

How hacktivist cyber operations surged amid Israeli-Iranian conflict

By charliesmith

Published: 2025-07-01 · Archived: 2026-06-04 02:00:11 UTC

Written By

In June 2025, Israel carried out airstrikes against key Iranian military and nuclear facilities. Iran swiftly retaliated, escalating regional tensions to unprecedented levels. This military confrontation has not only unfolded in conventional warfare but also triggered a massive **surge in cyber operations**.

Almost immediately after the kinetic attacks, numerous hacktivist groups began launching cyberattacks primarily targeting Israel and its international allies. The vast majority of these groups present themselves as pro-Iranian and pro-Palestinian actors, motivated by ideological, political, and religious narratives.

However, cybersecurity analysts caution that certain attacks may involve nation-state actors disguising their activity behind the facade of hacktivism. This phenomenon is widely referred to as **faketivism**.

Summary of hacktivist activity in the Israel-Iran conflict

This article provides a comprehensive, evidence-based analysis of the hacktivist activity surrounding the Israeli-Iranian conflict, examining public statements, claimed attacks, profiles of the key actors involved, and emerging patterns suggesting state-sponsored faketivist involvement.

- Over **80 distinct hacktivist groups** are actively conducting or supporting offensive cyber operations targeting Israel and its allies. To a lesser extent, there are some hacktivist groups supporting Israel as well.
- Primary motivations of these groups include **pro-Palestinian solidarity, anti-Western sentiment, Islamic ideological alignment**, and in some cases, direct **support for Iranian geopolitical objectives**.
- Attacks span across government, military, defense contractors, judicial systems, energy infrastructure, satellite operations, ICS/OT systems, social media platforms, and financial institutions.
- Several hacktivist entities (e.g., *Keymous+*, *Mr Hamza*, *Mysterious Team*, *Inteid*, *Cyber Islamic Resistance*) demonstrate coordination, sharing resources and intelligence, and form operational alliances.
- Suspected **faketivist entities** such as *CyberAv3ngers*, *Handala*, and *Predatory Sparrow* are likely operating with state support or directly under state direction.

Hacktivist groups' statements and strategic alliances

Following the Israeli military strikes on Iranian targets, dozens of hacktivist groups responded almost immediately with statements of solidarity and coordinated calls for cyber retaliation. Most of these communications occurred via **Telegram**, with some activity spilling onto X (formerly Twitter).

These public declarations are ideologically charged, often referencing anti-Zionist, pan-Islamic, and anti-Western narratives. Below is an overview of **key statements and alliances** made:

Mysterious Team Bangladesh

This group expressed full support for Iran, calling for “Operation True Promise 3” against Israel. The group warned Jordan, Egypt, and Saudi Arabia to avoid interfering with Iranian operations or risk retaliatory cyberattacks against their own infrastructure.

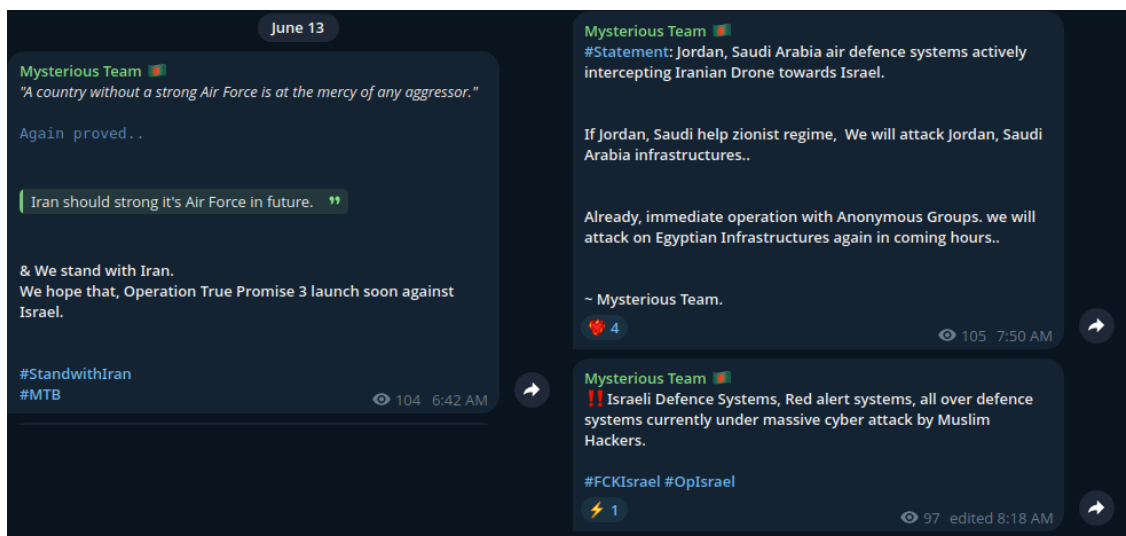


Figure 1: Mysterious Team Bangladesh announcing cyber operations against Israeli and regional defense systems supporting Israel.

Team Insane Pakistan

The pro-Pakistan hacktivist group expressed solidarity, urging Iran to aggressively challenge Israel. They compared the conflict to Pakistan’s recent confrontations with India.



Figure 2: Team Insane Pakistan showing explicit cyber support for Iran, framing its actions as resistance against regional powers.

Z-Alliance

In a statement written in Russian, *Z-Alliance* openly declared their full support for Iran. They rejected political neutrality and stated their readiness to conduct offensive operations without constraint.

June 17

Z-ALLIANCE 🇷🇺 🇮🇷 🇩🇪 🇫🇷 🇮🇹 🇮🇸 🇮🇶 🇮🇦

Официальное заявление

В условиях актуального ирано-израильского конфликта, когда многие предпочитают занимать позицию нейтралитета, заявляем следующее. Z-alliance не будет подчиняться чужим правилам и ограничиваться политикой компромиссов. Мы действуем по своим собственным убеждениям и на своих условиях — когда и где посчитаем нужным.

Мы открыто поддерживаем Иран в этом конфликте, признавая его право на защиту своих интересов и безопасности. От нас не стоит ждать деклараций о «принципах» или попыток выглядеть «порядочными». Наш подход прямой и решительный. В случае, если появится возможность — мы готовы действовать без оглядки, при необходимости используя любые средства, включая те, которые другие считают табу.

