actors banded together for greater visibility. Though many DDoS attacks have limited lasting effect, their volume, coordination, and media amplification reinforce Iran's influence through persistent digital harassment of Israeli infrastructure.

Claimed Attacks on Public Infrastructure

DieNet has emerged as one of the more visible and vocal hacktivist groups in the ongoing cyber conflict between Iran and Israel. Actively conducting DDoS attacks against Israeli infrastructure, DieNet publicly declared its support for the Iranian side in the cyberwar, framing its operations as part of a broader ideological and geopolitical resistance against what it labels "Zionist aggression". The group has targeted a variety of Israeli systems, often coordinating its actions with statements on Telegram and other hacktivist-friendly platforms.

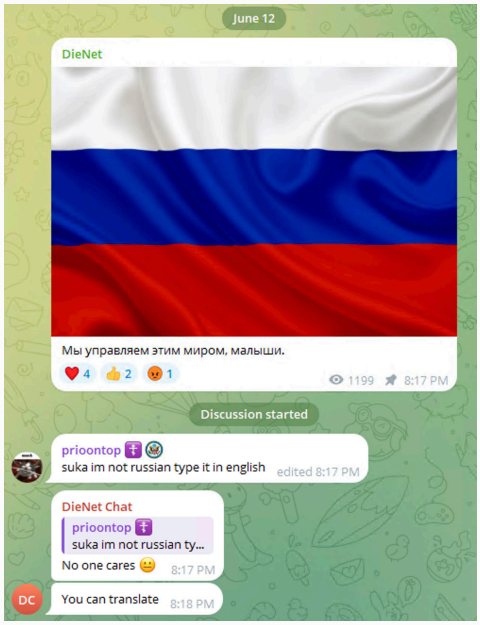


Figure 15: A statement from DieNet suggesting it has some Russian-speaking participants

What distinguishes DieNet from many other pro-Iranian actors is its hybrid identity: while it operates under a pro-Iranian and pro-Hamas narrative, there is mounting evidence of its Russian-speaking members and technical connections to cyber communities in Eastern Europe. Linguistic analysis of DieNet's messages,

as well as timestamps, metadata, and interaction pattern, suggests that at least part of the group communicates internally in Russian or uses Slavic-language resources. This points to the broader phenomenon of cross-regional cyber collaboration, where ideological alignment overrides geographic or national boundaries.

Figure 16: DieNet statement showing its preference in the Israel-Iranian cyberwarfare

Another notable feature is DieNet's visual branding, particularly its logo, which closely resembles that of KillNetKillNet, the infamous pro-Russian DDoS collective involved in cyberattacks on Western nations during the Russia–Ukraine war. The aesthetic similarity may be deliberate, either to signal ideological alignment, confuse attribution, or simply capitalize on KillNet'sKillNet's notoriety. Such mimicry is common in the hacktivist ecosystem, where branding, messaging, and even malware payloads are often recycled or rebranded across different regional conflicts.

DieNet's role in the Israel-Iran cyber crisis illustrates the growing interoperability among ideologically aligned cyber groups, even when they hail from different geopolitical environments. Much like how Russian hacktivist groups have provided loose coordination or inspiration for actors in the Middle East and Asia, DieNet appears to act as a bridge node, connecting the Iranian cyber axis, Palestinian militant cyber actors, and Russian-speaking cybercrime or hacktivist circles.

Their activities are consistent with tactical DDoS warfare: not highly advanced but disruptive enough to cause temporary outages, trigger public concern, and generate media coverage. DieNet's attacks often coincide with physical escalation on the ground, such as IDF strikes in Gaza or IRGC operations abroad, suggesting the group is at least loosely aligned with the timing and objectives of state-linked campaigns.

