

§



Israel-Iran War Cyber and Electronic Warfare Operations



From Shadows to Escalation: Overview and Analysis of Cyber and Electronic Operations as part of the Israel-Iran Conflict.

By Jeremy Makowski
Cyber Crime and Terrorism Intelligence Expert

June 2025

Table of Contents

1. Cyber Geopolitical Context 3
    1.1 Historical Context and Strategic Posture 3
    1.2 Since June 13, 2025 4
2. Cyber Forces in Presence, Strategy, and Capabilities 6
    2.1 Israel's Cyber Strategy: Doctrine, Capabilities, and Operations 6
        2.1.1 Strategic and Operational Overview of Israel's Cyber Activities 6
        2.1.2 Israel's Cyber Forces and Affiliates 6
        2.1.3 Recent Cyber incidents linked to pro-Israel hacking groups 12
        2.1.4 Contracting Ecosystem 14
        2.1.5 Operational Objectives and Tactics 14
    2.2 Iran's Cyber Strategy: Doctrine, Capabilities, and Operations 15
        2.2.1 Strategic and Operational Overview of Iran's Cyber Activities 15
        2.2.2 Iran's Cyber Forces and Affiliates 15
        2.2.3 Recent Cyber incidents linked to pro-Iran hacking groups 21
        2.2.4 Contracting Ecosystem 21
        2.2.5 Operational Objectives and Tactics 22
3. Electronic Warfare Operations 23
    3.1 Israel's Electronic Warfare Efforts 24
        3.1.1 Blocking Enemy Signals (Spectrum Denial & Jamming) 24
        3.1.2 Drone-Based EW Operations 24
    3.2 Iran's Electronic Warfare Response 24
        3.2.1 Defensive Jamming and Spoofing 24
4. Conclusion 25
5. About The Author 27
6. References 28

1. Cyber Geopolitical Context

1.1 Historical Context and Strategic Posture

For over a decade, the cyber domain has emerged as a critical and increasingly central theater in the protracted shadow war between Iran and Israel. This virtual battleground reflects their entrenched geopolitical rivalry, contrasting strategic cultures, and asymmetrical power dynamics. At the heart of this confrontation lies a deeply rooted ideological conflict, with Israel viewing Iran as an existential threat due to its nuclear ambitions and support for proxy groups such as Hezbollah. At the same time, Tehran perceives Israel as a Western-backed regional aggressor determined to curtail its influence.

Both states have recognized the strategic utility of cyberspace as a domain of modern statecraft offering relatively low entry costs, high potential returns, and, crucially, the veil of deniability. Israel, leveraging its world-renowned tech ecosystem and elite military cyber units, most notably Unit 8200, has pursued a doctrine centered on precision and preemption. Its cyber operations are typically intelligence-led, highly targeted, and geared toward neutralizing perceived existential threats. This was most clearly demonstrated in the landmark Stuxnet operation widely attributed to Israeli and U.S. collaboration, which physically disrupted Iran's uranium enrichment capabilities at Natanz. Israeli cyber tactics often reflect a strategy of disruption over destruction, aimed at degrading Iran's critical infrastructure, delaying its nuclear timeline, and sending strategic deterrent signals without provoking open conflict.

In contrast, Iran, constrained by technological and economic limitations, has adopted a more diffuse and often opportunistic cyber strategy. Its cyber apparatus comprises a mix of formal state actors such as the Islamic Revolutionary Guard Corps (IRGC), advanced persistent threat groups like APT34 (also known as OilRig), informal cyber militias, and ideologically motivated hackers. Rather than focusing solely on high-value military or nuclear targets, Iran's cyber strategy has increasingly embraced asymmetric disruption, targeting Israeli civilian infrastructure, including water utilities, transportation systems, and financial institutions. These attacks aim to sow public fear, create political pressure, and challenge Israel's domestic resilience. Moreover, Iran has been prolific in leveraging cyber tools for influence operations, engaging in online disinformation campaigns, psychological operations, and attempts to exacerbate social divisions within Israel and the broader region.

Cyberspace is an ideal theater for both nations because of its unique strategic attributes. It enables operations to remain in the "gray zone" below the threshold of kinetic warfare, allowing each side to inflict damage, assert influence, or retaliate without crossing red lines that might trigger a conventional military response. The inherent difficulty of attribution in cyberattacks provides Iran and Israel with plausible deniability, which is critical in managing escalation and controlling the international narrative. Furthermore, cyber conflict is key in signaling resolve and technological prowess to domestic audiences and global actors alike.

Ultimately, the Iran-Israel cyber conflict represents a broader evolution in 21st-century warfare where digital capabilities increasingly supplement traditional power projection, and where deterrence and coercion are exercised not just through missiles and tanks, but through malware and manipulated data streams. As both nations continue to invest in and refine their cyber arsenals, this domain will remain a volatile and strategic frontline, with implications for regional security and the evolving norms of international cyber conflict.

1.2 Since June 13, 2025

This ongoing cyber confrontation escalated significantly following Israel's June 13, 2025, launch of "Operation Rising Lion," which combined kinetic strikes on Iranian military infrastructure with a surge in digital offensives. In the weeks since, Israel-linked cyber groups, most notably "Predatory Sparrow," have intensified attacks on Iranian financial institutions and digital assets, reportedly wiping out millions in cryptocurrency and disrupting banking operations tied to the IRGC. These acts were designed not only to degrade financial resilience but to signal Israel's reach deep into Iran's digital economy. In retaliation, Iran has mobilized its cyber units and affiliated proxies to launch distributed denial-of-service (DDoS) campaigns and attempted cyber intrusions against Israeli power grids, rail systems, and government databases. Tehran has also escalated its domestic internet censorship and throttling mechanisms, aiming to shield internal networks and limit the external visibility of damage. Compounding the threat, Iran has strengthened cyber cooperation with Russia and China, seeking advanced technologies and evasion tactics to enhance resilience. Since June 13, both sides have also drawn support from hacktivist groups, but with a marked imbalance: pro-Israel digital actors have vastly outnumbered their pro-Iranian counterparts, conducting a broader array of operations with more sophisticated capabilities. As documented by open-source intelligence monitors such as the X account *@Cyberknow20*, the cyber battleground has been flooded with independent actors amplifying state objectives, further blurring the line between national operations and decentralized digital warfare (Figure 1).

With both nations openly embedding cyber operations into their military doctrines, cyberspace has evolved from a shadow theater into a primary front where the risks of escalation, miscalculation, and spillover into physical conflict are more acute than ever.