Это заявление — предупредительный сигнал: Z-alliance не будет ни пассивным наблюдателем, ни жертвой обстоятельств. Наши действия будут решительными и жесткими. Последствия таких действий полностью ложатся на тех, кто осмелится встать у нас на пути.

👍 5
❤️ 3
⚡ 2
👏 1
🔥 1

👁️ 57
📌
6:16 AM

Automated translation

Official statement

In the current Iranian-Israeli conflict, when many prefer to take a neutral position, we declare the following. Z-alliance will not obey someone else's rules and limit itself to a policy of compromise. We act according to our own convictions and on our own terms - when and where we deem it necessary.

We openly support Iran in this conflict, recognizing its right to defend its interests and security. We should not expect declarations of "principles" or attempts to appear "decent." Our approach is direct and decisive. If the opportunity arises, we are ready to act without looking back, if necessary using any means, including those that others consider taboo.

This statement is a warning signal: Z-alliance will not be a passive observer, nor a victim of circumstances. Our actions will be decisive and tough. The consequences of such actions will fall entirely on those who dare to stand in our way.

Figure 3: Z-Alliance openly declaring support for Iran and threatening cyber retaliation against perceived opponents.

Server Killers

Server Killers publicly aligned themselves with the anti-Israel campaign and initiated attacks against Israeli judicial, educational, and governmental web infrastructure. They simultaneously encouraged widespread participation from external supporters.



Figure 4: Server Killers explicitly calling for cyberattacks against Israeli governmental websites.

Akatsuki Cyber Team

Akatsuki Cyber Team positioned itself within the pan-Muslim hacktivist narrative, fully rejecting Israel's legitimacy as a state and expressing intentions to unite additional actors for a broader coordinated cyber offensive.



Figure 5: Akatsuki Cyber Team expressing refusal to recognize Israel and promising escalated cyberattacks.

GhostSec

GhostSec expanded its already ongoing campaigns against Israeli infrastructure, presenting a detailed summary of previously compromised Israeli water, industrial control, and satellite systems. The group outlined its ongoing multiphase attacks, reflecting both persistent operational capabilities and a continued escalation model.

GhostSec

With everything Israel is currently facing we will be adding the pressure, how we best can. The fight with Israel is not JUST about the oppression in Palestine while it started there Israel has continuously gone further and further, The fight is for all the nations affected by the injustice and wrong doings of the illegitimate "state" of Israel.

Besides shutting down over 500+ Websites and counting we present even more attacks

We have hit over 100 Modbus PLC devices affecting their industrial and OT systems all over the country

We have hacked over 40 Aegis 2 water devices, defacing some of them. And completely messing with the settings of the rest, Eventually shutting them down completely

We have hacked 8 Unitronics devices and after the absolute abuse of the systems shut them down too.

We have hacked a total of 10 VSAT devices belonging to Israel specifically the satellites we mentioned briefly in our previous posts affecting Satellites directly owned by Israel and the military.

We have a history of attacking Israel, all our previous attacks, breaches and much more. Our totalling record of 700+ devices hacked in the past year alone says a lot but today we provide a large scale attack to continue the pressure being applied on them.

Down with Israel, for a free world the oppressive and illegitimate state of Israel cannot continue with their shit.

We stand with all of you, We shout with all of you, We fight with all

Figure 6: GhostSec announcing attacks on Israeli infrastructure, detailing compromised Modbus and VSAT devices.

Keymous+ and Inteid

Keymous+ and *Inteid* announced collaboration, explicitly supporting Iranian cyberwar efforts and naming specific Israeli media targets, demonstrating operational coordination.

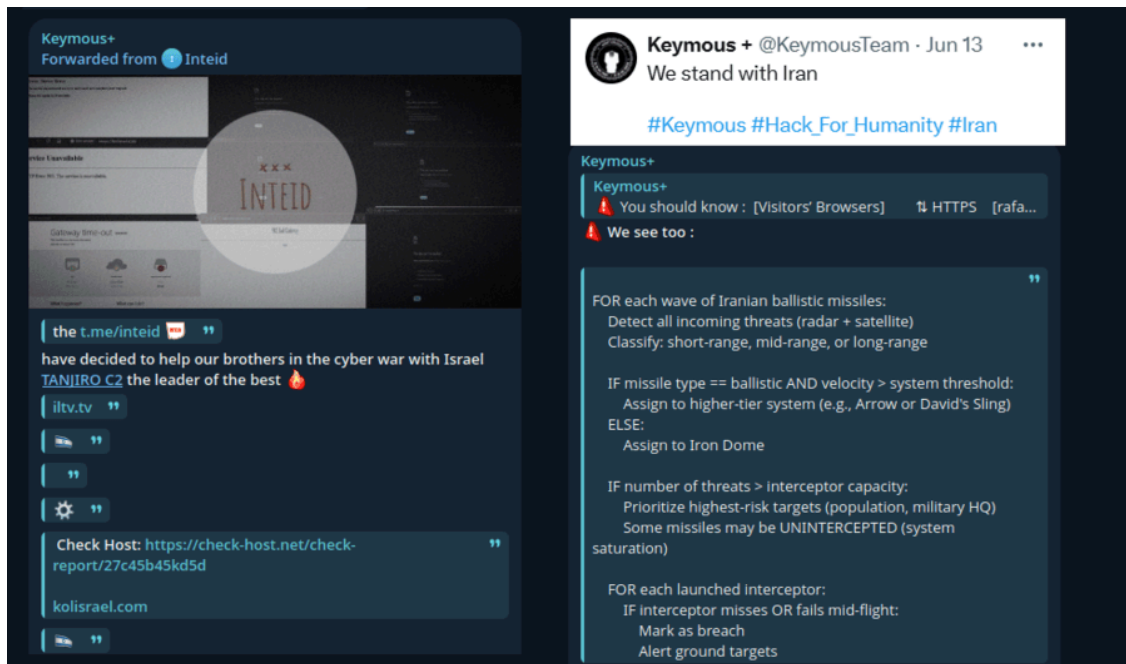


Figure 7: Keymous and Inteid groups coordinating cyberattacks supporting Iran against Israeli digital infrastructure.