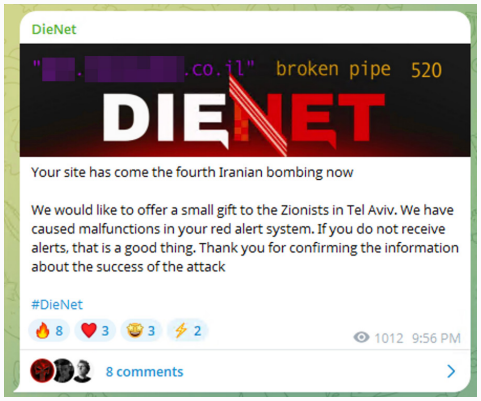


Figure 17: On June 15th DieNet claims to compromise Red Alert systems of Israel

During the current wave of cyber hostilities, DieNet have claimed DDoS attacks targeting Israel's alerting applications which are designed to warn civilians of incoming missile attacks. These claims are often amplified on Telegram and social media with the intent to sow fear or project disruption. However, as of the time of writing, there is no verified evidence that Israel's early warning systems have been successfully compromised or disrupted by these cyberattacks. While attempts may have been made, the Israeli alerting systems appear to have remained operational, underscoring the distinction between propaganda-driven claims and real-world impact in the cyber domain.

DieNet is a prominent example of transnational hacktivism in the Israel-Iran cyber conflict, a group that blends pro-Iranian rhetoric, pro-Hamas alignment, visual cues from Russian cyber groups, and operational tactics suited for fast, noisy disruption. Its existence reinforces the idea that cyberwarfare in 2025 is no longer defined by national borders alone but by dynamic, ideological alliances operating across continents and languages.

False Alerts

As part of an intensifying campaign of hybrid warfare, Iranian-linked cyber groups have begun disseminating fake emergency alerts to Israeli civilians, exploiting SMS spoofing, push notification systems, and messaging apps to spread false security warnings. These messages, designed to imitate official government alerts, often contain alarming disinformation, such as warnings of imminent Iranian airstrikes, instructions to evacuate bomb shelters, or claims that remaining in shelters places civilians in greater danger.

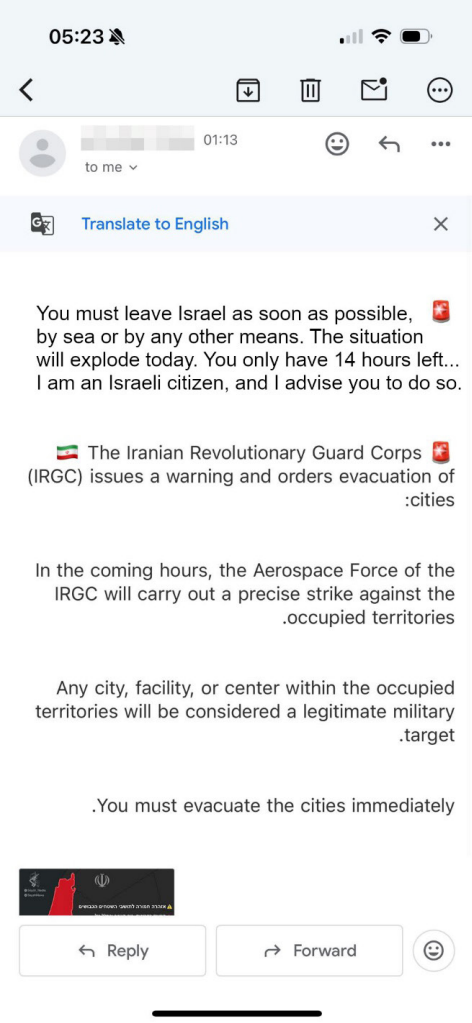


Figure 18: A translated screenshot from one of the Israeli phones receiving fake alert messages

This tactic represents a deliberate psychological operation, aiming to instill fear, create confusion, and erode trust in Israel's public alerting systems. By mimicking the authoritative tone and format of official warnings, attackers seek to bypass rational skepticism and trigger emotional, fear-based reactions. These efforts not only endanger individuals who might act on false instructions but also aim to undermine public confidence in legitimate civil defense infrastructure, which plays a critical role during times of conflict.

Such disinformation campaigns are a classic element of information warfare, where the goal is not technical damage but societal disruption. By blurring the lines between real and fake alerts, these operations attempt to paralyze response systems, overburden emergency services, and create psychological fatigue among the population. The tactic mirrors similar efforts seen in Russian operations against Ukraine, where fake evacuation orders and doctored media were used to manipulate civilian behavior.

