STAY ALERT. STAY SECURE

The Cyber Front of Iran-Israel

CONTENTS

EXECUTIVE SUMMARY

The current escalation between Iran and Israel marks a significant shift from prolonged shadow confrontation to overt military exchange. What was historically characterized by proxy warfare, covert action, sabotage, and cyber operations has transitioned into direct kinetic engagement, increasing the risk of accelerated and less controllable escalation dynamics.

Parallel to the physical confrontation, a cyber front has rapidly emerged. Pro-Iranian hacktivist groups have demonstrated high operational tempo, primarily conducting large-scale DDoS campaigns, website defacements, and opportunistic intrusion attempts against Israeli and regional targets. In contrast, pro-Israeli cyber activity appears comparatively low-profile and attribution-challenged, with limited public claims despite reports of potential compromises affecting Iranian government-linked entities.

At present, the cyber threat landscape is dominated by disruption-focused activity rather than destructive or strategically crippling operations. However, historical patterns indicate that sustained kinetic escalation can create conditions for more advanced cyber campaigns, including targeted access operations, credential harvesting, influence operations, and selective attacks against high-value infrastructure.

Regionally, Gulf states and US-linked assets are experiencing elevated exposure to both symbolic and operational cyber activity. Spillover risk remains credible, particularly for countries that maintain diplomatic, economic, or military ties with either party.

For Turkey, while not currently a primary target, strategic positioning as a NATO member and regional hub increases the probability of opportunistic targeting, influence operations, or indirect impact via supply chain and infrastructure dependencies.

Globally, organizations should anticipate elevated cyber risk levels, especially within government services, defense, financial services, media, aviation, and energy sectors. The most likely near-term threat remains high-volume DDoS and defacement activity; however, escalation pathways toward more targeted and intelligence-driven operations remain plausible.

Continuous monitoring of underground communications, strengthened defensive posture, and rapid incident response readiness are recommended as baseline mitigation measures during this evolving escalation cycle.

Drivers of the Conflict and Current Battlefield Situation

Why the Conflict Escalated

The current escalation between Iran and Israel did not emerge suddenly; it is the latest phase of a long-running shadow confrontation that has gradually intensified over the past decade. Both sides have historically preferred indirect engagement through proxies, covert operations, and cyber activity rather than open warfare.

Several structural factors contributed to the present crisis. Iran has continued to expand its regional footprint via allied non-state actors across the Levant and the Gulf, which Israel consistently views as a direct security threat. At the same time, Israel maintains a well-established doctrine of preemptive action when it assesses that strategic risks are approaching unacceptable levels.

Over time, repeated cycles of covert action, retaliation, and signaling have created a highly volatile deterrence environment. The latest strikes appear to have crossed the threshold from managed escalation into overt military confrontation.

From Shadow Conflict to Direct Military Exchange

Until recently, the Iran–Israel rivalry was largely characterized by:

- proxy warfare
- targeted sabotage
- maritime incidents
- cyber operations
- limited deniable strikes

The current situation marks a notable shift toward direct kinetic engagement. This transition is significant because once state actors move into open military exchange, escalation dynamics tend to accelerate and become harder to contain.

From a threat intelligence perspective, such transitions historically correlate with parallel activity in the cyber domain, particularly from state-aligned or sympathetic hacktivist communities.

Current Operational Picture

Based on available reporting, Israeli forces reportedly with US support conducted precision strikes against Iranian military-linked targets. Iran has since responded with missile launches targeting Israeli territory and US-associated assets in the region.

Military readiness levels across multiple Middle Eastern countries have increased, and air defense systems have been actively engaged. The situation remains fluid, with a credible risk of further retaliation cycles in the near term.

Cyber Threat Outlook (Initial Assessment)

Periods of overt military confrontation between these actors have historically been accompanied by a surge in cyber and information operations. Typical patterns include:

- rapid mobilization of pro-Iranian hacktivist groups
- retaliatory DDoS campaigns against symbolic targets
- website defacements and data leak claims
- influence and psychological operations

Early signals suggest elevated risk of cyber activity emerging alongside the kinetic conflict, warranting close monitoring in the coming days.