Anonymous Kashmir and Mr Hamza Cyber Force

Anonymous Kashmir and Mr Hamza Cyber Force formalized their alliance, explicitly stating unity based on shared ideological motives. They emphasized joint efforts in support of Palestine and Iran.

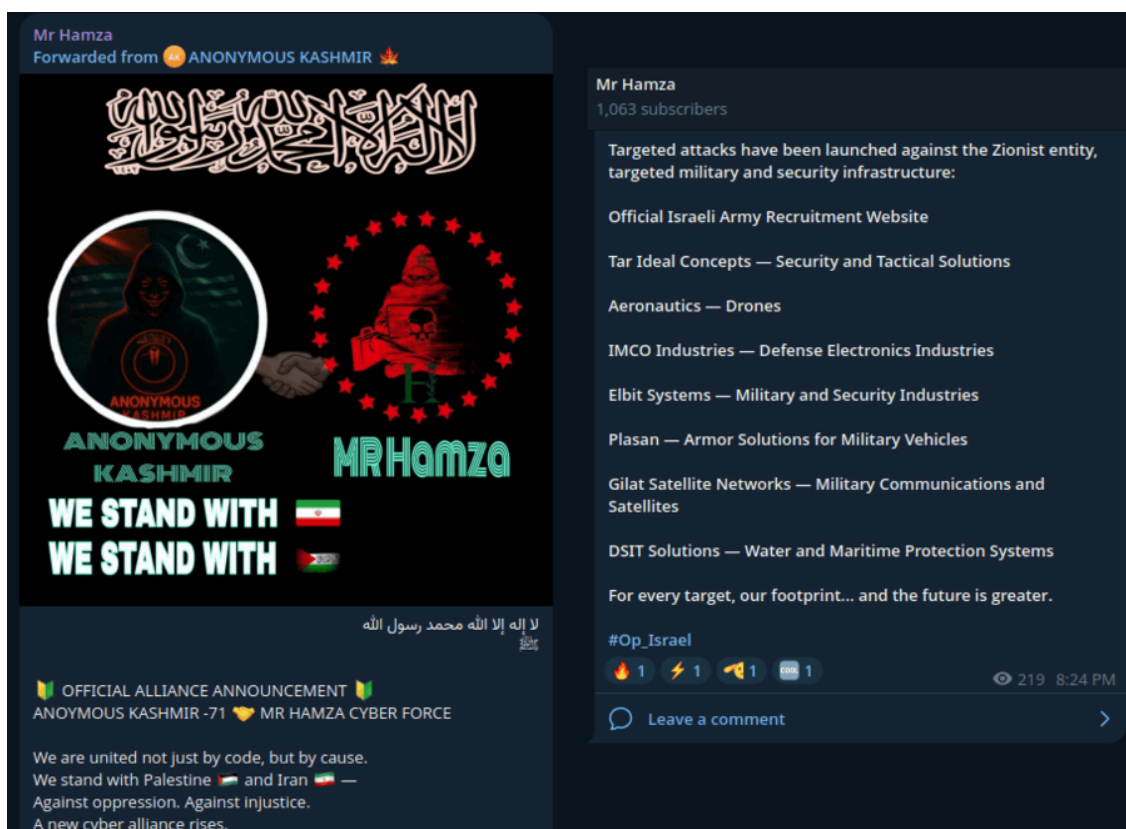


Figure 8: Mr Hamza and Anonymous Kashmir announcing an alliance and listing cyberattack targets in Israel.

DieNet

The group has positioned itself as a vocal supporter of Iran in the broader cyber conflict against Israel, amplifying Tehran's messaging while leveraging digital platforms for influence operations.



Figure 9: DieNet announcing support for Iran in an ongoing cyber conflict, detailing planned attacks on Israeli radio infrastructure.

BD Anonymous & Root Cyber 25

They have formed a new alliance with religious and ideological messaging, stating their intention to support Palestine and oppose Zionism, colonialism, and the West.

BD Anonymous



BD Anonymous **Root Cyber 25**

SAVE GAZA

ALLIANCE BD Anonymous Team 🇵🇸
Root Cyber 25
United for Justice | One Ummah One Mission

This is not just an alliance it is a call
A call to rise to awaken to stand for the truth when the world
chooses silence

Jihad is not just on the battlefield it is in every heart that refuses to
bow to injustice
It is in every soul that chooses truth over fear resistance over
silence unity over division

We are not just teams

Figure 10: BD Anonymous and Root Cyber 25 alliance banner promoting “One Ummah, One Mission”.

Claimed hacktivist cyber-attacks on Israeli government and critical industries

Hacktivist groups have claimed responsibility for a wide range of cyberattacks on Israeli systems. While many of these claims remain unverified, they reveal the breadth and ambition of these actors, from symbolic defacements to alleged disruptions of critical infrastructure.

Here is a structured breakdown of publicly claimed attacks:

Industry Sector	Organization / Targeted Systems	Claiming Hacktivist Group
Academic & Research Institutions	Weizmann Institute of Science (Data exfiltration)	Handala Hack
Agriculture & Food Security	Israeli Ministry of Agriculture and Food Security (data leak)	Digital Ghost
Commercial Services	BeatBox Karaoke (Israeli entertainment chain)	DieNet
Energy Infrastructure	Delek Group	Handala Hack
Energy Infrastructure	Paz Oil Company, Rapac Energy	Mr Hamza
Energy Infrastructure	Haifa Refinery, oil pipelines, gas transmission lines	Laneh
Financial Institutions	BNP Paribas Israel	R3VOXAnonymous
Financial Institutions	Mercantile Discount Bank (Israel)	Inteid
Financial Institutions	Agura B.C., LTD (crypto infrastructure vendor, Haifa)	Handala Hack
Financial Institutions	Nobitex (Iranian crypto exchange)	Gonjeshke Darande
Government Alert Systems	Tzofar Red Alert System	GhostSec, DieNet