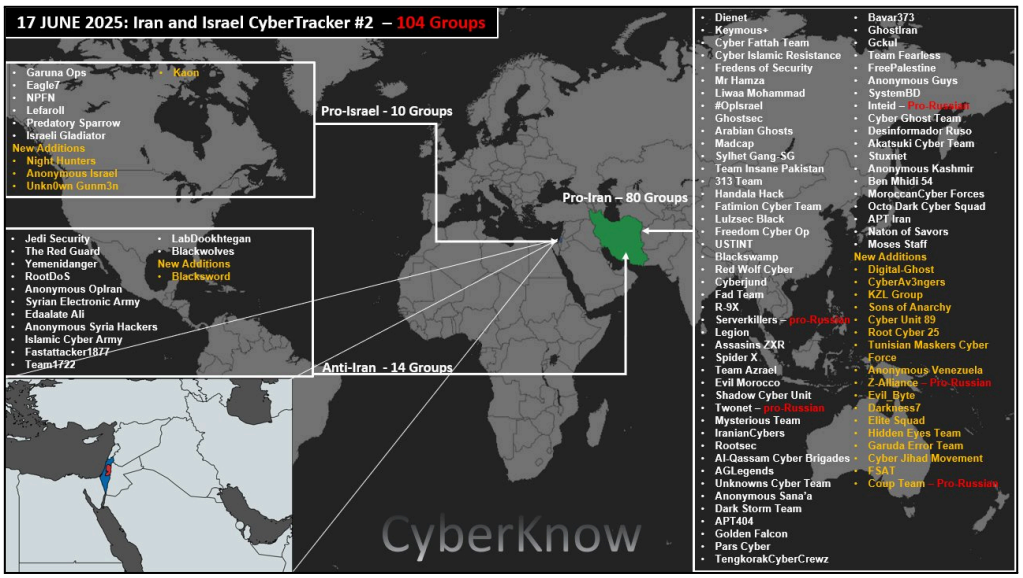


Figure 1 - Israel- Iran threat actors mapping (Source: CyberKnow)

Beyond the purely cyber aspect, both sides launched highly coordinated electronic warfare (EW) and cyberwarfare campaigns aimed at disrupting, degrading, and neutralizing each other's military operations and critical infrastructure. These efforts involved jamming communications and navigation systems, radar interference, and the deployment of electromagnetic pulses (EMP) to impair battlefield awareness and command and control capabilities. At the same time, cyberattacks targeted government networks, military databases, power grids, financial systems, and civilian communications platforms, with the aim of sowing confusion, gathering intelligence, and crippling logistical support. The integration of EW and cyberwarfare operations created a contested and unstable digital environment, where dominance of the electromagnetic spectrum and cyberspace became as crucial as air or land superiority.

2. Cyber Forces in Presence, Strategy, and Capabilities

2.1 Israel's Cyber Strategy: Doctrine, Capabilities, and Operations

2.1.1 Strategic and Operational Overview of Israel's Cyber Activities

Israel's cyber strategy is deeply rooted in its national security doctrine, prioritizing preemption, intelligence superiority, and strategic deterrence. Given the persistent threats from regional adversaries such as Iran, Hezbollah, and Hamas, as well as broader global cyber threats, Israel has developed a proactive and integrated cyber posture. The nation treats cyberspace as a key domain of warfare, on par with air, land, sea, and space. The 2017 launch of Israel's National Cyber Directorate (INCD) unified civil and military cyber efforts, establishing a doctrine that blends offensive capabilities with robust national defense. Strategic cyber activities range from infrastructure protection and cyber threat intelligence (CTI) sharing to coordinated offensive campaigns designed to degrade adversary command and control systems or disrupt critical infrastructure. This strategy is also tied to broader geopolitical objectives, including counterterrorism, surveillance, and the containment of regional actors via clandestine and hybrid warfare methods.

2.1.2 Israel's Cyber Forces and Affiliates

Israel has established itself as a global leader in cybersecurity by integrating cyberspace across its national infrastructure, both military and civilian. The country operates a complex ecosystem of cyber entities, including the following:

- **Israel Military Intelligence (Aman)**, the intelligence branch of the Israel Defense Forces, is responsible for strategic intelligence collection, analysis, and operations, and it commands some of the most elite cyber units in the world. Aman's two most notable cyber entities are Unit 8200 and Unit 81. Unit 8200 specializes in signals intelligence (SIGINT), cyber espionage, and offensive cyber operations. It is the largest and most technologically advanced unit in the Israeli military and serves as the backbone of cyber-intelligence gathering against hostile states and organizations. Unit 81, operating closely with 8200, develops advanced technologies, including offensive cyber tools, specialized hardware, and encryption-breaking systems, to support operations by the intelligence and special forces community. It is important to note that these units are not under the command of the IDF's C4I & Cyber Defense Directorate, but rather under the authority of its Military Intelligence (Aman). They are critical components of Israel's strategic cyber warfare capability, particularly for external operations and intelligence dominance.

- **Israel Defense Forces C4I and Cyber Defense Directorate**. The C4I and Cyber Defense Directorate (the J6 & Cyber Defense Directorate) is a branch of the IDF General Staff focused on cyber defense, military IT systems, and secure communication. This directorate oversees several specialized units responsible for infrastructure and defensive cyber operations. Mamram is the IDF's central computing unit accountable for developing and managing software systems, databases, and military IT infrastructure. Matzov (Center for Encryption and Information Security) develops encryption technologies and secures IDF and national communication systems. Hoshen focuses on civilian communications networks, while Maof serves as a command-and-control center for cyber defense operations, including real-time threat detection and response across IDF systems. Unlike Aman's units, which are outward-facing and intelligence-driven, the C4I Directorate's mission is internal: to protect IDF networks and enable secure operational functionality.

- **The Mossad,** operating under Israel's foreign intelligence service, plays a critical role in covert operations aimed at advancing national security objectives beyond Israel's borders. While less publicly recognized than the military's Unit 8200, these clandestine teams specialize in offensive cyber actions that align with Mossad's broader intelligence missions. Their operations often target hostile regimes, disrupt Iran's nuclear ambitions, or pave the way for physical missions through digital sabotage. Using tools such as malware, system breaches, and psychological cyber tactics, Mossad's cyber operatives execute stealthy intrusions and data theft, prioritizing deniability and synchronization with field operations to maintain their covert edge.