Pro-Iranian Underground and Hacktivist Ecosystem

At the time of writing, both pro-Iranian and pro-Israeli hacktivist communities have increased their operational tempo and public signaling. Activity announcements are frequently published via Telegram, X (formerly Twitter), and other fringe social platforms, often shortly before or immediately after claimed operations.

Observed operations primarily focus on DDoS campaigns, website defacements (“indexing”), and opportunistic data theft/leak claims. Defacement pages commonly contain political messaging, propaganda imagery, and psychological signaling intended to amplify perceived impact beyond the technical effect. Current early-phase activity suggests that pro-Iranian actors are prioritizing high-volume DDoS disruption over more complex intrusion operations.

DieNet

After the announcement by the Dietnet team regarding this activity, the group reportedly launched multiple DDoS attacks against various targets in Arab states, including Qatar, Bahrain, and the United Arab Emirates. The attacks primarily focused on government portals and airport-related websites.

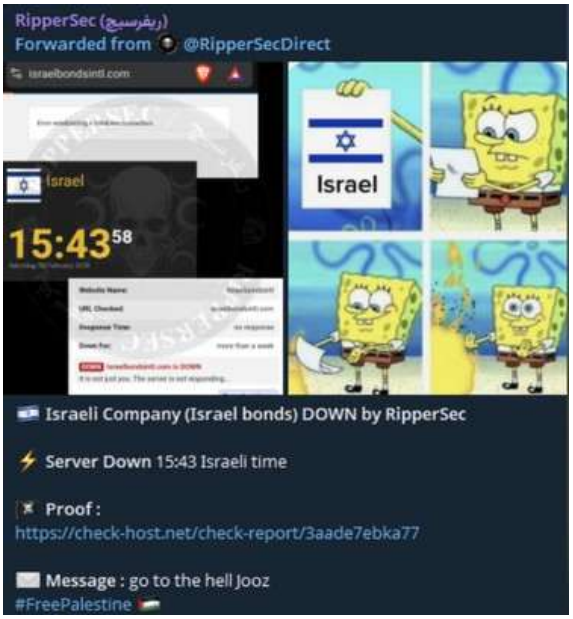
SYLHET GANG-SG

The Sylhet Gang-SG team has issued an announcement calling on other hacking groups to support large-scale attacks against targets in the United States and Israel. The group has been sharing DDoS activities conducted by other teams on its Telegram channels; however, it has so far remained inactive and has not carried out any attacks.

RipperSec

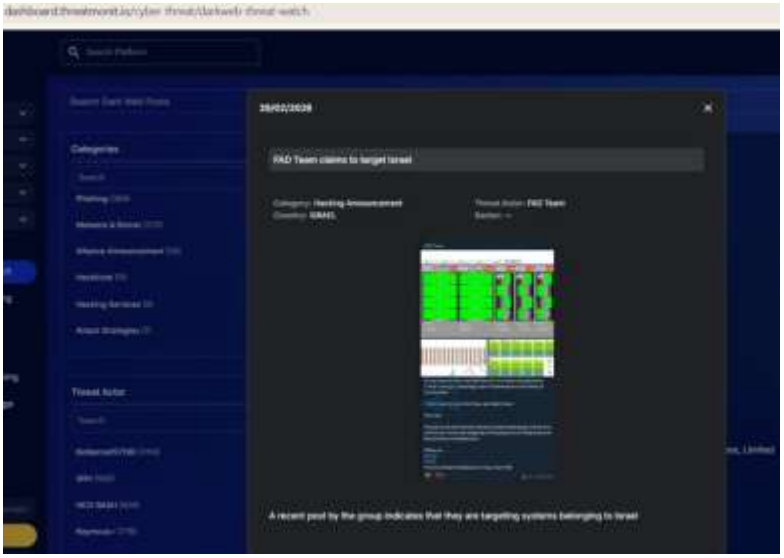
RipperSec conducted a DDoS attack against the website of the Neve David Community Center, causing service disruption and confirmed downtime.

RipperSec carried out a DDoS attack targeting the website of Israel Bonds, resulting in confirmed service downtime.