<i>Government Institutions</i>	Israeli Judicial Authority, Supreme Court of Israel	<i>Server Killers</i>
<i>Government Institutions</i>	Israeli Ministry of Education	<i>Server Killers, R3VOXAnonymous, Dark Storm Team</i>
<i>Government Institutions</i>	Jordanian Ministry of Education	<i>Arabian Ghosts</i>
<i>Government Institutions</i>	Israel Ministry of Justice	<i>Dark Storm Team</i>
<i>Government Institutions</i>	Israel State Archives	<i>Dark Storm Team</i>
<i>Government Institutions</i>	Israel Tax Authority	<i>Dark Storm Team</i>
<i>Government Institutions</i>	Israel Supreme Court	<i>Dark Storm Team</i>
<i>ICS/OT Systems</i>	100+ Modbus PLC devices, 40+ Aegis 2 water control devices, 8 Unitronics devices	<i>GhostSec</i>
<i>ICS/OT Systems</i>	Siemens S7 PLCs in Tel Aviv	<i>SYLHET GANG SG</i>
<i>Internet Infrastructure</i>	Tel Aviv Internet (ISP: R.L Internet and Networks Ltd.)	<i>Cyber Islamic Resistance</i>
<i>Logistics</i>	Part2Port (port logistics)	<i>Mr Hamza</i>
<i>Logistics</i>	Mor-Logistics Ltd (425GB data leak)	<i>Handala Hack</i>
<i>Media Networks</i>	Israeli television network TBN (data deletion)	<i>Cyber Islamic Resistance / @zerodayx1</i>
<i>Media Networks</i>	Israeli Radio Live services	<i>DieNet</i>
<i>Media Networks</i>	IsraelNews.co.il, Nana10.co.il	<i>Arabian Ghosts</i>
<i>Media Networks</i>	Times of Israel (DoS outage)	<i>Cyber Jihad Movement, Team Fearless (JOS)</i>
<i>Military & Security</i>	Cyber Command operations under IDF Maj. Gen. Shlomi Binder	<i>Handala Hack</i>

<i>Military & Security</i>	Ashot Ashkelon Industries, Meprolight, Orbit Communications Systems	<i>Mr Hamza</i>
<i>Military & Security</i>	Elbit Systems, Aeronautics, IMCO, Plasan, DSIT Solutions, Tar Ideal Concepts	<i>Mr Hamza</i>
<i>Military & Security</i>	Iron Dome System (alleged data leak)	<i>Digital Ghost</i>
<i>Municipal Infrastructure</i>	Israel Antiquities Authority (document breach 2016–2025)	<i>DieNet</i>
<i>Satellite Infrastructure</i>	Nof-Yam, Gilat Satellite Networks, Imagesat Intl.	<i>ARABIAN GHOSTS</i>
<i>Satellite Infrastructure</i>	10 VSAT devices	<i>GhostSec</i>
<i>Social Media Platforms</i>	Israeli Instagram Accounts	<i>Team Fearless / #WeAreRootSec</i>
<i>Social Media Platforms</i>	Personal data of PM Netanyahu (doxxing)	<i>Team Fearless / #WeAreRootSec</i>
<i>Statistical & Data Platforms</i>	Israel Central Bureau of Statistics (cbs.gov.il)	<i>WeAreRootSec</i>
<i>Transportation Services</i>	CityRide (Israeli ride-sharing platform)	<i>Inteid</i>
<i>Water Infrastructure</i>	Gan HaDarom pumping station, Gderot Regional Council	<i>Z-Alliance</i>

These incidents range from relatively unsophisticated DDoS and web defacement campaigns to disruptions of ICS/OT systems, exfiltration of sensitive data, and psychologically targeted doxxing campaigns. Some groups have even hinted at ransomware deployments, suggesting an escalation in both capabilities and intent.

Who are the main hacktivist groups involved, and what are their capabilities?

The following groups have notably increased their operational tempo amid this geopolitical conflict:

Mr Hamza

- **Focus:** Pro-Muslim, pro-Palestinian, anti-pornography, anti-Western platforms.

- **Activities:** Attacks on Israeli military suppliers, ports, energy companies, communications, defense contractors, IT, and government portals.
- **Tools:** Abyssal DDoS V3, botnets (Maple, Onyx C2, RebirthStress, Squid C2).
- **Alliances:** *Anonymous Kashmir, Anonymous Guys, Team Fearless, Azzasec, Arab Ghosts Hackers.*
- **Origin Hypothesis:** Possibly Moroccan-managed (unconfirmed).