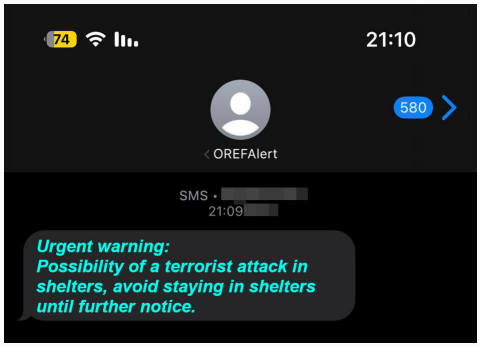


Figure 19: A translation of an SMS received by one of the Israeli phones, calling Israelis to Leave Their Shelters

From an operational standpoint, these messages are typically broadcast through mass SMS platforms, spoofed sender IDs, or hacked community messaging apps. In some cases, targeting is highly localized, suggesting the use of previously leaked citizen databases or mobile geolocation tools. Fake alert campaigns are a strategic extension of Iranian cyber doctrine, aimed at destabilizing the Israeli civilian front, distracting from kinetic operations, and weakening societal resilience. As cyberwarfare continues to evolve beyond infrastructure into the cognitive and emotional domains, these manipulative tactics underscore the growing threat of non-technical but highly impactful digital influence operations.

Fake Data Leaking

In the midst of intensifying cyber activity between Israel and Iran, a large-scale Israeli-related data leak has surfaced on a Dark Web forum, raising concerns not necessarily for its origin, but for its potential impact within the broader influence and psychological dimensions of cyber warfare. The individual who posted the dataset did not attribute it to any specific political or ideological motive. However, the mere appearance of such an extensive collection of Israeli-linked user data, especially during a period of heightened geopolitical tension, is enough to draw serious attention from threat actors and media alike.

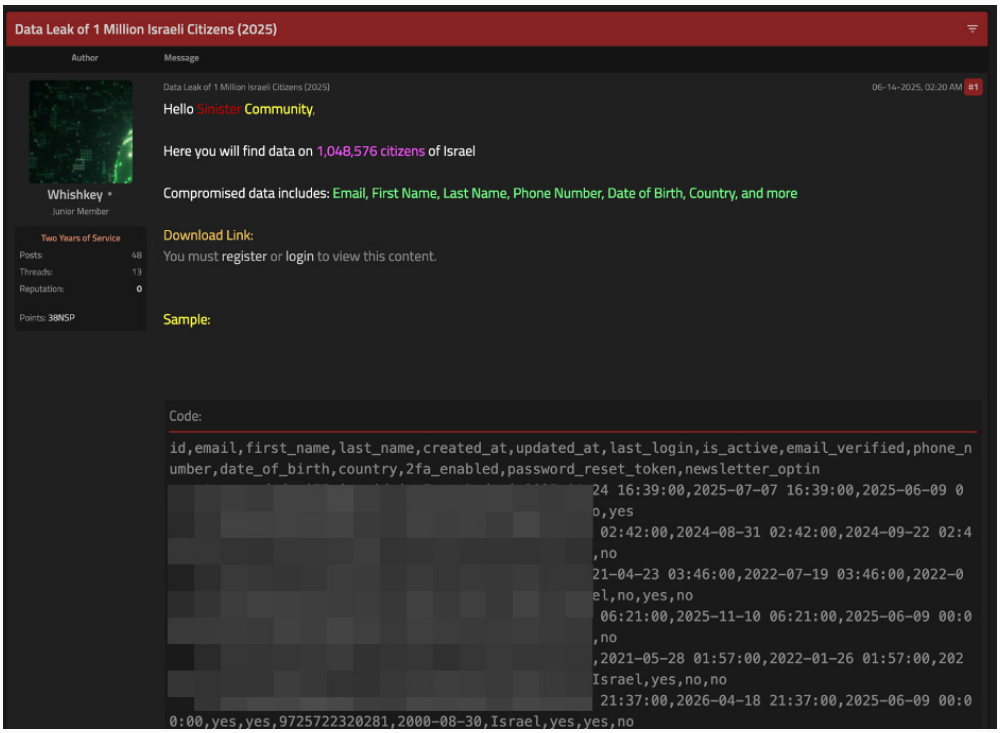


Figure 20: The actor shares more than one million records claimed to be related to Israeli citizens on the Dark Web forum.

The dataset, once downloaded and reviewed, contained 1,048,576 rows, of which 1,034,750 were found to be unique records. Upon further analysis, a highly unusual pattern emerged. The records were distributed across 10 different domains, each of which claimed roughly 10% of the total dataset. This perfectly even distribution strongly suggests automated generation or structured planting, rather than natural data aggregation resulting from a breach of a real-world system.