- **Shabak (Israel Security Agency)** is responsible for domestic security, counterterrorism, and cyber defense within Israel's borders. It operates cyber units that focus on preventing terrorist use of cyberspace, detecting hostile cyber activities within the country, and securing government institutions against attacks. These units play a pivotal role in identifying online radicalization, thwarting cyber plots by terrorist organizations such as Hamas or Islamic Jihad, and monitoring domestic threats that involve cyber components. Shabak also collaborates with the Israel Police and INCD to protect public sector systems and critical civilian infrastructure from cyber intrusions and cyberterrorism.

- **The Ministry of Defense (MoD)** manages research, procurement, and development of cyber capabilities in collaboration with military and intelligence agencies. Through its Directorate of Defense Research and Development (DDR&D), the MoD funds and oversees cyber technology programs and dual-use platforms, often in coordination with the IDF and Mossad. It also handles security oversight of export-controlled cyber technologies and authorizes cyber-related arms deals under the Israeli Defense Export Control Agency (DECA). Although it does not conduct cyber operations directly, the MoD plays a strategic role in building and sustaining national cyber capabilities through innovation, regulation, and industrial partnerships.

- **The Israel National Cyber Directorate (INCD)** is the primary civilian authority for national cybersecurity. Reporting directly to the Prime Minister's Office, the INCD is responsible for cybersecurity policy, coordination, critical national infrastructure (CNI) protection, and response to cyber incidents across the public and private sectors. It functions as Israel's CERT (Computer Emergency Response Team) and leads the development of national resilience through regulation, standards enforcement, and public-private partnerships. INCD also engages in international cyber diplomacy, capacity-building, and knowledge-sharing with allied countries. It does not perform offensive operations but ensures systemic protection and strategic coordination at the national level.

- **Israel Police National Cybercrime Unit (NCCU, Lahav 433)**, is the Israel Police's elite cyber law enforcement branch. While its primary mission is to investigate, prevent, and prosecute cybercrimes, including financial fraud, ransomware, child exploitation, darknet operations, cyberstalking, and politically motivated hacking, the NCCU also plays a vital role in combating cyberterrorism, working closely with Shabak and international agencies such as Europol and Interpol. The unit conducts digital analysis, arrests cybercriminals, and collaborates with technology companies to support legal surveillance and criminal investigations. It is crucial in bridging the operational gap between civilian law enforcement and national cyber intelligence.

In addition to its official cyber forces within military and intelligence institutions, such as Unit 8200, Israel is also supported by several independent pro-Israel and anti-Iranian regime hacktivist groups. These non-state actors operate in cyberspace to advance Israeli interests, often conducting cyberattacks against Iranian infrastructure, government institutions, and affiliated organizations. Their activities frequently align with Israel's broader geopolitical objectives, particularly in the ongoing cyber conflict with Iran. Among the most significant groups are:

- **Gonjeshke Darande** (Persian: گنجشک درنده), which means *Predatory Sparrow*, is a mysterious and highly sophisticated hacktivist group that first came into public view in the latter half of 2021 (Figures 2 and 3). The group made headlines after it claimed responsibility for a significant cyberattack that disrupted Iran's nationwide smart-card fuel distribution system in October 2021. This attack caused widespread chaos at gas stations across the country, drawing immediate attention from both Iranian authorities and international cybersecurity analysts. The group primarily communicates via its Telegram channel, which releases statements, evidence of breaches, and sometimes even leaked documents or videos taken from compromised surveillance systems. It presents itself as anti-regime, directly targeting entities and infrastructure linked to the Islamic Revolutionary Guard Corps (IRGC), a powerful military and political force in Iran. Predatory Sparrow has since claimed responsibility for several other major cyberattacks, including:
    - Iran's railway system was disrupted in July 2021, and digital boards displayed messages such as "Long live Rajavi" (a reference to the exiled opposition figure Maryam Rajavi of the MEK) and a false emergency contact number attributed to the office of Supreme Leader Ali Khamenei.
    - Attacks on steel companies in June 2022, notably Khouzestan Steel Company, one of Iran's most significant industrial producers, where the group released footage of furnaces malfunctioning. It claimed these attacks were in retaliation for the regime's aggression and not aimed at civilians.
    - Strikes against financial institutions and surveillance infrastructure, including hacking internal systems of security agencies and the public broadcasting network (IRIB).

  The group frames its operations as ethical cyber warfare, emphasizing avoiding civilian harm. In its own words, Predatory Sparrow claims to carry out operations that "minimize harm to innocent individuals" by carefully choosing targets related to the oppressive regime, particularly those tied to military or paramilitary operations, censorship, or human rights violations. Despite its visibility, the true identity and backing of the group remain unclear. Cybersecurity experts have speculated that *Predatory Sparrow* may be more than a grassroots activist group, given its attacks' technical sophistication and scale. Some analysts believe it could receive state-level support, possibly from a foreign government opposed to Iran, although no direct links have been confirmed. Organizations such as Trustwave, Time Magazine, and Iran International have covered the group's activities, pointing to a trend of

increasingly strategic and public-facing cyber disruption aimed at delegitimizing and pressuring the Iranian regime.



Figure 2 - Gonjeshke Darande X account (source: Social network X)

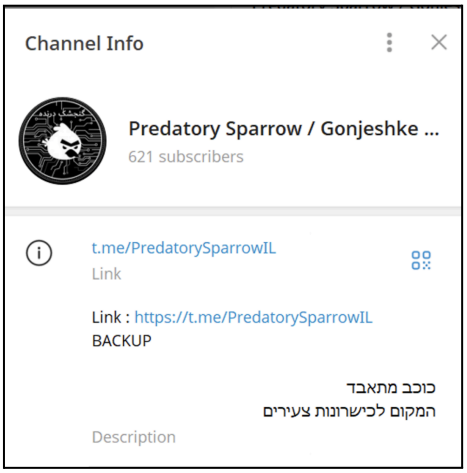


Figure 3 - Gonjeshke Darande Telegram channel (source: Telegram)

- **LabDookhtegan** (Persian:لب دختگان) is an anti-Iranian regime hacktivist group that gained attention for exposing the Iranian government's cyber operations. First emerging around 2019, the group became known for leaking tools and internal documents linked to Iranian intelligence units, particularly those of the Islamic Revolutionary Guard Corps (IRGC) and cyber espionage groups like APT34 (Figures 4 and 5).

