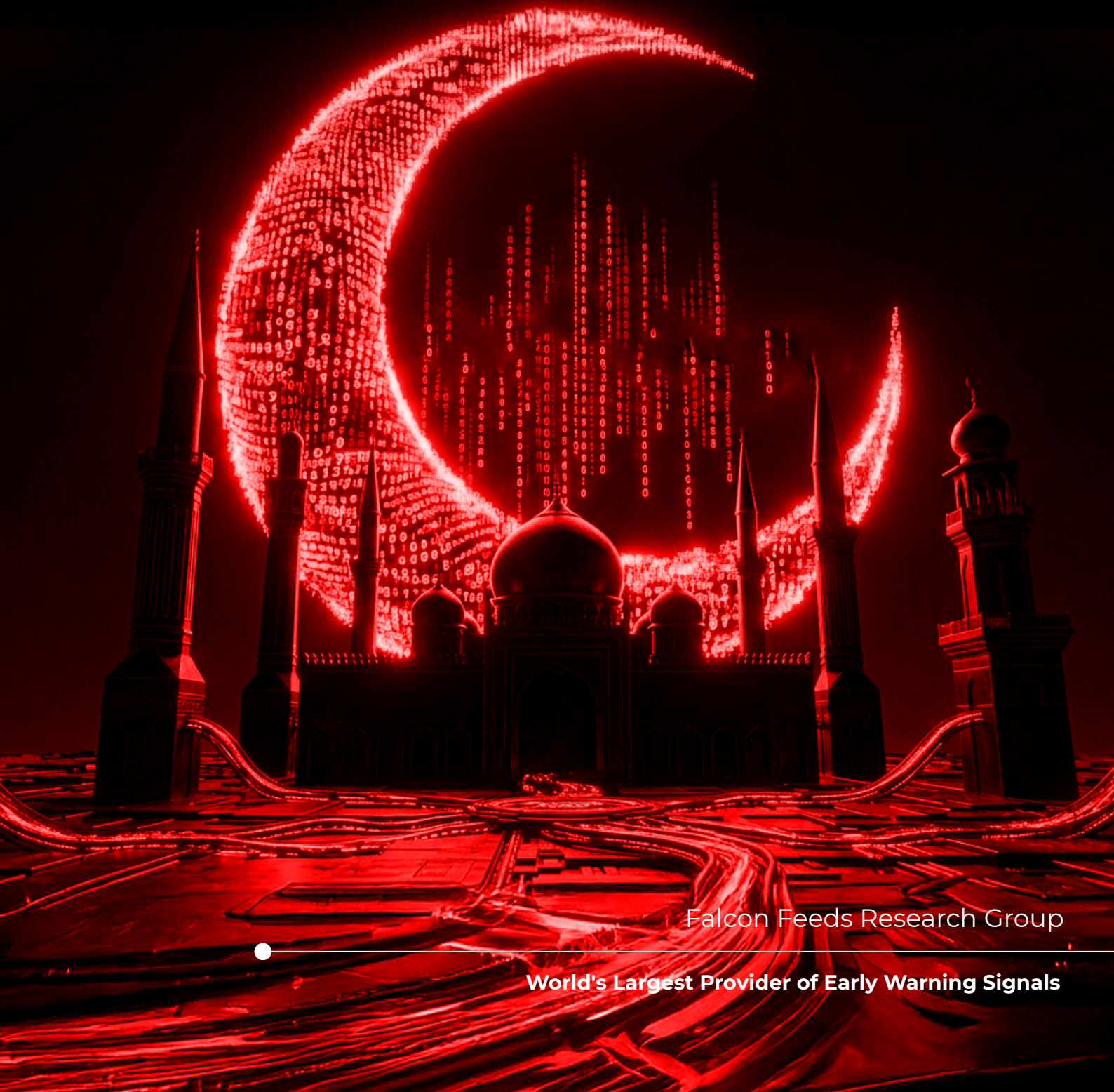
FalconFeeds

Democratising Cybersecurity
www.falconfeeds.io

CYBER ISLAMIC RESISTANCE-AXIS

& the Iran–Israel Shadow War



Falcon Feeds Research Group

World's Largest Provider of Early Warning Signals

The Deepest Watch on the Darkest Web

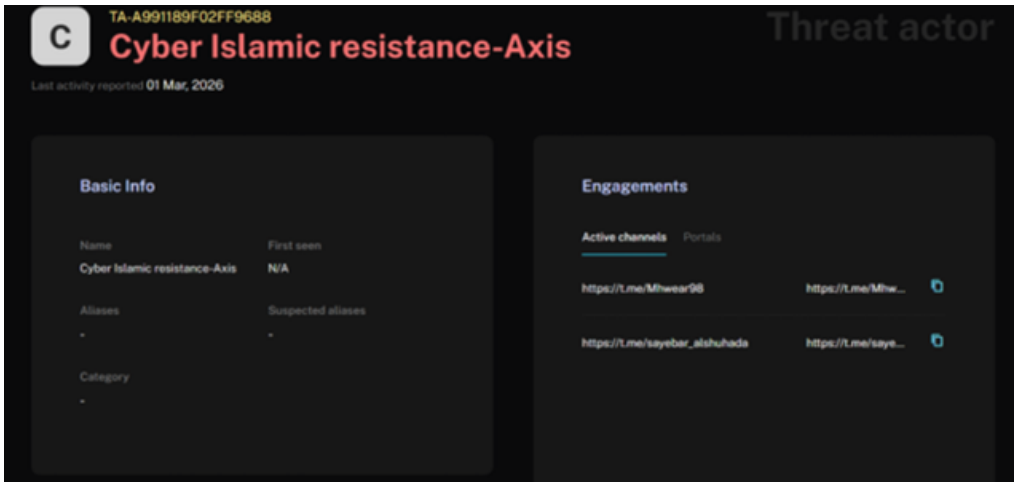
FalconFeeds.io delivers the largest real-time monitoring of deep and dark web activity—from ransomware gangs to Telegram dumps and access marketplaces.