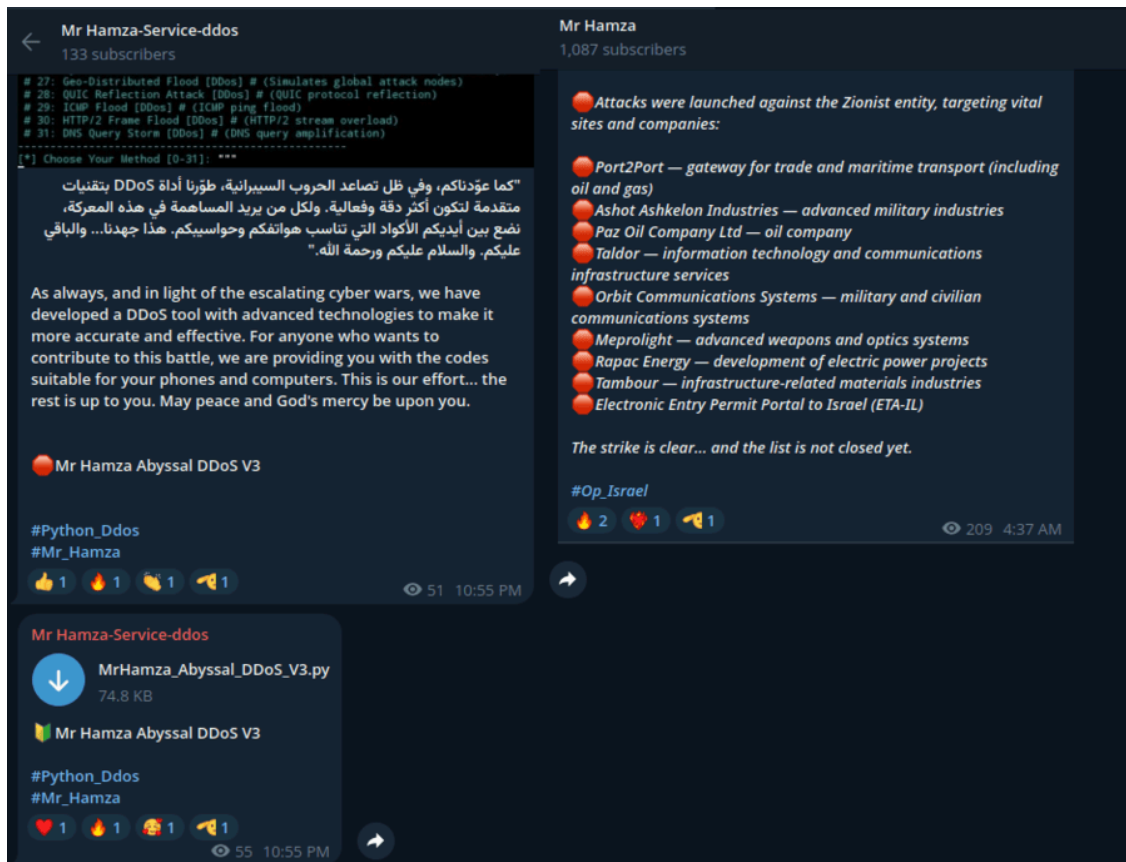


Figure 11: Mr Hamza sharing a distributed denial-of-service (DDoS) attack tool and listing Israeli companies targeted.

Dark Storm Team

- **Focus:** Pro-Palestine, pro-Russia, anti-NATO, anti-Israel, financially motivated hacktivism.
- **Activities:** DDoS-for-hire services, web defacements, data leaks, crypto-based fundraising, anti-Western propaganda.
- **Tools:** Arthur C2 botnet, Telegram-based DDoS orchestration platforms.
- **Alliances:** *Moroccan Black Cyber Army, Akatsuki Cyber Team, Z-Pentest, Keymous+, Noname057(16).*
- **Origin Hypothesis:** Egyptian leadership.

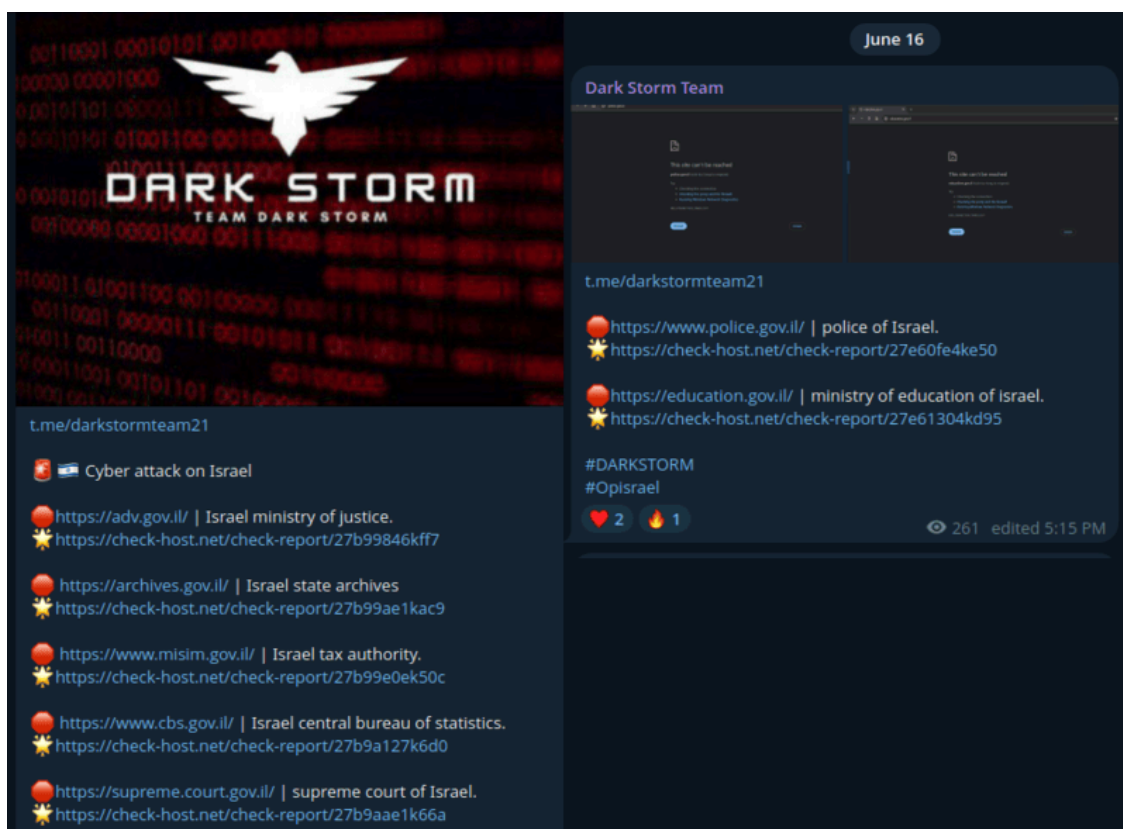


Figure 12: Dark Storm Team claiming responsibility for cyberattacks on multiple Israeli government services, including the Ministry of Justice, Police, Education, and the Supreme Court.

GhostSec

- **Focus:** Pro-Islam, anti-Israel, human rights hacktivism; highly organized; former commercial cybercrime activity.
- **Activities:** DDoS, ICS targeting, industrial sabotage, data exfiltration, extortion, ransomware (GhostLocker), doxing, spamming, zero-day sales.
- **Tools:** Custom tools (GhostLocker ransomware, GhostStealer, Ghostly Development malware), botnet services; DarkZone forum launched in 2024.
- **Alliances:** *SiegedSec* (longstanding partner), *Stormous* (joint ransomware), *Five Families* (until 2024).



Figure 13: GhostSec detailing their extensive cyber campaign targeting critical Israeli industrial systems.

DieNet

- **Focus:** Anti-Zionist, anti-US, anti-Trump hacktivism; increasingly aligned with Iranian geopolitical narratives.
- **Activities:** DDoS attacks on Israeli emergency alert and radio broadcasting infrastructure; data leaks from government and media entities; defacements of commercial websites; public psychological operations via Telegram; announced development of the “LockNet” ransomware platform.
- **Tools:** Custom botnet for DDoS attacks (unnamed); third-party verification tools (e.g., Check-Host.net); bespoke scripts for service availability monitoring and attack confirmation.
- **Alliances:** Possible relation with *Arabian Ghosts*; public rivalry with *Dark Storm Team*.
- **Origin:** Decentralized international actor network; most of its members are allegedly from Russia.