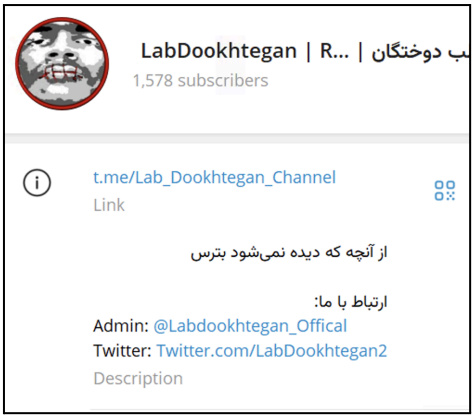


Figure 4 - LabDookhtegan Telegram Channel (Source: Telegram)



Figure 5 - LabDookhtegan post claiming the disclosure of IRGC crypto wallets

Over time, LabDookhtegan evolved from a whistleblowing outfit into an offensive cyber actor. In one of its most significant operations, the group claimed responsibility for a widespread cyberattack that disabled satellite communications on over 100 vessels operated by Iran's state-run shipping companies. This action reportedly disrupted maritime logistics and communications for weeks. LabDookhtegan framed the operation as retaliation against Iran's military support for regional proxy groups, signaling a shift toward more aggressive and direct cyber sabotage. LabDookhtegan's cyber activities against the Iranian regime have been extensive, strategic, and increasingly bold. Initially, the group operated as a whistleblower entity, leaking sensitive documents, operational manuals, source code, and internal communications from Iran's cyber-espionage units—most notably APT34 (also known as OilRig), a group believed to be linked to the Iranian Ministry of Intelligence. These leaks exposed malware tools used by the regime for surveillance, phishing, and data exfiltration campaigns across the Middle East and beyond.

LabDookhtegan also published names, photos, and personal details of Iranian cyber operatives, aiming to dismantle the secrecy around the regime's offensive cyber units and compromise their ability to operate covertly. Over time, their tactics shifted from passive leaking to active disruption. In 2025, they conducted one of their most high-profile operations by targeting Iran's maritime sector. This involved a coordinated cyberattack that disabled VSAT (Very Small Aperture Terminal) satellite communications on over 100 ships belonging to Iran's national shipping and tanker companies. By exploiting vulnerabilities in onboard systems, LabDookhtegan effectively crippled ship-to-port and crew communications, causing significant delays and logistical chaos. The group claimed the attack was a direct response to Iran's regional interventions, particularly its support for Houthi militants.

LabDookhtegan's campaigns are notable not just for their technical proficiency but for their messaging. They consistently frame their operations as part of a larger ideological struggle against oppression, corruption, and state-sponsored terror. Their communications are often laced with satire, defiance, and a clear anti-regime tone, aimed at undermining the Iranian government's image both domestically and internationally. Their transition from leaking to sabotage marks a new phase in cyber resistance that blends hacktivism with real-world disruption.

2.1.3 Recent Cyber incidents linked to pro-Israel hacking groups

June 13, 2025

- **Drone-assisted sabotage and airstrikes:** Israel's Intelligence deployed covert explosive UAVs that disabled Iranian missile launchers and air defenses ahead of broader Israeli airstrikes. This operation had strong cyberwarfare and sabotage components, coordinated with hacking and drone teams deep inside Iran.

June 17, 2025

- **Cyberattack on Sepah Bank:** On June 17, the Iranian state-owned and IRGC-affiliated Bank Sepah was hit by a major cyberattack, causing widespread service disruptions. The pro-Israel hacking group Gonjeshke Darande also known as Predatory Sparrow, claimed responsibility for the attack, stating it had infiltrated the bank's systems and destroyed its data.

As a result, customers reportedly faced outages across ATMs, online banking, and even gas station payment systems, with many unable to access their accounts, withdraw cash, or use bank cards. Predatory Sparrow, believed to be linked to Israeli cyber units, has previously carried out high-impact operations targeting Iran's infrastructure, including steel plants, railway systems, and gas distribution networks (Figure 6).



Figure 6 - A statement posted by the hacking group Predatory Sparrow on X claiming to target the infrastructure of the Islamic Revolutionary Guard Corps "Bank Sepah" (source: Social network X)

June 18, 2025

- Nobitex cryptocurrency heist: On June 18, Predatory Sparrow targeted Iran's largest cryptocurrency exchange, Nobitex, stealing and effectively "burning" about $90 million in crypto assets. They transferred the holdings to inaccessible addresses carrying anti-IRGC messages; the exchange's site was taken offline (Figure 7).

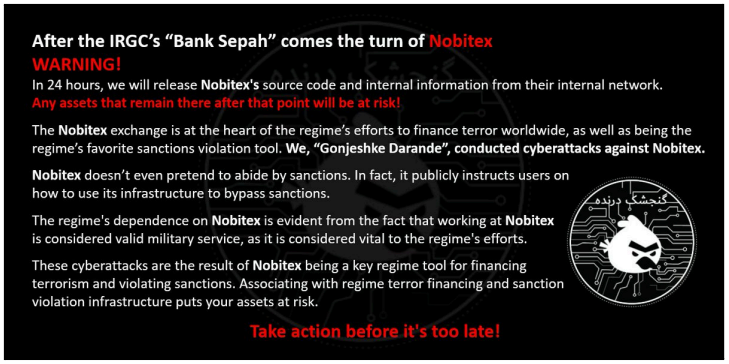


Figure 7 - A statement posted by the hacking group Predatory Sparrow on X claiming to target Nobitex's source code and internal information from their internal network (source: Social network X)

June 19–20, 2025

- **Nationwide internet blackout:** Following the Nobitex breach, Iran experienced extensive internet outages. While Iran attributed this to stability measures, analysts consider this part of the cyber-offensive ripple effects led by Predatory Sparrow

2.1.4 Contracting Ecosystem

The Israeli cyber contracting ecosystem is a powerful extension of its national cyber strategy. Many cybersecurity startups are spin-offs founded by veterans of Unit 8200 or Mossad's cyber teams, forming an innovation pipeline closely aligned with state needs. The Ministry of Defense, in collaboration with the Directorate of Defense Research and Development (DDR&D) and INCD, frequently contracts Israeli firms to develop surveillance tools, cyber-attack platforms, and advanced intrusion software. Companies like NSO Group, Cellebrite, CyberArk, and Check Point exemplify how private industry and government share resources, talent, and objectives. This partnership creates a dual-use ecosystem where tools developed for national security also enter global markets, sometimes raising legal and ethical controversies, especially concerning spyware use. Moreover, the ecosystem benefits from Israel's robust venture capital environment, fostering rapid prototyping and deployment of cyber technologies.