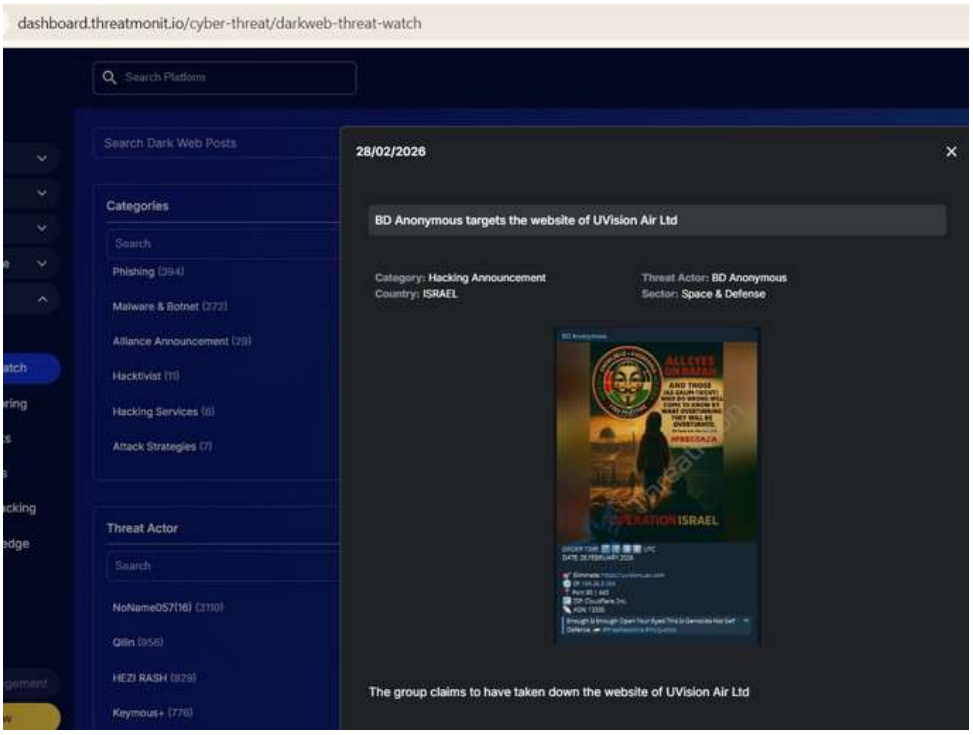
FAD Team

The FAD Team continues its operations targeting entities in Israel. Unlike groups that primarily rely on DDoS activity, the team more frequently focuses on website intrusions, attempting data exfiltration and defacement. Their targeting does not appear limited to a specific sector, though government-related websites are among the primary focuses.



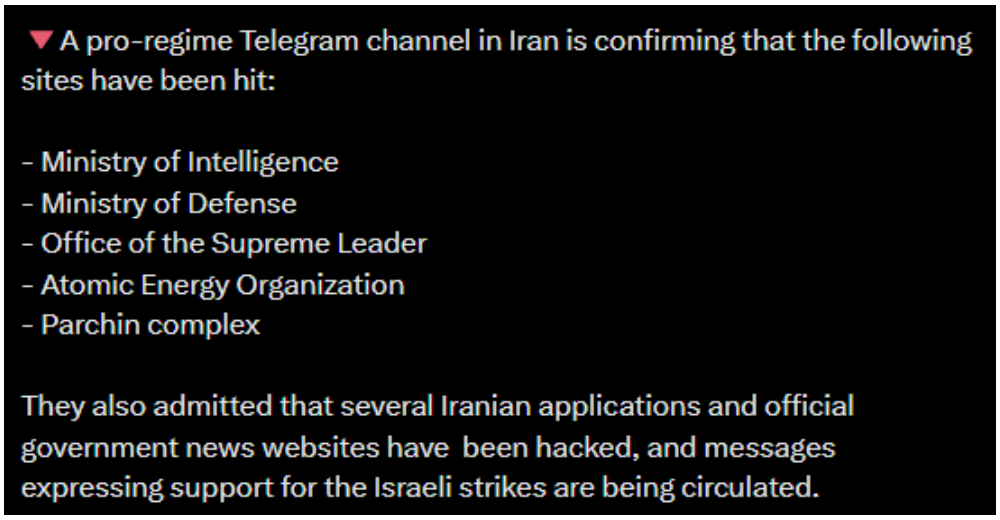
BD Anonymous

The BD Anonymous team has been conducting DDoS attacks against targets in Israel, aiming to disrupt services. Their most recent target was the website of UVision Air Ltd.