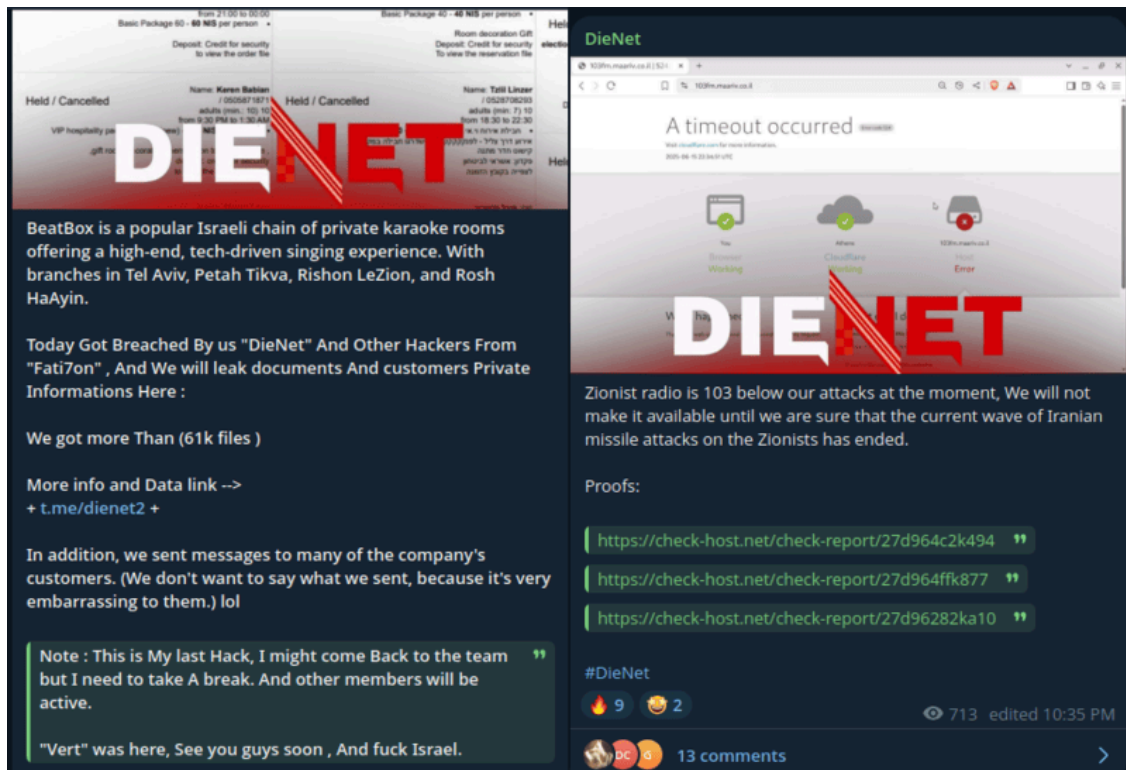


Figure 14: DieNet claims responsibility for breaching Israeli karaoke chain BeatBox, and targeting Israeli radio infrastructure (103FM) during ongoing missile strikes.

Arabian Ghosts

- **Focus:** Regional and ideological hacktivism; initially anti-Iran/Russia, now aligned with anti-Israel operations.
- **Activities:** DDoS, defacements, ICS/OT disruption, data leaks. Claimed Red Alert app attack; announced but unconfirmed ransomware project *BadLadyBird*.
- **Origin Hypothesis:** Likely Syrian; self-identified as “Syrian Ghosts” supporting Anonymous Syria.
- **Alliances:** No formal ties, but recurrent references to *DieNet*, *Mr. Hamza*, *SYLHET_GANG_SG*, and others suggest informal collaboration.