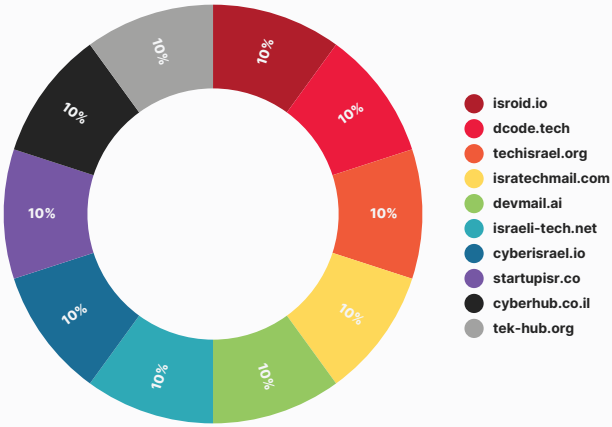


Figure 21: The domain names distribution among the records from the downloaded file advertised by the actor

A cross-check of the ten domains revealed that none were currently parked, active, or resolving through standard DNS queries. Their absence from domain registries and web infrastructure indexes further reinforces the theory that they may have been fabricated as part of a synthetic data set or at least anonymized via an automated domain masking technique. Such techniques are sometimes used to obfuscate original sources or to create the illusion of a broader attack surface than exists.

In this context, it's crucial to view such events through a wider lens. Not every breach is tactical, some are theatrical. As with many aspects of modern cyber conflict, the perception of compromise can be as potent as compromise itself. Whether authentic or partially fabricated, such leaks play into a larger psychological and media-driven layer of cyber warfare, especially relevant in the Israel–Iran narrative, where strategic information placement is often weaponized.

Following a series of accurate Israeli attacks on senior commanders, officials and nuclear scientists, the Iranian government has issued strict warnings to its officials, military personnel, and security staff regarding the use of mobile phones and digital devices. According to Iranian and Israeli media sources, Iran's Cybersecurity Command instructed functionaries to avoid using smartphones, laptops, smartwatches, and any internet-connected devices, particularly those linked to public networks. Officials were told to either switch off these devices entirely or replace them with secure, tamper-resistant alternatives.

These measures are based on growing concerns that Israeli intelligence units are leveraging mobile technologies to track, geolocate, and potentially target Iranian officials. Reports suggest that similar tracking techniques have been used in the past to assassinate senior figures, including nuclear scientists. By restricting digital device usage, Iran aims to deny adversaries access to location data, communication metadata, or personal movement patterns that could aid surveillance or attacks.

Operationally, the restrictions are designed to enhance security by minimizing digital exposure, but they will likelyalso complicate internal communications and logistics. The decision signals a deepening of Iran's defensive cyber posture, reflecting fears that cyber intrusions could directly translate into physical threats. It also aligns with Iran's broader strategy of limiting digital vulnerabilities, echoing past actions such as app bans and nationwide internet shutdowns during periods of political unrest. These developments underscore how cyber and physical security are increasingly intertwined in the Iran-Israel conflict.

Cross-Conflict Similarities in Cyber Warfare

While the geopolitical contexts of the Israel-Iran, Hamas–Israel, and Russia–Ukraine conflicts differ significantly, the cyber warfare strategies employed across these arenas reveal striking parallels. Each conflict demonstrates how cyber operations have become an integral tool of modern statecraft and hybrid warfare, used to supplement kinetic actions, influence public perception, and disrupt critical infrastructure.

A key similarity lies in the integration of cyberattacks with broader military campaigns. In the Hamas–Israel and Russia–Ukraine conflicts, cyber operations often precede or accompany missile strikes, disinformation campaigns, or major military escalations

For example, after the October 7, 2023 conflict between Hamas and Israel, cyber offensives targeting Israeli alerting systems, infrastructure, and media were tightly coordinated with physical rocket attacks. Similarly, Russia used cyberattacks as a preparatory phase in its military campaign against Ukraine, targeting power grids, government portals, satellite communications, and local news outlets to create confusion and reduce defensive coordination.