2.1.5 Operational Objectives and Tactics

Israel's cyber operations are strategically designed to achieve multiple overlapping objectives: early warning, deterrence, disruption, and strategic surprise. Offensive cyber operations often aim to delay or disrupt adversarial capabilities, such as nuclear programs (e.g., Stuxnet, allegedly developed jointly with the U.S. against Iran), communications networks, and weapons systems. Tactics include advanced persistent threats (APTs), zero-day exploitation, ransomware-like disruption, data exfiltration, and even the psychological use of information operations. On the defensive front, Israel adopts a "digital Iron Dome" model, leveraging AI and real-time threat intelligence to detect and neutralize incoming attacks, especially against critical infrastructure like energy, finance, and water systems. The IDF has publicly acknowledged its willingness to respond to cyberattacks with kinetic force, establishing cyber deterrence through credible cross-domain escalation.

2.2 Iran's Cyber Strategy: Doctrine, Capabilities, and Operations

2.2.1 Strategic and Operational Overview of Iran's Cyber Activities

While Iran has not publicly defined an official cyberwarfare doctrine, its operational behavior demonstrates a pragmatic and targeted approach, aligned with national strategic objectives. Iranian cyber operations systematically pursue three key objectives. The first is domestic regime stability, where cyber tools are leveraged to monitor, suppress, and disrupt dissident activity. Surveillance targets include activists, journalists, and perceived agents of foreign influence.

The second objective is national defense and intelligence gathering. Cyber espionage tracks adversaries like the United States, Israel, and Saudi Arabia. Intelligence is gathered to anticipate threats and inform strategic decisions. The third objective centers on foreign policy and regional influence. Iran uses cyber capabilities to project power, shape regional narratives, and influence geopolitical outcomes across the Middle East and beyond. These cyber strategies emerged from pivotal events, including the 2009 Green Movement protests and the 2010 Stuxnet cyberattack, which revealed both vulnerabilities and opportunities in cyberspace for Iran. Recent developments such as the hardline presidency of Ebrahim Raisi, the stalling of JCPOA nuclear negotiations, domestic unrest spurred by the Mahsa Amini protests, and Iran's alignment with Russia continue to shape Tehran's cyber priorities.

2.2.2 Iran's Cyber Forces and Affiliates

The development of cyber agencies in Iran has been a strategic priority over the past two decades, driven by the country's desire to bolster national security, counter external threats, and assert its influence in cyberspace. Following increased cyber vulnerabilities and notable incidents like the Stuxnet attack, Iran invested heavily in establishing and expanding state-controlled cyber institutions. Central to this effort are organizations like the Islamic Revolutionary Guard Corps (IRGC) Cyber Command, the Supreme Council of Cyberspace (SCC), and the Passive Defense Organization, each playing a distinct role in shaping policy, conducting cyber operations, and securing digital infrastructure. These institutions reflect Iran's shift toward a more coordinated and sophisticated approach to cyber power and include the following:

- **The Islamic Revolutionary Guard Corps (IRGC**) is an elite military force fiercely loyal to Iran's Supreme Leader and maintains robust and multifaceted cyber capabilities distributed among its various subdivisions.

The IRGC's cyber operations are primarily executed by specialized units within the Basij Militia and the Quds Force, both implicated in offensive and espionage cyber activities. These units orchestrate cyber intrusions aimed at foreign governments, defense industries, academic institutions, and NGOs through techniques like spear-phishing and sophisticated social engineering campaigns. Notable IRGC-linked cyber intrusion groups include:

- **APT35 (Charming Kitten, TA453, Cobalt Mirage)**: A broad cluster of cyber espionage actors conducting targeted operations against diplomatic entities, dissidents, and journalists, using tailored phishing to gather intelligence and conduct influence operations.
- **APT42** is a subgroup of APT35, which focuses on individuals and organizations connected to policy research, human rights advocacy, and civil society. It emphasizes surveillance of political opposition and international human rights bodies.
- **Nemesis Kitten:** Operating under contract through Iranian private companies like Afkar System and Najee Technologies, this group executes covert cyber operations supporting IRGC objectives, often engaging in espionage and digital sabotage.
- **Cotton Sandstorm (formerly NEPTUNIUM):** A sophisticated IRGC-linked threat actor engaged in broad espionage campaigns targeting geopolitical adversaries and critical infrastructure.

- **Ministry of Intelligence and Security (MOIS)** is Iran's primary foreign intelligence and internal surveillance agency, reporting directly to the president. Unlike the IRGC, MOIS is noted for a more technically sophisticated approach and a comparatively less ideologically driven operational style. MOIS's cyber activities emphasize targeted intrusions into critical sectors such as energy, telecommunications, maritime infrastructure, and government systems. Its cyber units are linked to several advanced persistent threat (APT) groups that conduct espionage, cyber reconnaissance, and sabotage:

  - **MuddyWater**: Known for targeting Middle Eastern governments and telecommunications firms, this group conducts espionage through custom malware and credential theft.
  - **OilRig (APT34):** Focuses on the energy sector and government organizations in the Middle East, leveraging phishing campaigns and credential harvesting to extract sensitive information.

- **Hexane:** Engages in cyber reconnaissance and espionage, often targeting telecommunications and infrastructure entities.
- **Agrius:** A lesser-known MOIS-linked group that conducts targeted cyber espionage operations, particularly against maritime and industrial sectors.
- **DarkBit (DEV-1084):** Specializes in sophisticated malware development and targeted intrusion campaigns primarily aimed at regional adversaries.

While MOIS and IRGC share overlapping mission scopes, MOIS's cyber operations focus more on technical exploitation and intelligence collection than overt influence or ideological campaigns. The competition between the two agencies occasionally drives innovation and intensity in Iran's cyber warfare efforts.

In addition to Iran's military, intelligence, and state-sponsored APT groups, a growing ecosystem of ideologically motivated pro-Iran hacktivist groups operates in parallel, often amplifying Tehran's cyber and psychological warfare objectives. While these groups maintain a degree of plausible deniability for the Iranian regime, their tactics and targets align closely with Tehran's regional interests. These actors specialize in breaching data repositories, deploying destructive malware, and disseminating false narratives or manipulated content, particularly targeting the Israeli government, defense, and civilian infrastructure. Many act as auxiliaries to official cyber units, conducting preparatory intrusions, information operations, and propaganda dissemination on platforms like Telegram, Twitter (X), and obscure forums.
Unlike state APTs, their operations are less technically sophisticated but highly disruptive due to their focus on exfiltration and narrative warfare.

Threat actors involved in data breaches, malware, and disinformation activities.s

Cyber Av3ngers

- It specializes in ICS/SCADA targeting and breaches of critical infrastructure firms.
- Known for data leaks from the Israeli electric and water sectors.

Soldiers of Solomon (Askar Suleiman)

- Engaged in disinformation and psychological operations.
- Claims operations involving email leaks and spyware on Israeli officials.