Iran–Israel Cyber Shadow War Brief

Cyber Islamic Resistance-Axis is a pro-Iranian hacktivist group operating under the Axis of Resistance. It mainly uses Telegram and acts as a cyber proxy for Iran, targeting governments and organisations it sees as hostile to Iran, supportive of Israel, or opposed to Iran-aligned groups such as Hezbollah, Hamas, and the Houthis.

The group uses ideological and religious messaging inspired by Shi'a resistance movements. Its operations are branded as "The Great Epic Battle within the War of the Hereafter", language drawn from Quranic eschatology and used to justify cyberattacks against Israel and the U.S., signalling alignment with Iran's IRGC doctrine.

The group's activity grew alongside the escalating Iran–Israel conflict. It has since conducted DDoS attacks, claimed infrastructure intrusions, and coordinated with allied groups across sectors in Israel, the U.S., and the wider Middle East. Recent operations have targeted Israeli drone detection and air-defense systems.



KEY STATISTICS

- **Active Telegram Channels:** 4 (Primary, Backup, Thar Allah Brigade, Affiliated)
- **Primary Platform:** Telegram + X (Formerly Twitter)
- **Countries Targeted:** Israel, Usa, Plus Broader Western Asia & Americas
- **Industries Targeted:** 12+ Documented
- **Victim organisations documented:** 15+ Confirmed; additional claimed
- **Primary Ttps:** DDoS, Network Intrusion, Critical Infrastructure Targeting, Information Operations, Coalition Coordination
- **Threat Level:** Medium-high

Threat Actor Profile

Identity and Ideology

Cyber Islamic Resistance-Axis positions itself as part of the Iranian-led Axis of Resistance, aligning ideologically with groups such as Hezbollah, the Houthis, Hamas, and Iraqi PMU factions. Its communications—mainly in Arabic—use strong religious and political messaging, frequently quoting Quranic verses, framing operations as acts of jihad carried out by "mujahideen," and portraying targets as enemies of Islam and the oppressors of Palestine.

The group consistently signs its operations with the hashtags #**Cyber_Islamic_Resistance and #Cyber_Islamic_Resistance_Axis**, and its statements often include Quranic citations to justify attacks. It brands its overall campaign as **"The Great Epic Battle,"** echoing the apocalyptic language commonly used by IRGC-aligned militias in the region.

Structurally, the group mirrors Iranian proxy organisations by using named "brigades" with specific operational roles—an unusual level of organisation for hacktivist groups. Although no official state attribution exists, its behaviour aligns closely with Iran-supported or Iran-directed cyber proxies documented by intelligence agencies.

Active Communication Channels

- **Primary Telegram:** @Mhwear98
- **Backup Telegram:** @Mehwar99
- **Affiliated Group:** @CEArmy (C_E_Army)
- **X (Twitter):** @Mhwear98

All operations and TTPs are claimed and coordinated via Telegram.

Iran–Israel Conflict Alignment Analysis

Strategic Positioning within the Axis of Resistance

Cyber Islamic Resistance-Axis targets Israeli infrastructure, Israeli civil society, and U.S. military assets, closely matching Iran's strategic goals in the Israel–Hamas conflict. It also uses an "Electronic Operations Room" to recruit and coordinate other hacktivist groups, allowing Iran to apply pressure on its adversaries while maintaining deniability.

The group brands its operations as the "War of the Hereafter," a phrase drawn from religious doctrine used by IRGC and Hezbollah to justify attacks against Israel. This links the group's cyber activities to the same ideological and strategic framework driving Iran-aligned militant operations across the region.

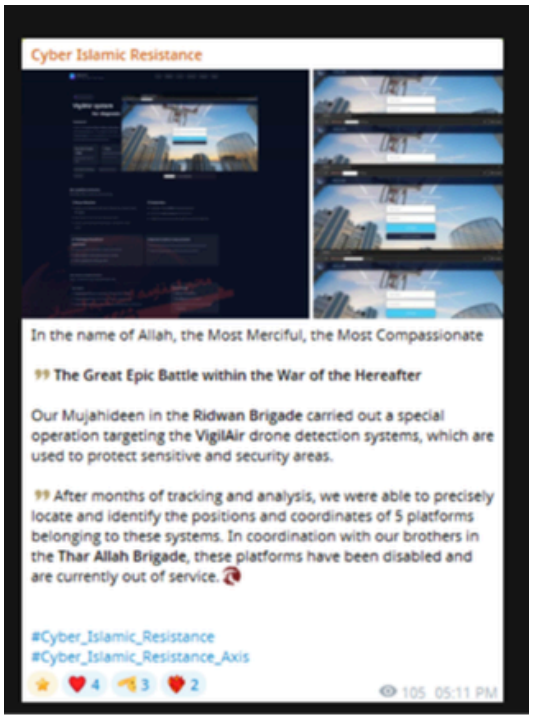
Activation and Operational Context

Unlike 313 Team, which activated precisely on 30 November 2023 in the immediate aftermath of October 7, Cyber Islamic Resistance-Axis has a longer operational history and represents a more established node within the Iranian-aligned cyber ecosystem.

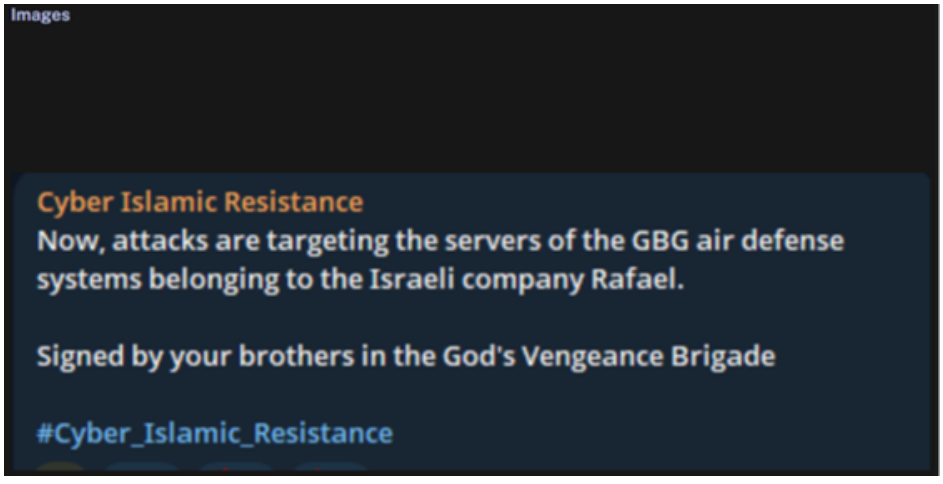
Its sustained activity through 2025 and into 2026 — including its most recent and most operationally significant claimed operation targeting VigilAir drone detection systems — indicates a mature and persistent threat actor with growing ambitions rather than a reactive mobilisation.