Another shared characteristic is the targeting of civilian infrastructure to create psychological pressure. Iranian-linked groups, like MuddyWater and APT34, have attacked Israeli water systems and transport networks. Hamas-affiliated groups have tried to disrupt emergency response systems and public broadcasting. In Ukraine, Russian threat actors such as Sandworm and APT28 have aimed to paralyze hospitals, railways, and energy providers. In each case, the line between combatants and civilian targets is intentionally blurred, a hallmark of hybrid warfare doctrine.

The reuse and recycling of threat actor identities and infrastructure is another point of overlap. Several groups first observed in the Hamas–Israel cyber theater, such as Gaza Cybergang, APT-C-23 (AridViper), and entities under the Cyber Av3ngers or Storm-1133 labels, have also been detected in operations linked to Iranian interests. These actors often exhibit technical, linguistic, and operational patterns consistent with Iranian cyber doctrine, suggesting either direct coordination or shared resources. The blurred affiliations raise questions about centralized versus distributed command in the cyber arms of proxy forces. In some instances, these groups operate under local branding (e.g., “al-Qassam Cyber Brigades”) but use malware and infrastructure observed in broader Iranian operations.

This proxy model resembles Russia’s use of loosely affiliated or state-nurtured hacking groups such as KillNet, Sandworm, and UNC1151, which operate in tandem with official military units or intelligence objectives. Iran and Russia rely on cyber militias and plausible deniability, allowing them to engage in aggressive operations while disavowing direct responsibility. These groups often communicate through Telegram channels or low-tier forums, coordinating campaigns that blur the line between activism, cybercrime, and state-sponsored sabotage.

Finally, all three conflicts feature a strong disinformation component, with cyber operations aimed not only at infrastructure but also at influencing the public narrative. In the Israel-Iran and Hamas–Israel contexts, this has included website defacements, propaganda videos, and false-flag attacks. In Russia’s war on Ukraine, the manipulation of news, social media bots, and fabricated leaks has reached an industrial scale.

The cyber warfare patterns across these three conflicts show a convergence of doctrine: preemptive attacks on civilian systems, characterized by proxy actor deployment, coordinated cyber-physical strategies, and narrative control. Many of the threat groups observed in the Hamas–Israel conflict operate as extensions or affiliates of Iranian cyber strategy, while both Iran and Russia demonstrate similar preferences for ambiguity, disruption, and information warfare, signaling a global normalization of hybrid cyber conflict.

Many of the threat groups observed in the Hamas–Israel conflict, operate as extensions or affiliates of Iranian cyber strategy, while both Iran and Russia demonstrate similar preferences for ambiguity, disruption, and information warfare, signaling a global normalization of hybrid cyber conflict.

Summary

Though most of the attacks Spiderlabs has observed have been restricted to Israel and Iran, companies, institutions, and governments beyond the region should maintain a heightened level of caution as this conflict progresses. As mentioned above, the balance of hacktivists is largely in the pro-Iranian camp, and because these are non-state actors, they often cast a wide net for targets.

Anyone perceived as being supportive of one side or another in this conflict may become a potential target. With reports of the US government increasingly aligning itself with Israel, US and Western companies should be on high alert. This is particularly the case for those with US government business, as the example of an Argentine company with Israeli defense ties mentioned in this report shows.

Organizations globally, including those in the US, Australia, and the UK, must recognize that this digital conflict poses a tangible risk. Even without direct involvement, threat actors often exploit heightened global awareness to enhance social engineering and phishing attacks, making vigilance crucial for all sectors, particularly critical infrastructure, defense, and government.

While Iranian-backed groups exhibit a higher volume of activity, pro-Israel entities demonstrate elite, surgical strike capabilities. Organizations in these Western nations should implement robust cybersecurity hygiene, including updated patches, MFA, restricted access, and strong incident response plans, as well as prepare for soft cyber operations like fake emergency alerts to defend against potential collateral damage and maintain resilience.

Remediations

Remediation Measures Against Israel-Iran Cyberwarfare Threats

DDoS Attacks on Government, Finance, and Infrastructure

- Adopt Always-On DDoS Protection: Partner with CDN and security providers to deploy automatic traffic filtering, geo-fencing, and rate-limiting, especially for critical infrastructure and banking services.
- Redundancy and Failover Networks: Ensure national and sectoral websites can be quickly mirrored or rerouted to backup environments.
- Simulation and Drills: Regularly simulate DDoS events to test real-time response coordination across public and private sector stakeholders.