Altahrea Team

- Conducts defacement and data breaches; involved in releasing sensitive employee information.
- Operates parallel to groups like Moses Staff but avoids APT-level sophistication.

Moses Staff

- It is not classified as APT; it focuses on leaking surveillance footage and personnel data.
- Known for high-profile breach-and-leak campaigns with ideological messaging.

Handala Hack

- Engages in breaching government and private sector servers.
  Leaked internal Israeli police documents and files from military contractors.

Anonymous Arabic

- This variant, not affiliated with the global Anonymous, focuses on Israeli data leaks and malware deployment.
- Active in spreading forged documents and attacking databases.

Khodkar (Self-Made) Team

- Pro-Iranian cyber collective focused on social engineering and access selling.
- Disseminates compromised Israeli credentials and internal communications.

Ghiyath Cyber Forces

- Engages in data leaks and manipulation of digital media to promote false narratives.
- Typically uses Telegram to distribute stolen content.

Cyber Toufan (Cyber Storm)

- Active since the Gaza conflict escalation, not state-aligned but highly organized.
- Targets include logistics, healthcare, and Israeli municipal services, primarily with breach tactics and malware payloads.

Revenge Soldiers

- Focused on information warfare and theft of sensitive strategic documentation.
  Targets include academic, defense, and public health institutions in Israel.

Threat Actors involved in DDoS attacks.

Since June 13, 2025, according to the cybersecurity company Radware, Iranian-linked cyber activities targeting Israel have intensified, focusing on distributed denial-of-service (DDoS) attacks aimed at disrupting critical infrastructure and public-facing systems. On the day Operation Rising Lion was launched, a coordinated cyber campaign was announced by a prominent pro-Iranian threat actor known as Mr. Hamza, working with affiliated groups including Anonymous Guys, Team 1722, and Desinformador Ruso (Figure 8). This alliance declared intentions to target not only Israel but also its Western allies, notably the United States and the United Kingdom. In the days following the announcement, Israeli government portals, media websites, and transportation systems experienced intermittent outages and slowdowns, attributed to sustained DDoS waves originating from networks likely supported or amplified by Iranian cyber infrastructure. While the technical sophistication of these attacks has varied, the campaign marks a deliberate attempt to coordinate international pro-Iranian hacktivism into a force multiplier against Israeli digital defenses, highlighting Tehran's reliance on proxy groups to wage asymmetric cyber warfare beyond its borders.

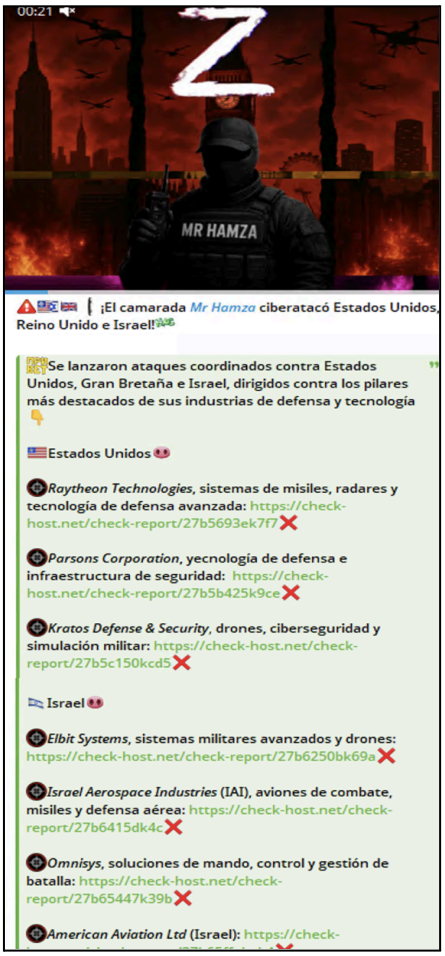


Figure 8 - Mr. Hamza, hacktivist group claiming responsibility for a DDoS campaign targeting the United States, the United Kingdom, and Israel (source: Telegram)

Primary Actors

- **Mr Hamza, Presumed** Middle Eastern origin
- **Arabian Ghosts** Middle East (Likely Gulf region)

Middle East & North Africa (MENA)

- **Cyber Fattah Team** Middle East (likely pro-Islamist affiliation)
- **Coup Team** Likely Middle Eastern origin
  Moroccan Black Cyber Army Morocco
- **Tunisian Maskers Cyber Force** Tunisia
- **Desinformador Ruso** may have ties to Arabic-speaking pro-Russian propaganda; the exact origin is unclear.

South Asia

- **Mysterious Team Bangladesh** Bangladesh
- **Sylhet Gang** Bangladesh (Sylhet region)

Southeast Asia

- **Garuda Error System** Indonesia

Unknown Origin

The following groups have limited public attribution or are known for obscuring their origins.)

- Server Killers
- Unknowns Cyber Team
- TwoNet
- DieNet
- RipperSec
- Anonymous Guys
- Lulzsec Black
- Elite Squad
- Nation of Saviors
- Keymous+
- Red Wolf Cyber
- Team Fearless
- Ghost Clan
- MadCap

2.2.3 Recent Cyber incidents linked to pro-Iran hacking groups

June 4–12, 2025

- Researchers from Radware observed 3–4 distributed denial-of-service (DDoS) attacks per day targeting Israeli infrastructure.

June 13, 2025

- DDoS volume jumped to 21 attacks in a single day, marking the beginning of a sustained surge.

June 14, 2025

- Attack volume increased again, reaching 34 DDoS attacks in one day.

June 15 – Present

- The intensity has remained high, with 25 or more DDoS attacks daily.
- As of this writing, Israel accounts for nearly 40% of all global hacktivist DDoS attacks, far exceeding any other country.

June 18, 2025

- The Handala hacktivist group claimed two major breaches:
    - A 425GB data leak from Mor Logistics Ltd, an Israeli shipping company.
    - Alleged access to 4TB of internal documents, research, and classified material from the Weizmann Institute of Science, a prominent Israeli research university.
    - The Weizmann Institute was also reportedly struck by an Iranian missile on the same day, suggesting potential coordination between physical and cyber operations.

2.2.4 Contracting Ecosystem

Iran heavily relies on private contractors and academic institutions to extend its cyber reach. Emennet Pasargad operates Cotton Sandstorm for the IRGC. Ravin Academy, founded by MOIS veterans, serves as a recruitment and training hub for MOIS-affiliated operators. Legacy contractors like Mabna Institute, Rana Institute, and ITSecTeam contributed to foundational cyber campaigns but have faded from recent reporting.