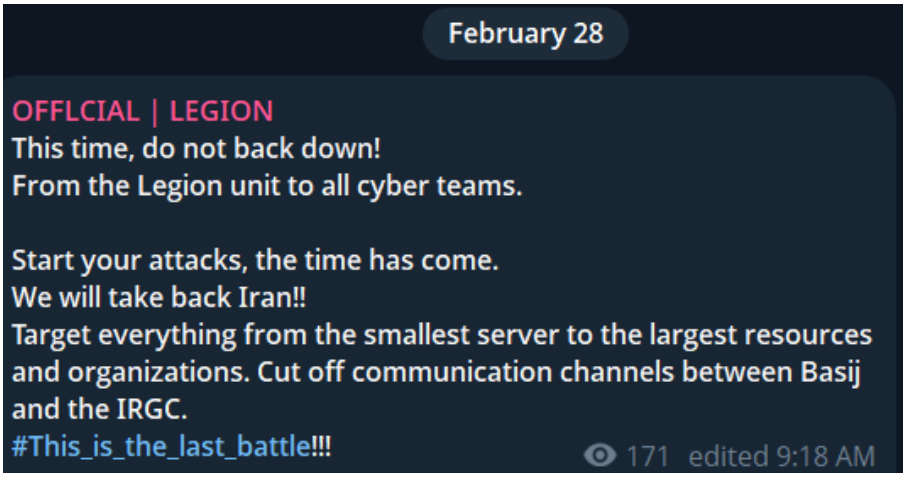
Pro-Israel Groups

A pro-regime Telegram channel in Iran claims several major government-related sites were hit including the Ministries of Intelligence and Defense, the Supreme Leader's office, the Atomic Energy Organization, and the Parchin complex. It also says some Iranian government apps and news sites were hacked, with messages supporting Israeli strikes being spread.



An "official statement" from a group calling itself Team Cyber Troll says it launched a cyberattack on the news site "Khabar-e Irani," allegedly bypassing security and causing a 502 error. The group claims it will target the infrastructure of news agencies across Iran and threatens further operations against networks of the Islamic Republic, including IRIB. It frames the attacks as supporting the security of Israel and says some services are already inaccessible while attacks continue.

According to the statement, OFFICIAL LEGION called for coordinated cyberattacks against government-linked entities, infrastructure, and communication networks in Iran, specifically referencing organizations associated with the Basij and the Islamic Revolutionary Guard Corps. Hours after the announcement, the group has remained silent with no further public updates.



According to the message, the group known as Ali Bk claims to have carried out a cyberattack against an Iranian prayer and call-to-prayer (adhan) mobile application. The announcement states that the app was targeted as part of their operations

Pro-Israeli hacktivist groups have largely remained low-profile and operationally silent, conducting activities without public announcements on Telegram, X, or other social platforms. Multiple reports indicate that Iranian government portals, military systems, and major websites have been compromised during the ongoing escalation. However, no known Israeli-aligned group has claimed responsibility for these incidents, making it difficult to accurately assess the true technical impact on Iranian systems. Consequently, observed pro-Israeli cyber activity remains stealthy and attribution-challenged at this stage.

Emerging Cyber Front Between Iran-Aligned and Israel-Aligned Actors

The ongoing kinetic escalation has triggered a parallel cyber front that mirrors the conventional conflict. Both pro-Iranian and pro-Israeli actors have been observed engaging in activities consistent with disruption, signaling, and opportunistic intrusions, although the operational approaches differ significantly.

Pro-Iranian Cyber Operations

Pro-Iranian hacktivist groups have been the most active on the cyber front. Key trends include:

- High-volume DDoS campaigns against regional targets such as government portals, airports, and financial services, particularly in Gulf states like UAE, Qatar, Bahrain, and Kuwait.
- Website defacements and indexing, often embedding political messaging to amplify the psychological impact of operations.
- Data exfiltration attempts, with occasional successful intrusions targeting Israeli entities and regional contractors.
- Organizational coordination via Telegram and fringe social platforms, allowing loosely affiliated teams to synchronize campaigns while maintaining operational security.