Data Leaks and Identity Theft

- Automated Data Leak Detection: Monitor paste sites, Telegram channels, and dark web markets for signs of leaked Israeli datasets.
- Citizen Alert Mechanisms: Notify potentially exposed individuals and organizations through secure government platforms and recommend immediate password hygiene measures.
- Metadata Forensics: Trace patterns in leaked datasets (e.g., domain clustering, distribution anomalies) to detect fabricated or influence-driven "leaks."

Critical Infrastructure Intrusions (Water, Energy, Healthcare)

- Segment Operational Technology (OT) Networks: Physically and logically separate industrial control systems from external-facing IT networks.
- 24/7 SOC Monitoring: Expand real-time threat detection using behavioral analytics and anomaly detection tailored to SCADA and ICS environments.
- Mandatory Reporting Framework: Enforce rapid breach disclosure for utilities and industrial sectors to ensure timely government response.

Hacktivist Campaigns and Defacement

- Real-Time Web Monitoring and Auto-Restore Tools: Implement website monitoring with instant rollback capabilities to restore defaced or disabled sites.
- DNS Hardening: Secure domain records against hijacking and implement DNSSEC to ensure integrity of online assets.
- Brand Defense Programs: Monitor open channels for impersonation or fake branding of entities used in social engineering or media manipulation.Brand Defense Programs: Monitor open channels for impersonation or fake branding of entities used in social engineering or media manipulation.

Cross-Sector Coordination

- Joint Cyber Coordination Units: Maintain regular threat intel exchanges between military, civilian, and commercial cyber defense teams (e.g., MoD, CERT-IL, financial ISACs).
- Nationwide Incident War-Gaming: Simulate a coordinated cyber-physical attack (e.g., DDoS + misinformation + infrastructure disruption) to test inter-agency resilience.

The Israeli-Iranian cyber conflict is characterized by a mix of advanced state-sponsored intrusions, ideologically driven hacktivism, and psychological warfare. Effective remediation requires a layered defense approach, combining technical controls, operational readiness, and public resilience. Israel's advanced cyber posture provides a strong foundation, but maintaining it under sustained pressure requires constant adaptation, visibility, and cross-sector trust.

Remediation Measures Against Psychological Operations

Strengthen Authentication of Official Alerts

Implement end-to-end digital signature mechanisms on emergency messages (e.g., SMS, app-based, or cell broadcast) to help civilians verify authenticity. Public awareness campaigns should explain how to identify signed or certified messages from the government.

Harden Civil Alert Infrastructure

Review and upgrade security protocols for all systems used to generate and distribute emergency communications, especially municipal apps, local broadcast platforms, and mass notification APIs. Multi-factor access controls and regular penetration testing should be enforced.

Real-Time Monitoring and Takedown Response

Establish a dedicated national task force to monitor fake alerts and rapidly issue counter-notifications debunking disinformation in real time. Partnerships with telecom providers and social platforms are critical for swift takedown and warning dissemination.

Public Education and Resilience Campaigns

Equip the public with tools to critically evaluate emergency messages, what official alerts look like, how to verify them, and where to turn in case of doubt. Messaging should reinforce "verify before you act" behavior during crises.

Telecom and SMS Provider Collaboration

Work with domestic and global SMS aggregators to block spoofed sender IDs mimicking emergency services. Consider implementing country-wide sender ID whitelisting for critical alerts, especially during periods of military escalation.

Behavioral Simulation & Training

Conduct simulated drills involving fake alerts as part of cyber-psychological resilience exercises, helping communities and emergency services recognize, contain, and report such incidents without panic.

Leverage Threat Intelligence Sharing

Integrate this threat type into Israel's broader cyber threat intelligence frameworks. Sharing real-time indicators of spoofing, phishing, or disinformation methods with CERTs, security vendors, and allies helps detect patterns early.

Legal and Diplomatic Measures

Explore legal tools to sanction or disrupt infrastructure used in these influence campaigns, especially when linked to foreign actors. This includes targeted takedowns, coordinated reporting, and pressure on jurisdictions hosting malicious platforms.

These recommendations aim not only to defend technical systems but also to build societal resilience against cognitive and emotional manipulation, which is the core objective of such cyber-psychological operations.