Direct Israeli Targets

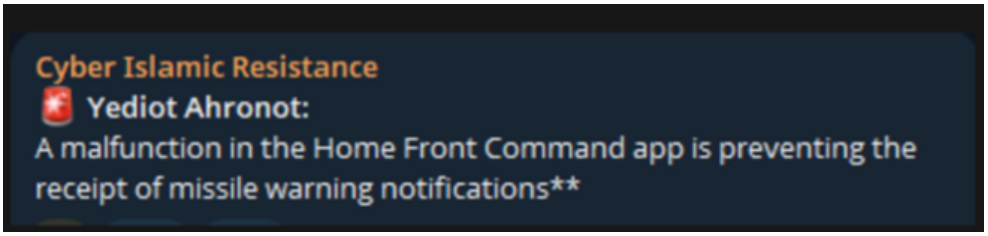
The following Israel-linked targets have been documented by FalconFeeds threat intelligence:
VigilAir Drone Detection Systems — Critical infrastructure; drone detection platforms used to protect sensitive Israeli military and security zones. The group's Ridwan Brigade claimed months of tracking and reconnaissance to identify the physical coordinates of five platforms, then claimed disablement in coordination with the Thar Allah Brigade.



Rafael Advanced Defense Systems' GBG Air Defense unit, one of Israel's key air-defense pillars was reportedly targeted by the group's "God's Vengeance Brigade," which claims to have struck servers linked to the GBG system

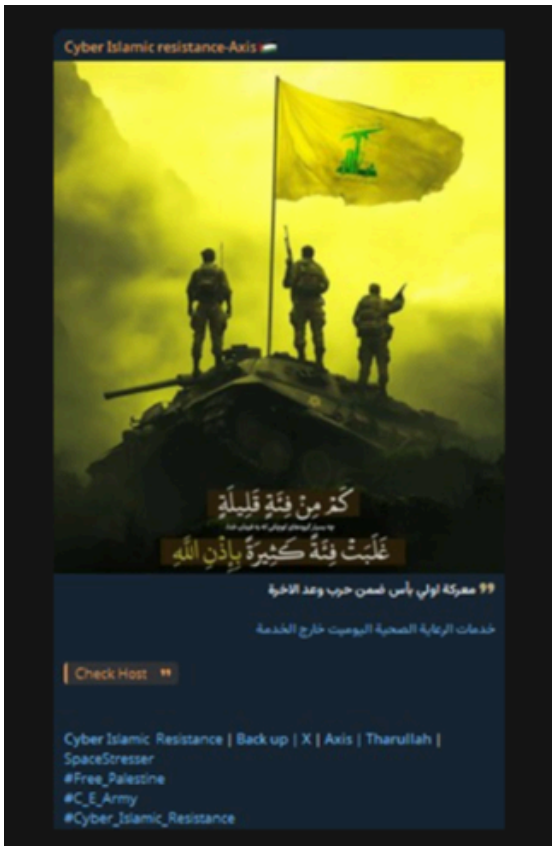


Israel's Home Front Command app—responsible for missile alerts to civilians—experienced a malfunction that blocked warnings. The group quickly seized the moment, claiming responsibility and amplifying the outage to portray it as a direct hit on Israel's emergency-alert system.



Hebrew University of Jerusalem (new.huji.ac.il) — Education sector; DDoS attack claimed with check-host.net downtime verification.

Leumit, Maccabi, and Meuhedet Health Services (Israeli healthcare system): 3 of Israel's largest health funds targeted simultaneously.



Additional Israeli Civilian & Institutional Targets

- **PayPlus** (payplus.co.il) — Financial services; Israeli payment platform.
- **Municipality of Lod** (lod.muni.il) — Government administration; local municipal government.
- **Wikimedia Israel** (wikimedia.org.il) — Non-profit and open knowledge; DDoS attack sustained for one hour.
- **The Israel Museum, Jerusalem** (imj.org.il) — Cultural institution.
- **Temple Mount Sifting Project** (tmsifting.org) — Archaeological and cultural institution.
- **Maayan Magazine** (maayanmagazine.com) — Israeli literary and cultural publishing; DDoS attack sustained for one hour.
- **Netivot Moshe Schools** — Education sector.
- **DGM Technology** (dgm.co.il) — Information technology services.
- **Michlala** (michlala.com) — Academic institution.

U.S. Targeting in the Iran–Israel Proxy Conflict

Strike on U.S. Military Digital Infrastructure

The group hit the MilitaryINSTALLATIONS / MilitaryONESOURCE portal with a DDoS attack, supported by check-host.net proof. They followed it with a stark warning: “We will strike you until the end and we will not hesitate to strike you”, signalling a sharp escalation against U.S. military-linked systems in response to American support for Israel.

Iranian Regime Alignment Signals

Clear indicators show the group’s pro-Iranian alignment, extending beyond Palestinian solidarity to active support for Iranian state interests:

- Use of the **“Axis of Resistance” (محور المقاومة)** framework — Iran’s formal proxy coalition.
- Reliance on Islamic resistance rhetoric mirroring **IRGC Quds Force and Iraqi PMU** communications.
- Presence of named internal brigades — the **Ridwan Brigade** (intelligence) and **Thar Allah Brigade** (strikes) — reflecting Iranian **paramilitary-style structure.**
- Targeting key Israeli defense systems like **VigilAir** and **Rafael GBG**, directly aligning with Iran’s strategy to weaken Israel’s air-defense and drone detection capabilities.
- Coordination through an **Electronic Operations Room,** recruiting allied groups under a **unified command,** mirroring Iranian **cyber-proxy models.**

Targeting Analysis

Primary Target Geography

The group hit the MilitaryINSTALLATIONS / MilitaryONESOURCE portal with a DDoS attack, supported by check-host.net proof. They followed it with a stark warning: “We will strike you until the end and we will not hesitate to strike you”, signalling a sharp escalation against U.S. military-linked systems in response to American support for Israel.