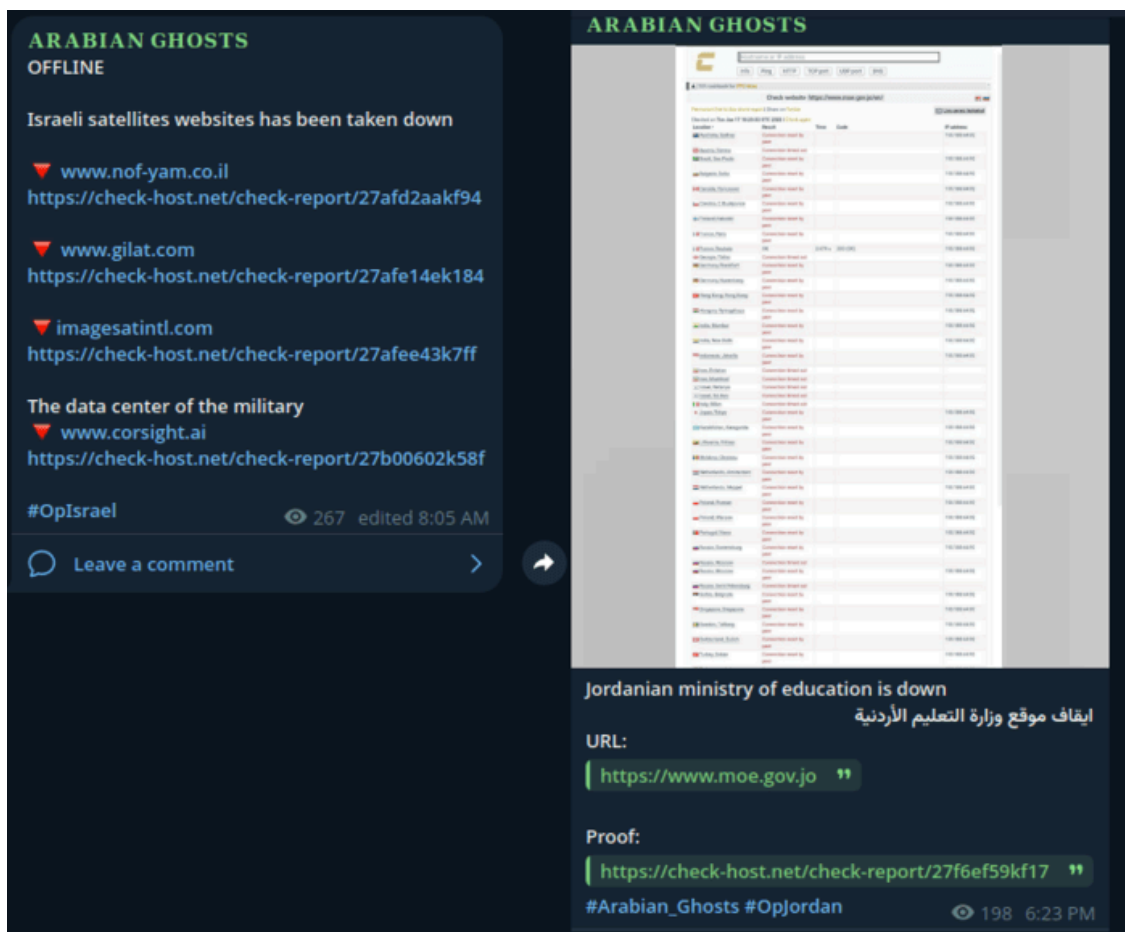


Figure 15: Arabian Ghosts claiming responsibility for takedowns of multiple satellite and defense-related domains, as well as the Jordanian Ministry of Education.

Laneh Dark

- **Focus:** Pro-Iran, anti-Israel, anti-Gulf states; ideologically driven hacktivism with elements of cyber extortion.
- **Activities:** Data theft and ransom-style pressure tactics on companies in Saudi Arabia, Jordan, UAE, and Azerbaijan; public leaks of sensitive infrastructure data; political messaging aligned with Iranian strategic interests; alleged mass device access via “All Seeing Eye” vulnerability.
- **Tools:** Custom leak operations; extortion demands; Telegram/X for psychological ops; claims of undisclosed vulnerability exploitation tools affecting 45,000 global systems.
- **Alliances:** NoName057(16); part of “Nest Security Group” alliance with Russian, Palestinian, and Iranian-affiliated actors.
- **Origin Hypothesis:** Likely Iranian-managed, ideologically motivated with indirect state alignment; emerged in 2024 with increasing visibility post-June 2025.

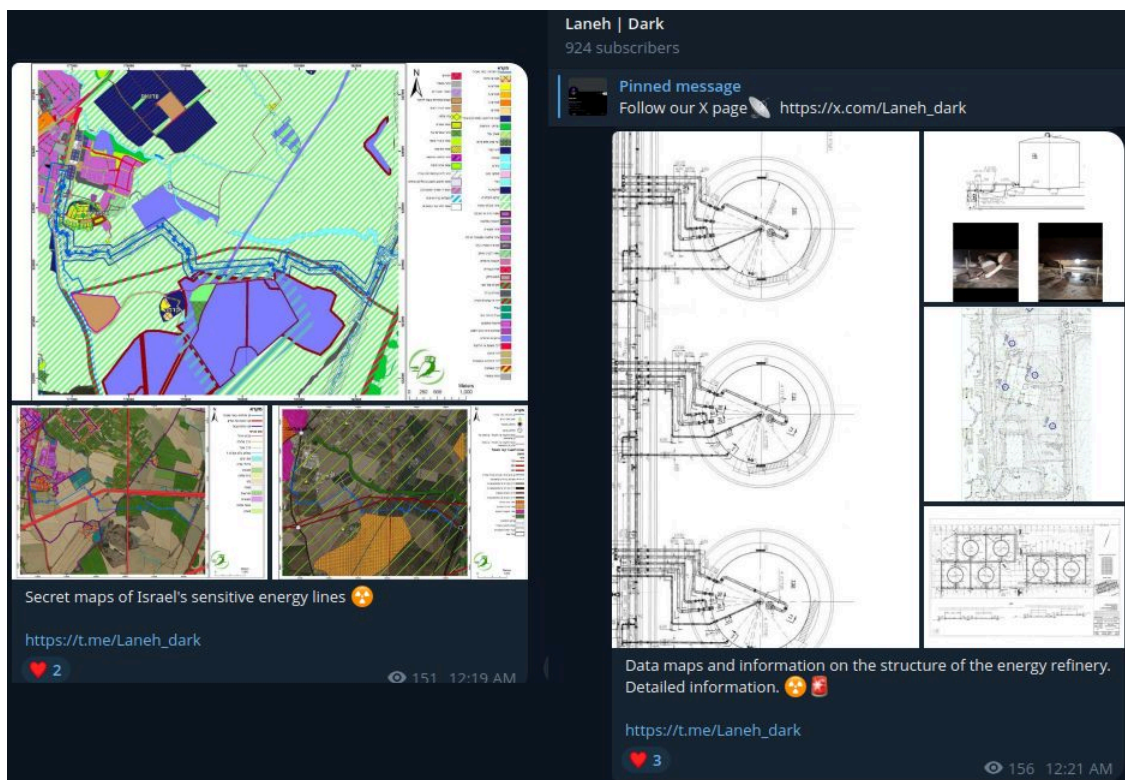


Figure 16: Laneh Dark publishes what it claims to be classified topographical and structural maps related to Israeli energy infrastructure.

Are nation-states disguising themselves as hacktivists?

While many hacktivist groups appear motivated by ideological or political convictions, several actors involved in the Israeli-Iranian conflict are suspected of being state-controlled or heavily state-influenced, blurring the lines between grassroots hacktivism and state-sponsored cyber operations.

These so-called fakativist entities serve as plausible deniability fronts for nation-states, complicating attribution and escalating geopolitical risks. These groups blur the line between independent hacktivism and state-sponsored cyber warfare, complicating attribution and increasing the geopolitical risks of escalation.

Notable fakativist entities that analysts continuously monitor include:

Cyber Av3ngers

- **Attribution:** Iran-linked fakativist group likely operated under IRGC (Islamic Revolutionary Guard Corps) control.
- **Focus:** Disruption of Israeli and U.S. critical infrastructure (ICS/OT, energy, water systems).
- **Activities:** Targeting Israeli companies (e.g., BAZAN Group), U.S. water plants (Unitronics PLCs), oil & gas (Sophos firewall exploits); data exfiltration, limited sales of compromised data in underground forums.
- **Tools:** IOControl embedded Linux backdoor with wiper capabilities; AI-assisted vulnerability research; ICS/SCADA exploit development.
- **Alliances:** May have indirect links with other Iranian groups such as Moses Staff; unconfirmed relations with IRGC's "Soldiers of Solomon".