2.2.5 Operational Objectives and Tactics

Iranian cyber actors prioritize intelligence collection on geopolitical adversaries and domestic threats in espionage and surveillance. Oilrig targeted Jordan's Foreign Ministry in 2022 using custom malware. Domestic surveillance groups like Domestic Kitten use mobile spyware such as FurBall to track Iranian citizens. APT35 deployed TelegramGrabber, focusing on devices within Iran using Farsi-language tools. Regarding destructive cyber operations, Iran conducts cyber sabotage, often under the guise of activism or ransomware. The Shamoon attack in 2012 was a landmark, destructive incident targeting Saudi Aramco. In 2022, the Albanian cyberattack was conducted by Oilrig and Hexane under the false front of Homeland Justice. In 2023, DarkBit carried out a destructive attack on Israel's Technion Institute, masquerading as ransomware, with access handed over by MuddyWater. Iran's increasing use of deceptive hacktivist fronts suggests a strategy to obscure state involvement while enabling plausible deniability. Tehran integrates cyber operations with influence campaigns to sway public opinion and sow discord, forming the backbone of its information operations (InfoOps). Cotton Sandstorm led coordinated campaigns against targets like Charlie Hebdo and regional opponents like Bahrain. Operations often leverage fake social media accounts and fabricated personas to amplify narratives aligned with Iranian state interests. Although not Iran's primary cyber objective, financially motivated operations are sometimes conducted by IRGC-linked contractors. Fox Kitten and Nemesis Kitten have exploited vulnerabilities like Log4j for ransomware and crypto-mining campaigns. Whether these operations are sanctioned or self-directed remains unclear.

3. Electronic Warfare Operations

While Israel and Iran are engaged in both physical and cyber conflicts, electronic warfare plays a crucial, if not indispensable, role in their ongoing hostilities. Both nations have developed and deployed sophisticated electronic warfare (EW) capabilities that serve not only to disrupt enemy communications and radar systems but also to shape the broader strategic landscape. These capabilities include jamming, spoofing, signal interception, and electromagnetic attacks, all used to gain tactical advantages on the battlefield and cyberspace. Israel has long invested in advanced EW technologies, integrating them into its military doctrine to neutralize threats from both state and non-state actors. Iran, in response, has expanded its EW infrastructure, leveraging asymmetric tactics to counter Israel's technological superiority. The use of these tools is not limited to conventional warfare; they are also integral to covert operations, intelligence gathering, and the protection of national assets. Electronic warfare thus serves as both a shield and a sword in this high-stakes rivalry, with each side continuously adapting to the other's innovations and countermeasures. The scope and sophistication of EW operations underscore its pivotal role in modern conflict between these regional powers (Figure 9).

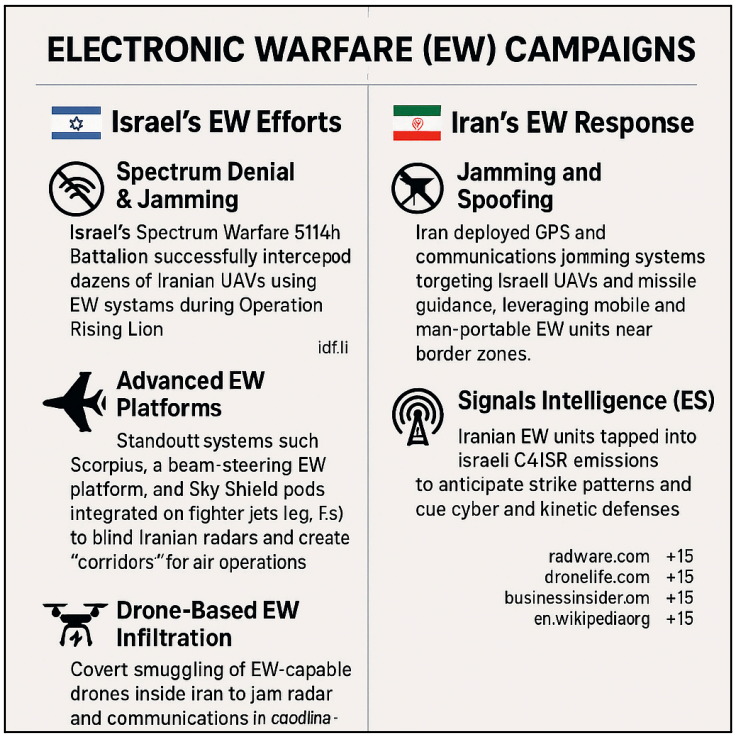


Figure 9 - Israel vs Iran Electronic Warfare activities

3.1 Israel's Electronic Warfare Efforts

3.1.1 Blocking Enemy Signals (Spectrum Denial & Jamming)

Israel's 5114th Battalion, part of its special electronic warfare unit, used powerful jammers to disrupt the control signals of Iranian drones. Such operations include:

- Blocked communication between Iranian drones and their operators.
- Used signal spoofing (sending fake signals) to confuse drones.
  Carried this out during major operations like "Rising Lion".

3.1.2 Drone-Based EW Operations

Israel used drones to secretly jam Iranian radar and communications from inside Iran. Such operations include:

- Drones were smuggled in or launched from nearby places.
  Worked with ground agents to jam or trick Iranian radar.
  Some drones acted as decoys to distract Iran's defenses.

3.2 Iran's Electronic Warfare Response

3.2.1 Defensive Jamming and Spoofing

Iran tried to fight back by jamming GPS and communication signals used by Israeli drones and missiles. Such operations include:

- Set up mobile jammers near conflict zones.
- Send fake GPS signals to confuse drones.
  Aimed to interfere with the accuracy of Israeli weapons.

3.2.2 Signals Intelligence (SIGINT)

Iran tried to intercept Israeli signals to gather intelligence and prepare defenses.Such operations include:

- Monitored drone data and encrypted communications.
- Used this info to guess when and where attacks would happen.
- Shared data with cyber teams for hacking or digital defense.

4. Conclusion

The current cyber conflict between Israel and Iran constitutes one of the most persistent and complex confrontations in contemporary digital warfare. Escalating since June 13, 2025, this conflict has evolved into a sustained campaign marked by an increased operational tempo, visible cycles of retaliation, and the growing involvement of state-linked actors and independent hacker groups. This escalation reflects deep-rooted geopolitical hostilities and the ever-increasing strategic centrality of cyberspace in modern conflicts.

Israel's cyber capabilities are distinguished by their technological sophistication, strategic integration within its national defense architecture, and operational focus on precision, intelligence dominance, and deterrence. With the backing of various pro-Israeli cyber actors, Israel employs a multifaceted approach to targeting Iran's critical infrastructure, intelligence networks, and digital command systems. These operations are designed to be proactive and calculated, closely aligned with broader military and geopolitical objectives.