- **Israel — Primary adversary**

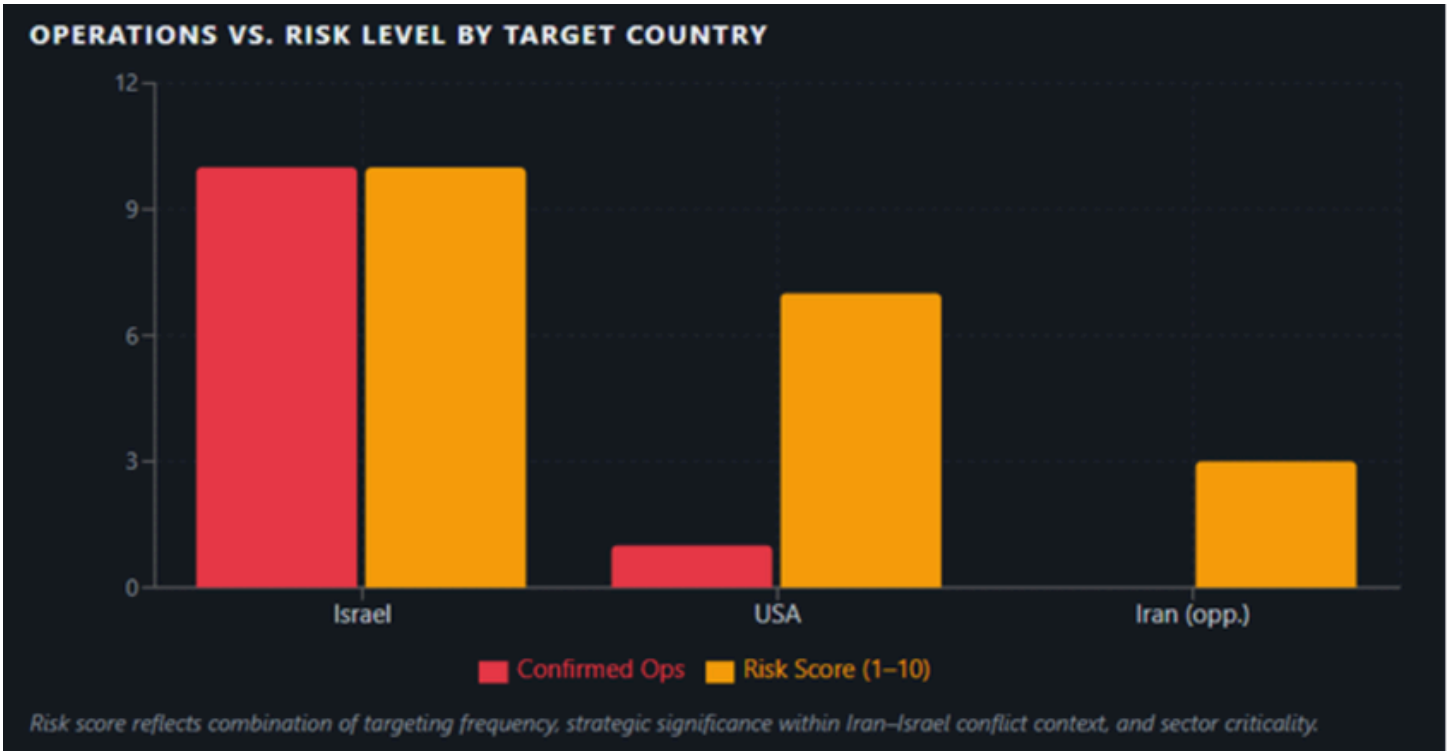
  Targets span defense, health, education, government, finance, culture, and civil-emergency infrastructure.
  Risk: CRITICAL

- **United States — Israel’s main security guarantor**

  Targeting includes a U.S. military portal, accompanied by escalatory messaging.
  Risk: HIGH

- **Iran — Contextual targeting**

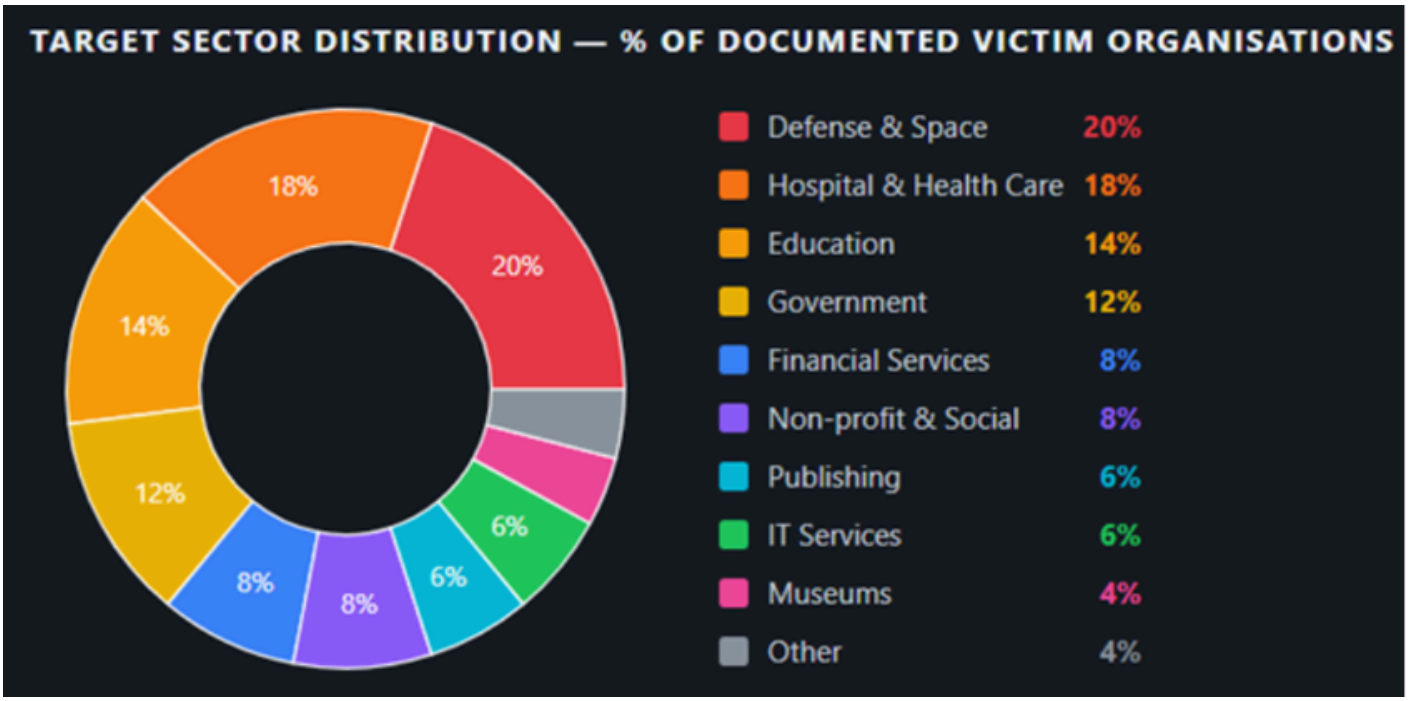
  Likely refers to internal opposition or diaspora groups hostile to the Iranian regime.
  Risk: CONTEXTUAL