- **Commercial Activity:** Participated in data sales via Breached and DarkForums, though with limited underground presence.

Handala Hack Team

- **Attribution:** Likely Iranian-controlled faketivist persona posing as pro-Palestinian hacktivist group.
- **Focus:** Phishing-based wiper deployment using social engineering around high-profile events.
- **Activities:** Claimed “Operation HamsaUpdate” (Hatef/Hamsa wipers exploiting F5 vulnerabilities) and phishing during the 2024 CrowdStrike outage.
- **Indicators of State Backing:** High sophistication in targeting, Hebrew language proficiency, victim data inclusion, consistent with state-level preparation.
- **Tools:** Hatef (Windows wiper), Hamsa (Linux wiper); social engineering campaigns leveraging trending security incidents.
- **Underground Presence:** Brief activity in BreachForums and RAMP after December 2023 creation; maintains active Telegram channels and TOR domains.

Handala Hack
787 subscribers

LEAK OF 300K CONFIDENTIAL DOCUMENTS

DELKOL Delek

WEIZMANN INSTITUTE OF SCIENCE HACKED
And was targeted by a missile days ago!

WEIZMANN INSTITUTE OF SCIENCE

More info and sample data coming soon!

Israel's fuel supply system Data

Just as missile damages are always denied, the CEO of Delek also dismissed our cyber operation, claiming the leaked data was "old" and "irrelevant."

But today, 300,000 classified documents prove otherwise.

These files reveal extensive collaboration between Delek Group and the Israeli military, including detailed fuel supply contracts and access to their updated internal databases.

Download the full archive now and see the truth they tried to bury.

Visit our website...

In a complex, coordinated hybrid operation, the Handala Group has successfully breached and compromised the core infrastructure of the Weizmann Institute of Science, an institution deeply embedded in the architecture of occupation, military aggression, and the development of weapons of mass destruction.

This institute is not merely an academic body, it is a central node in the machinery of genocide, surveillance, and scientific apartheid.

We have seized internal documents, sensitive research, and classified data revealing the full extent of its complicity.

Data +4 TB

This is not just a cyberattack. This is a strike against a system of oppression, and it is only the beginning.

The full data dump will be made public imminently.

To the collaborators: You are not untouchable.

To the oppressed: You are not alone.

Figure 17: Handala Hack group claiming the breach of sensitive data from Delek Group and Weizmann Institute of Science.

Preadtory Sparrow (aka [Gonjeshke Darande](#))

- **Attribution:** Highly likely Israeli state-sponsored offensive actor masquerading as an Iranian opposition group. Read our recent analysis into their attack on the Nobitex crypto exchange.
- **Focus:** Strategic disruption of Iranian critical infrastructure.
- **Activities:** Sabotage of Iran's railway (Meteor wiper), gas stations (payment system attacks), steel industry (Khouzestan mill sabotage), energy infrastructure.
- **Tools:** Custom wipers (Meteor, Stardust, Comet), lockscreen message payloads; highly tailored attacks involving prior detailed reconnaissance.
- **Narrative Control:** Justifies operations via Telegram/X accounts with anti-IRGC (Quds Force) rhetoric, emphasizing civilian protection.
- **Tactics:** Long periods of dormancy between highly impactful operations, often coinciding with major regional escalations.



Gonjeshke Darande ✓
@GonjeshkeDarand



Destruction of the infrastructure of the Islamic Revolutionary Guard Corps "Bank Sepah"

We, "Gonjeshke Darande", conducted cyberattacks which destroyed the data of the Islamic Revolutionary Guard Corps' "Bank Sepah".

"Bank Sepah" was an institution that circumvented international sanctions and used the people of Iran's money to finance the regime's terrorist proxies, its ballistic missile program and its military nuclear program.

This is what happens to institutions dedicated to maintaining the dictator's terrorist fantasies.

We thank the brave Iranians whose help made this operation possible.



10:00 AM · Jun 17, 2025 · **40.7K** Views

Figure 18: Gonjeshke Darande claiming responsibility for a cyberattack targeting the infrastructure of Iran's Islamic Revolutionary Guard Corps, specifically Bank Sepah.

What can we expect next in this evolving cyber conflict?

The dramatic rise in hacktivist cyber operations following recent **geopolitical escalations** between Israel and Iran underscores the increasingly central role cyber conflict plays within modern warfare. **Ideologically-driven hacktivists**, alongside possible **nation-state faketivists**, have clearly demonstrated their readiness to exploit geopolitical tensions to pursue diverse **strategic objectives**.

Given that the [Israeli-Iranian confrontation is still developing](#), it's hard to predict whether a ceasefire will hold. If cyber activity re-intensifies, expected trends would likely include:

- **Increased DDoS campaigns** targeting Israeli energy, telecom, defense, and government systems.
- **Escalation towards allies** such as the US, UK, and Arab states aligned with Israel.
- **Emerging retaliatory operations** by pro-Israeli groups such as Predatory Sparrow, already engaging in offensive activity against Iranian systems.
- **Sustained propaganda and psychological operations**, further exploiting public fear and political instability.

Organizations across all geopolitical fault lines are advised to adopt heightened cybersecurity postures to defend against what may evolve into a prolonged and highly disruptive cyber conflict.

Stay ahead of emerging threats

[Outpost24's CompassDRP solution](#) combines the asset discovery powers of [our EASM platform](#) with threat-intelligence powered DRP modules. Customers are backed up by our world-class human-led threat intelligence team, KrakenLabs. [Get in touch to learn more](#).

About the Author



Lidia is a Senior Threat Intelligence Analyst at Outpost24's KrakenLabs Strategic Research team. Her role involves researching and profiling threat actors, monitoring their campaigns, IOCs, and TTPs. She also creates threat intelligence reports and keeps a close eye on fraudulent activity in the cybercriminal underground.

Source: <https://outpost24.com/blog/hacktivist-cyber-operations-iran-israel/>