For its part, Iran has developed a cyber strategy characterized by adaptability, indirect engagement, and asymmetric tactics. Iran has expanded the scope and impact of its cyber operations by leveraging a diverse network of proxies, contractors, and ideological groups. Its focus is often on civilian and economic targets in Israel, psychological influence operations, and disruptive attacks aimed at offsetting conventional power asymmetries.

In addition to cyber operations, electronic warfare (EW) has emerged as a critical complement in the Israel-Iran conflict, blurring the lines between kinetic and digital battlespaces. EW tactics such as signal jamming, spoofing, and electromagnetic interference are increasingly employed to disrupt communications, radar systems, and command-and-control infrastructure. These techniques serve not only as force multipliers for cyber operations but also as tools to undermine situational awareness and operational effectiveness in both military and civilian spheres. Israel's advanced electronic warfare platforms, integrated into its broader military systems, offer strategic depth and precision, while Iran has leveraged more decentralized, cost-effective EW tools to support its asymmetric doctrine. As both nations invest further in EW capabilities, this often-overlooked dimension reinforces the convergence of cyber and electromagnetic domains in shaping the future of hybrid conflict.

The ongoing digital conflict between these two nations highlights several persistent challenges in cyberwarfare. The mix of state and non-state actors increases operational ambiguity and the possibility of denial. Civilian infrastructure, now a common target, is on the front lines of this conflict, exposing the vulnerabilities of critical services and raising humanitarian concerns. As this confrontation intensifies, cyberspace becomes entrenched as a domain of persistent strategic competition. Both nations are refining their existing tools and institutionalizing their cyber capabilities within broader security doctrines, ensuring that this digital standoff will remain a defining element of Middle Eastern geopolitics. Understanding the operational patterns, technological dynamics, and structural implications of the Israeli-Iranian cyber conflict is essential to assess regional stability and inform global cyber defense and diplomacy in an increasingly contested digital landscape.

5. About The Author



I am a cyber intelligence expert with over ten years of experience in various environments, including academia, high-tech, military, and law enforcement. My expertise includes intelligence strategy, collection, research, and analysis, and the lead of Cyber HUMINT operations on criminal and terrorist activities within cyberspace. I also focus my research on cyber geopolitics and conflicts. I have trained many civilian analysts and Military and Law Enforcement officers on the Deep and Dark Web environments, Cyber intelligence collection, and Cyber HUMINT operations.

6. References

- Radware. (2025, May 2). Cyberattacks, Hacktivism and Disinformation in the 2025 Israel-Iran War. Radware Threat Advisories and Attack Reports. https://www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-hacktivism-and-disinformation-in-the-2025-israel-iran-war/

- CloudSEK. (2024, December 11). The Iran-Israel Cyber Standoff – The Hacktivist Front (Part 1). CloudSEK Blog. https://www.cloudsek.com/blog/part-1-the-iran-israel-cyber-standoff---the-hacktivist-front

- Flashpoint Intel Team. (2024, October 27). Escalation in the Middle East: Israel-Iran Conflict and the Cyber Threat Landscape. Flashpoint Blog. https://flashpoint.io/blog/escalation-middle-east-israel-iran-conflict

- CybelAngel. (2024, November). Israel-Iran Cyber Conflict – Flash Report. CybelAngel Cyber Intelligence. https://cybelangel.com/israel-iran-cyber-conflict-flash-report/

- Wired. (2025, June 19). Israel-Tied Predatory Sparrow Hackers Are Waging Cyberwar on Iran's Financial System. Wired. https://www.wired.com/story/israels-predatory-sparrow-hackers-are-waging-cyberwar-on-irans-financial-system/

- Politico. (2025, June 22). Bank hacks, internet shutdowns and crypto heists: Here's how the war between Israel and Iran is playing out in cyberspace. Politico. https://www.politico.com/news/2025/06/22/us-israel-iran-war-cyber-attacks-00417782

- The Verge. (2025, June). Iran is going offline to prevent purported Israeli cyberattacks. The Verge. https://www.theverge.com/politics/688875/iran-cutting-off-internet-israel-war

- Washington Post. (2025, June 24). Iran's cyber forces have many ways to attack U.S., experts warn. Washington Post. https://www.washingtonpost.com/technology/2025/06/24/iran-cyber-attacks-us-possible/

- Wall Street Journal. (2025, June). U.S. Warns of Potential Retaliation for Iran Strikes, Including Hate Crimes and Cyberattacks. WSJ Live Coverage.

https://www.wsj.com/livecoverage/iran-israel-us-latest-news/card/u-s-warns-of-potential-retaliation-for-iran-strikes-including-hate-crimes-and-cyberattacks-9ageo46DM94j5zwTntqM

- Axios. (2025, June). CISOs eye Iran. Axios Future of Cybersecurity. https://www.axios.com/newsletters/axios-future-of-cybersecurity-1038e950-4889-11f0-b558-17dac864894e

- The Hacker News. (2025, June 23). DHS Warns Pro-Iranian Hackers Likely to Target U.S. Networks After Iranian Nuclear Strikes. The Hacker News. https://thehackernews.com/2025/06/dhs-warns-pro-iranian-hackers-likely.html

- IndustrialCyber. (2025, June 23). NTAS bulletin highlights rising cyber, terror threats to US critical infrastructure from Iran-linked hackers. IndustrialCyber. https://industrialcyber.com/2025/06/23/ntas-bulletin-highlights-rising-cyber-threats-to-us-critical-infrastructure/

- SecAlliance. (2025, June 13). Iran's Cyber Strategy and the Israel-Iran Conflict. SecAlliance Blog. https://secalliance.com/2025/06/irans-cyber-strategy-and-the-israel-iran-conflict

- Dark Reading. (2025, June 19). Iran-Israel War Triggers a Maelstrom in Cyberspace. Dark Reading. https://www.darkreading.com/iran-israel-war-triggers-cyberspace-maelstrom

- The Jerusalem Post (June 2025), Israeli Defense Forces' 5114th Spectrum Battalion, https://www.jpost.com/israel-news/defense-news/article-858717idf.il+2timesofisrael.com+2jpost.com+2

- The Times of Israel (June 2025), the IDF's 5114th Battalion has thwarted numerous Iranian drone attacks through real-time electronic countermeasures, https://www.timesofisrael.com/liveblog_entry/idf-says-it-has-been-intercepting-dozens-of-iranian-drones-using-electronic-warfare-means/