Confirmed Target Sectors

The group's documented targeting spans 12 industries. Highest-priority sectors based on operational frequency and strategic significance:

- **Defense & Space** — Targets include **VigilAir** and **Rafael GBG**, aligning with Iran's aim to weaken Israeli military defense systems.
- **Government & Public Sector** — Includes the **Municipality of Lod** and a **U.S. military portal**, indicating political signalling and disruption.
- **Hospital & Health Care** — **Leumit, Maccabi, and Meuhedet** health services attacked simultaneously, showing intent to disrupt civilian healthcare.
- **Education** — Targets such as Hebrew University, Netivot Moshe Schools, and Michlala, revealing a pattern of striking Israeli academic institutions.
- **Financial Services** — **PayPlus**, indicating an economic disruption objective.
- **Information Technology (IT) Services** — **DGM Technology**, focusing on supply-chain and IT infrastructure.
- **Non-profit & Social Organizations** — **Wikimedia Israel**, targeting civil society platforms.
- **Museums & Institutions** — **Israel Museum, Jerusalem**, a symbolic cultural target.
- **Publishing Industry** — **Maayan Magazine**, targeting cultural soft power.
- **Health & Fitness** — Listed in the group's sector profile.
- **Government Administration — Municipality of Lod**, signalling local government disruption