Notable actors include DieNet, SYLHET GANG-SG, RipperSec, FAD Team, and BD Anonymous, who collectively represent a spectrum of capabilities from mass DDoS disruption to targeted intrusion and defacement.

Pro-Israeli Cyber Operations

Pro-Israeli groups have largely maintained a low-profile posture, focusing on operational security rather than public signaling. Observed activity includes:

- Opportunistic targeting of Iranian government portals, military systems, and high-value websites.
- Limited reported incidents such as attacks on news applications and specific infrastructure components, although no group has publicly claimed responsibility.
- Attribution challenges make it difficult to fully quantify the technical impact of pro-Israeli operations, which remain stealthy, carefully measured, and likely preparatory for potential escalation.

Characteristics of the Emerging Cyber Front

Several patterns are evident across both sides:

- Divergence in operational style: pro-Iranian actors favor visible disruption and political signaling, whereas pro-Israeli actors prioritize stealth and selective targeting.
- Overlap with physical operations: cyber attacks often coincide temporally with kinetic strikes, suggesting integrated campaign planning or reactive operations.
- Potential escalation pathways: both sides possess the capability to move from volume-based disruption toward more targeted intrusions, credential harvesting, or attacks against high-profile individuals and infrastructure.
- Regional spillover: Gulf states and US-linked regional assets are increasingly part of the operational environment, both as cyber targets and symbolic signaling points.

Potential Attack Scenarios and Target Profiles

Based on current escalation dynamics and historical behavior of Iran-aligned cyber actors, the near-term threat landscape is expected to remain disruption-focused but may gradually expand toward more targeted intrusions.

Likely Near-Term Activity

In the short term, pro-Iranian hacktivist groups are likely to continue prioritizing DDoS operations and website defacements, particularly against high-visibility targets. Government-based portals especially public-facing services remain among the most probable targets due to their symbolic value and typically broader attack surface.

There is also a credible risk of cyber operations targeting US-linked assets, including government web infrastructure, defense-adjacent contractors, and regionally deployed support systems. Such activity would be consistent with past retaliatory patterns observed during periods of heightened geopolitical tension.

Regional Spillover Risk

Recent reporting indicates that infrastructure and digital assets in Gulf states including the UAE, Qatar, Kuwait, and Bahrain have already experienced both physical and cyber pressure attributed to Iran-aligned actors. If the current escalation persists, opportunistic cyber activity against organizations in these countries is likely to increase.

Potential objectives in these environments include:

- service disruption for political signaling
- defacement of public-facing platforms
- opportunistic data access from poorly secured systems
- psychological and information operations

Potential Shift Toward Targeted Access Operations

While current activity is heavily disruption-focused, there is a moderate risk that more capable or state-aligned actors may attempt targeted access operations in parallel with hacktivist noise.

One area of concern is potential targeting of high-profile individuals, including:

- government officials
- defense personnel
- policy advisors
- regionally relevant business executives

Threat actors may attempt credential harvesting, phishing, or device-level access to obtain sensitive communications or enable future influence operations.

Assessment

At present, the threat environment is dominated by volume-based disruption, but escalation pathways toward more selective and intelligence-driven cyber operations remain plausible if kinetic tensions continue to rise.

Potential Impact on Turkey

Geopolitical and Strategic Positioning

As a NATO member and a regional power maintaining diplomatic and economic relations with both Iran and Israel, Turkey occupies a uniquely sensitive position in the current escalation. Ankara's geographic proximity to the conflict theater, combined with its role as a regional transit hub for energy, logistics, and finance, increases its exposure to both direct and indirect spillover effects.

Turkey has historically sought to balance its regional relationships while preserving strategic autonomy. However, periods of heightened Iran–Israel confrontation typically increase the risk of secondary pressure, particularly in the cyber and information domains.

Cyber Risk Exposure

From a cyber threat perspective, Turkey faces several exposure vectors:

1. **Opportunistic Targeting by Hacktivist Groups**

Pro-Iranian hacktivist groups have previously targeted Gulf states and NATO-aligned entities for symbolic purposes. Turkish government portals, financial institutions, aviation infrastructure, and media platforms could become opportunistic DDoS or defacement targets either due to NATO alignment or perceived political positioning.