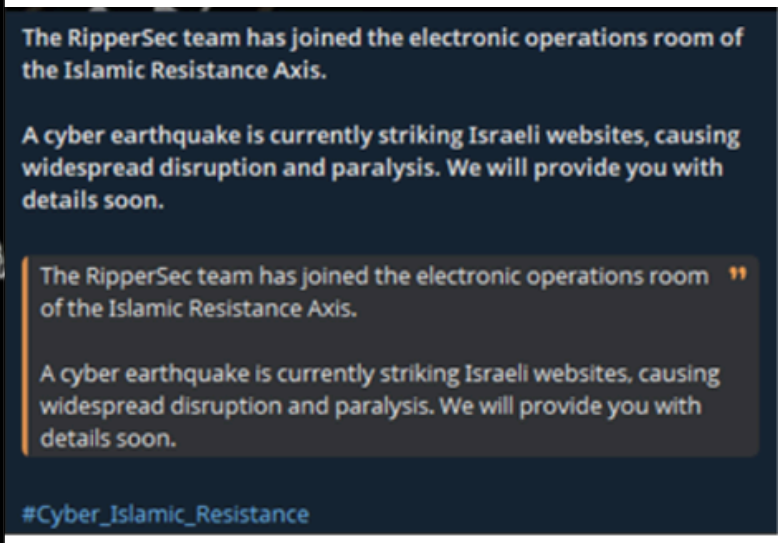


Coalition And Affiliated Actors

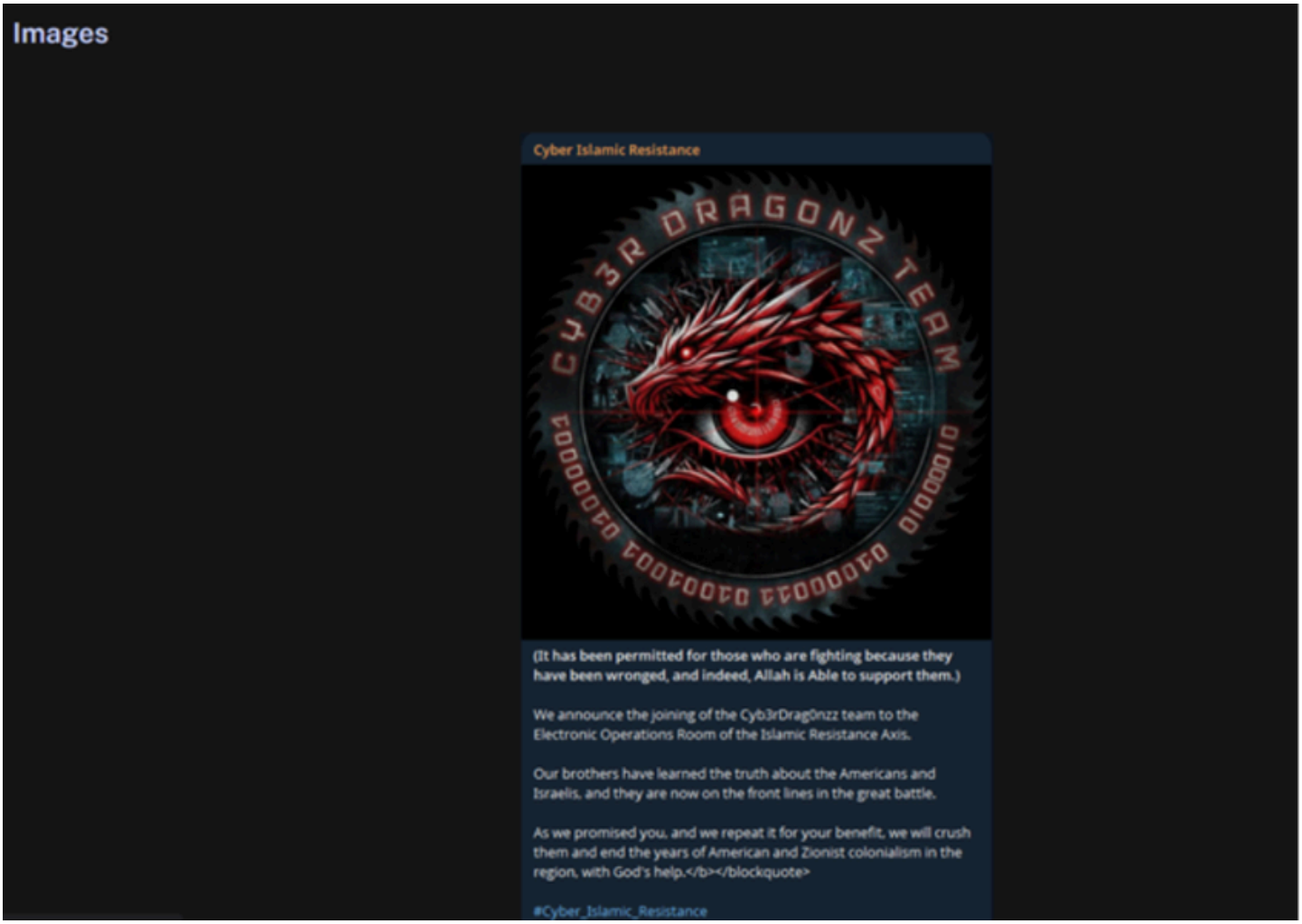
One of the most strategically significant aspects of Cyber Islamic Resistance-Axis is its role as a **coordinator and force multiplier** within a broader coalition of hacktivist groups. The group operates what it designates as the "**Electronic Operations Room of the Islamic Resistance Axis"**, a formal coordination structure through which it recruits, onboards, and directs allied hacker groups. This model mirrors Iranian proxy military coordination structures and significantly amplifies the coalition's effective attack surface.

Confirmed Allied Groups:

- **RipperSec —** High-profile pro-Palestinian hacktivist group; known for DDoS and defacements; its joining significantly boosts the coalition's attack capacity.



- **Cyb3rDrag0nzz** — Joined the Electronic Operations Room in March 2026; frames its role as part of ending “American and Zionist colonialism.”



- **C_E_Army** — Affiliated actor frequently appearing in group signatures and hashtags, indicating a wider coordinated network.

- **Thar Allah Brigade (God’s Vengeance Brigade) —** Offensive strike unit responsible for executing attacks, including the Rafael GBG server targeting.

- **Ridwan Brigade —** Intelligence and reconnaissance unit; conducted months-long tracking to identify VigilAir drone detection system coordinates.

TACTICS, TECHNIQUES AND PROCEDURES (TTPs)

Detailed Breakdown of the Group's Core Cyber Tactics and Capabilities

DDoS Attacks

- Their **primary capability**, using large-scale, one-hour waves hitting multiple targets.
- Always provide **check-host.net** proof to validate attacks — unlike low-tier groups.
- Use commercial **booter/stresser** tools like SpaceStresser to boost attack volume.

Critical Infrastructure Targeting

- A more advanced capability involving **VigilAir** and **Rafael GBG** air-defense systems.
- Requires **reconnaissance, mapping, and coordinated brigade operations,** showing higher sophistication.

Network Intrusion & Data Collection

- Claims include compromising **Israeli routers** and extracting **physical address data.**
- If true, this supports **intelligence gathering** and could enable further cyber or physical operations.

Information Operations (PSYOP)

- All attacks are broadcast **live on Telegram** with screenshots, downtime proof, and religious messaging.
- Exploit events—like the **Home Front Command app malfunction**—to create **fear and psychological impact.**

Coalition Building & Force Multiplication

- The Electronic Operations Room recruits groups like RipperSec and Cyb3rDrag0nzz.
- Creates a multi-actor, multi-vector attack force across several sectors and regions.

Operational Signature Patterns

- Consistent hashtags: **#Cyber_Islamic_Resistance** and **#Cyber_Islamic_Resistance_Axis.**
- Campaign framed as **“The Great Epic Battle within the War of the Hereafter.”**
- Every DDoS attack includes **check-host verification.**
- Operates through a **multi-channel Telegram structure** (primary, backup, brigade channels).

MITRE ATT&CK MAPPING

Breakdown of Offensive Capabilities Aligned to MITRE ATT&CK Techniques

TA0040 — Impact

- **T1498 — Network Denial of Service:** Sustained, high-volume DDoS attacks on Israeli and U.S. websites.
- **T1498.001 — Direct Network Flood:** Intense HTTP/HTTPS flooding validated with check-host.net.
- **T1489 — Service Stop:** Claimed shutdown of VigilAir and Rafael GBG defense systems.

TA0043 — Reconnaissance

- **T1595.001 — Active Scanning:** Ridwan Brigade performed months-long mapping of VigilAir coordinates.
- **T1596 — Search Open Technical Databases:** OSINT scanning of Israeli organisational infrastructure.
- **T1591 — Gather Victim Information:** Collected details on sectors, infrastructure, and web-facing assets.

TA0001 — Initial Access

- **T1190 — Exploit Public-Facing Applications:** Claimed compromise of Israeli routers via default credentials or vulnerabilities.
- **T1133 — External Remote Services:** Used exposed remote-management interfaces to access edge devices.

TA0009 — Collection

- **T1005 — Data from Local System:** Extracted physical address data from compromised routers.

TA0011 — Command and Control

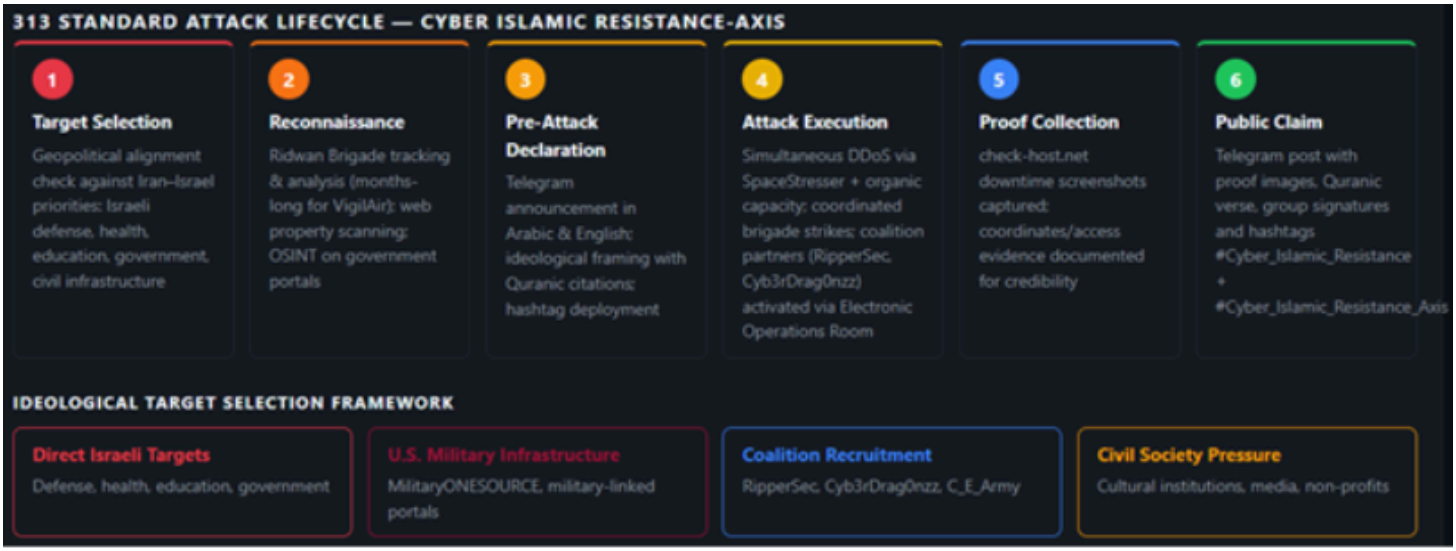
- **T1102 — Web Services:** Telegram used as the main C2 + public broadcast platform, with primary, backup, and brigade channels.

TA0042 — Resource Development

- **T1583.006 — Acquire Infrastructure:** Use of **SpaceStresser** for DDoS-for-hire.
- **T1585 — Establish Accounts:** Multiple Telegram and X accounts created and maintained.
- **T1588 — Obtain Capabilities:** Leveraged coalition partners **(RipperSec, Cyb3rDrag0nzz)** to enhance operational capacity.

TA0014 — Psychological Operations (PSYOP)

- **T1566 — Information Operations:** Real-time attack broadcasts, Quranic messaging, brigade announcements, screenshots, and downtime proof to amplify fear and psychological impact.



INDICATORS OF COMPROMISE (IOCs)

Important Note:

Cyber Islamic Resistance-Axis mainly conducts DDoS attacks, network intrusion claims, and information operations. Unlike advanced APT groups, it does not rely on custom malware or persistent C2 infrastructure. Instead, its IOC footprint is shaped by targeted systems, communication channels, and third-party tools. No malware files or hashes are attributed to the group in the FalconFeeds IOC database. All listed IOCs come directly from operational intelligence gathered through FalconFeeds threat feeds.

Third-Party Attack Infrastructure and Tools

Type	Indicator	Context	Confidence
Domain	spacestresser.com	DDoS-for-hire (booter/stresser) service explicitly referenced in group's operational posts	High
Service	check-host.net	Third-party proof-of-downtime verification service used systematically across all DDoS claims	High

Telegram and Social Media Actor Infrastructure

Type	Indicator	Context
Telegram Handle	@Mhwear98	Primary operational channel — all operations claimed here
Telegram Handle	@Mehwar99	Backup/secondary channel
Telegram Handle	@Mhwear100	Thar Allah Brigade (God's Vengeance Brigade) dedicated channel
Telegram Handle	@sayebar_alshuhada	Secondary affiliated channel
Telegram Handle	@CEArmy	C_E_Army affiliated group channel
X (Twitter) Handle	@Mhwear98	Cross-platform amplification and PSYOP account

Confirmed Attack Target Domains (Network-Layer IOCs)

Domain	Organisation	Country	Attack Type
installations.militaryonesource.mil	U.S. MilitaryINSTALLATIONS	USA	DDoS
new.huji.ac.il	Hebrew University of Jerusalem	Israel	DDoS
wikimedia.org.il	Wikimedia Israel	Israel	DDoS
maayanmagazine.com	Maayan Magazine	Israel	DDoS
leumit.co.il	Leumit Health Services	Israel	Claimed attack
maccabi4u.co.il	Maccabi Health Services	Israel	Claimed attack
meuhedet.co.il	Meuhedet Health Services	Israel	Claimed attack
payplus.co.il	PayPlus Financial Services	Israel	Claimed attack
lod.muni.il	Municipality of Lod	Israel	Claimed attack
imj.org.il	The Israel Museum, Jerusalem	Israel	Claimed attack
tmsifting.org	Temple Mount Sifting Project	Israel	Claimed attack
dgm.co.il	DGM Technology	Israel	Claimed attack
michlala.com	Michlala Academic Institution	Israel	Claimed attack