2. Spillover from Regional Campaigns

If cyber operations expand beyond Israel-focused targeting, Turkish organizations may be affected indirectly through:

- Shared hosting providers
- Regional cloud infrastructure
- Third-party contractors operating in Israel or Gulf states
- Supply chain dependencies

3. Information and Influence Operations

Turkey's active social media ecosystem makes it a potential arena for influence campaigns. Disinformation narratives designed to polarize domestic audiences or manipulate perceptions of Ankara's foreign policy stance may increase during escalation cycles.

4. Energy and Logistics Sector Risk

Given Turkey's role as an energy transit corridor between East and West, disruption attempts whether symbolic or operational against energy operators, port infrastructure, or transportation networks cannot be ruled out. While large-scale destructive attacks remain unlikely in the near term, reconnaissance and access-establishment activity is plausible.

Recommended Monitoring Priorities for Turkish Organizations

Organizations in Turkey should consider prioritizing:

- Monitoring for DDoS chatter on Telegram channels associated with Iran-aligned groups
- Increased alerting for defacement attempts and web application exploitation
- Phishing campaigns targeting public officials, defense contractors, and policy institutions
- Dark web and underground forum monitoring for data leak claims referencing Turkish entities

At present, Turkey does not appear to be a primary target. However, the country's strategic positioning and NATO membership elevate the probability of opportunistic or symbolic cyber activity if escalation persists.

Global Impact Assessment

Cyber Domain Expansion

The transition from shadow conflict to overt military exchange between Iran and Israel increases the likelihood of cyber domain expansion beyond the immediate region. Historically, similar escalations have resulted in:

- Global DDoS waves targeting allied states
- Ideologically motivated hacktivist mobilization
- Copycat operations by unaffiliated actors seeking visibility
- Opportunistic ransomware activity exploiting geopolitical distraction

While current activity remains largely disruption-focused, escalation could create conditions conducive to more sophisticated campaigns, including supply chain targeting or credential harvesting against multinational organizations.

Economic and Infrastructure Implications

Global markets may experience indirect pressure through:

- Energy price volatility
- Disruption to maritime routes in strategic waterways
- Increased insurance and risk premiums for regional operations

Critical infrastructure operators worldwide particularly those connected to Middle Eastern energy flows should maintain elevated situational awareness. Financial services institutions may also observe increased DDoS attempts, particularly from ideologically aligned hacktivist groups seeking symbolic targets.

Threat Actor Ecosystem Mobilization

Periods of geopolitical escalation often catalyze broader underground ecosystem activity. This includes:

- Recruitment messaging within extremist or nationalist online communities
- Collaboration between loosely affiliated hacktivist collectives
- Amplification of propaganda via coordinated bot networks
- Opportunistic scams leveraging conflict-related themes

Although state-aligned actors tend to operate with discipline, the broader ecosystem including unaffiliated cybercriminal groups may exploit instability for financial gain.

Conclusion

The current escalation between Iran and Israel represents a significant shift from prolonged shadow confrontation to overt military engagement. This transition has immediate implications not only for regional security but also for the cyber threat landscape.

Key assessments include:

- Pro-Iranian hacktivist groups are currently driving visible cyber disruption activity, primarily through DDoS campaigns and defacements.
- Pro-Israeli cyber operations remain comparatively stealthy and attribution-challenged.
- The most probable near-term cyber threat vector remains high-volume disruption rather than destructive infrastructure attacks.
- Escalation pathways toward targeted access operations, credential harvesting, and intelligence-driven campaigns remain plausible if kinetic hostilities intensify.

For Turkey and other regionally connected states, the primary risk lies in spillover effects, opportunistic targeting, and influence operations rather than direct strategic cyber warfare.

Globally, organizations should interpret the current situation as a catalyst for elevated cyber risk particularly in sectors linked to government services, defense, finance, media, and energy.

Continued monitoring of underground communications, rapid response readiness for disruption campaigns, and strengthened authentication and perimeter controls are recommended as baseline defensive measures during this escalation cycle.