Campaign and Behavioural Signatures

Type	Indicator	Context
Hashtag	#Cyber_Islamic_Resistance	Universal operational signature across all claims
Hashtag	#Cyber_Islamic_Resistance_Axis	Used in coalition-level operation announcements
Hashtag	#Free_Palestine	Used in DDoS attack posts as ideological framing
Hashtag	#The_Great_Epic	Campaign tracking hashtag
Campaign Name	"The Great Epic Battle within the War of the Hereafter"	Overarching campaign branding in all communiqués
Verification Pattern	check-host.net proof-of-downtime links appended to all DDoS claims	Consistent operational credibility behaviour

Defensive Recommendations

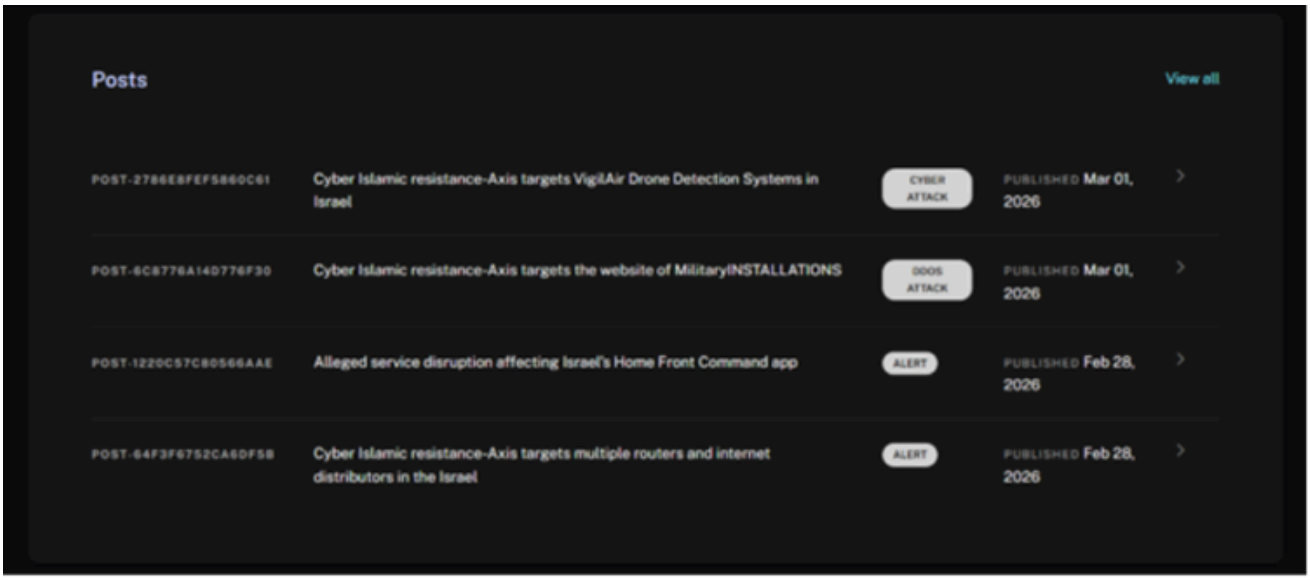
For entities within the identified target profile — particularly Israeli defense, health, government, education, financial, and civil society sectors, and U.S. military-linked digital infrastructure:

- **Deploy enterprise-grade DDoS protection with CDN volumetric scrubbing** for multi-actor attacks like those involving RipperSec.
- **Monitor Telegram channels @Mhwear98 and @Mhwear100 for pre-attack alerts.**
- **Audit routers and edge devices for unauthorised access, default credentials, and unpatched firmware.**
- **Enable uptime monitoring + automated alerts** on all **public-facing assets** listed in the IOC table.
- **Use incident-response playbooks** for **critical infrastructure claims**, focusing on **rapid verification and public communication.**
- **Share IOCs and TTPs with CERTs, CISA**, and regional cybersecurity bodies in **Israel** and the **U.S.**
- **Increase alert posture** during **Iran–Israel escalations** (ceasefires, military operations, political shifts, significant Shi'a dates).
- **Treat coalition recruitment updates** (e.g., **RipperSec, Cyb3rDrag0nzz**) as signs of **imminent multi-vector attack waves.**
- **Review credential hygiene and CMS integrity** for **defense-adjacent and government-linked websites.**
- **Block or monitor traffic** related to known **DDoS booter services like SpaceStresser (spacestresser.com).**

HOW FALCONFEEDS.IO CAN HELP

FalconFeeds.io provides real-time intelligence on threat actors, hacktivist campaigns, dark-web activity, and IOCs. For organisations targeted by Cyber Islamic Resistance-Axis — including Israeli defense, health, education, government, finance, and U.S. military-linked sectors — it offers fast, actionable visibility into emerging threats

- **Real-time actor monitoring** — Live tracking of the Cyber Islamic Resistance-Axis via directly sourced Telegram updates, enabling pre-attack warning windows.
- **Structured threat feeds** — Every operation is categorised by attack type, victim country, industry, organisation, and domain for seamless SIEM/SOAR integration.
- **IOC distribution** — Provides target domains, Telegram infrastructure identifiers, behavioural signatures, and booter tool indicators in structured formats for defensive controls.
- **Ecosystem mapping** — Visualises relationships between groups such as RipperSec and Cyb3rDrag0nzz, helping analysts understand coalition behaviour and anticipate coordinated attack surges.
- **Historical intelligence archive** — Searchable history of all group operations for pattern analysis, threat briefings, and incident-response timelines.
- **API access** — Direct ingestion of threat actor profiles, feeds, and IOCs into SIEM, SOAR, and TIP environments for automated workflows.
- **Broader Axis of Resistance coverage** — Tracks the full Iranian-aligned cyber ecosystem, improving regional threat modelling and cross-actor correlation.



Conclusion

Cyber Islamic Resistance-Axis continues to operate as a highly active, Iranian-aligned hacktivist actor whose tactics, ideology, and target selection closely reflect Iran's strategic goals in the ongoing regional conflict. Its use of DDoS attacks, infrastructure targeting, coordinated coalition activity, and psychological operations demonstrates a maturing threat profile with growing regional impact.

As tensions persist, organisations across Israeli and U.S. defense, government, health, education, and financial sectors must remain alert and strengthen monitoring, readiness, and threat-intelligence integration to counter this evolving threat.