Graphika

Everything Everywhere All at Once:

The Pro-Iran Playbook for Narrative Control

The Graphika Team

02.2026

Everything Everywhere All at Once

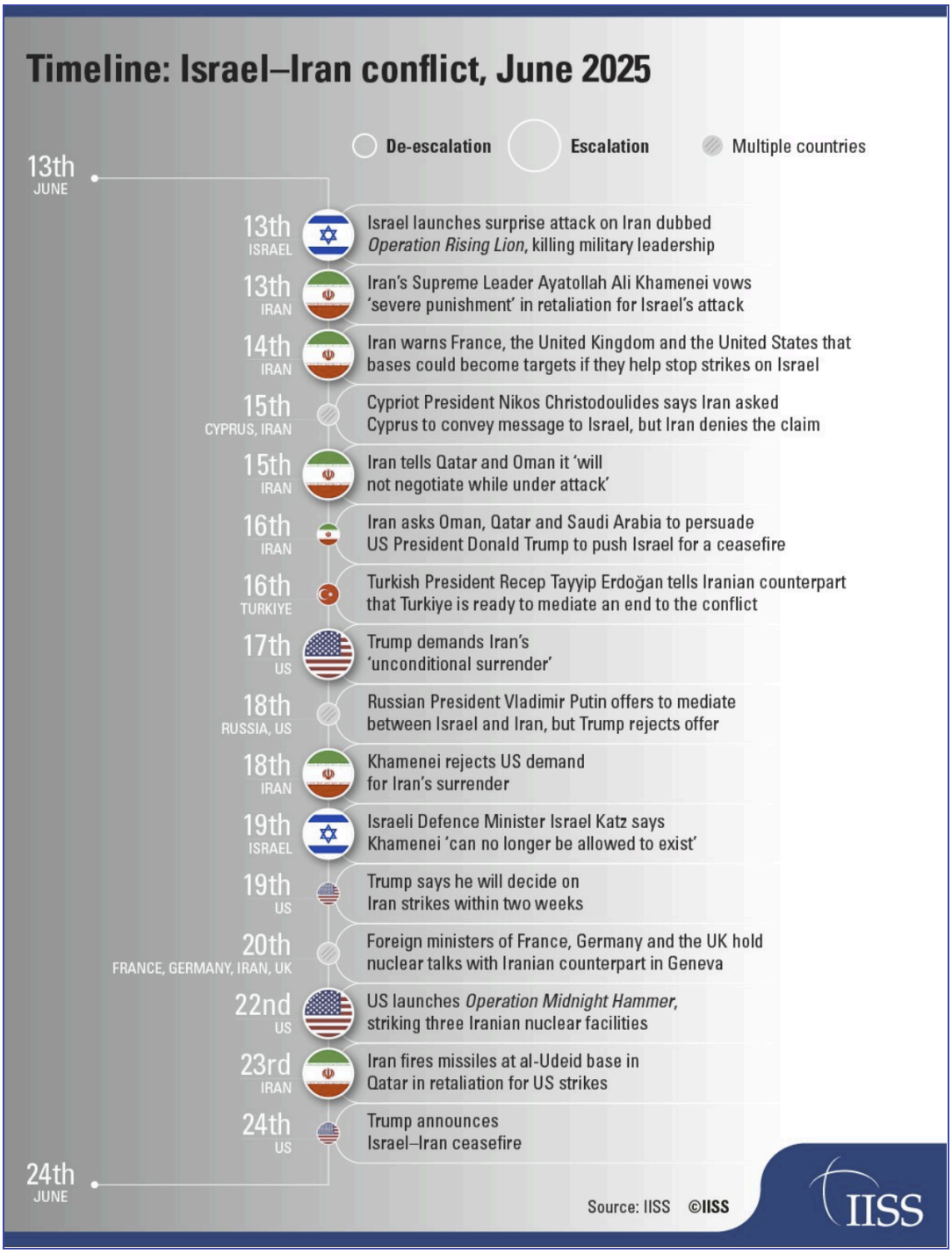
The Pro-Iran Playbook for Narrative Control - Part 2

Overview

In June 2025, the long-standing tensions between Israel and Iran escalated into direct conventional warfare. Through our intelligence monitoring, Graphika tracked and analyzed the activities of Iranian state and state-aligned media outlets, networks of inauthentic social media accounts, and pro-Iran hacktivist groups. This two-part report details how these actors mobilized to spread unified narratives, despite varying levels of proven state affiliation.

Our analysis reveals a playbook used by pro-Iran actors to manage perceptions during and after the war. We observed a notable delay in the initial mobilization of an information response, suggesting a lack of preparation for a large-scale on-the-ground conflict. Once mobilized, however, these actors collectively clouded the information space by disseminating a mix of breaking news alerts, aggressive threats, and unverified claims. Our reporting outlines the tactics employed to target domestic and global audiences.

While the first part in this series covered activity from state and state-aligned media as well as sets of inauthentic social media accounts, this second part covers the activity we observed from pro-Iran and Iran-linked hacktivist groups. In particular, we examine a new group that is regularly amplified by the Iranian Revolutionary Guard Corps (IRGC)-backed media, and which we assess with medium confidence is an Iranian-sponsored persona. These findings stem from our June 13-25 monitoring, alongside our tracking of previously identified Iranian state-backed and state personas, the groups that revolve around them, and the overall Iran-aligned hacktivist community.



The International Institute for Strategic Studies' [timeline] of the Israel-Iran war.

Key Findings

We identified the following key findings across parts 1 and 2 of this report.

- Pro-Iran hacktivist groups, media, and social media mobilized during the 2025 Israel-Iran war and spread similar narratives regardless of their proven or self-described state affiliation.
- Organic pro-Iran activity accounted for most of the hacktivist cyberattacks we observed during the war, with over 100 pro-Iranian hacktivist groups originating from the broader pro-Palestine and pro-Russia movement.
- Iranian state-run and -sponsored hacktivist personas reactivated, redirected their efforts, or reframed some of their campaigns to support Iran and attack Israel.
- At least one new group - Cyber Isnaad Front - that we assess with medium confidence is an Iranian-run hacktivist front, given its similarity to previously attributed personas, emerged during the June escalation. The group gained amplification through Iranian official channels, and sought to depict Israel as exposed, unprepared, and technically inferior to Iran in cyberspace.

Overall Activity

During the 12-day Israel-Iran war, Graphika and our industry partners witnessed a surge of organic hacktivist activity from groups that are geopolitically and ideologically motivated, alongside activity from groups that are either attributed to, or backed by, Iranian actors. This surge of organic and inorganic activity unfolded over the two days following Israel's first strikes on Iran, with some groups initially issuing threats against Israel without acting, and others immediately launching attacks in reaction to the strikes. These actors, whose claims often remain unsubstantiated and exaggerated, are part of a broader hacktivist trend to muddy the information space while attempting to portray Israel and its allies as unable to stand up to Iranian superiority online.

This report focuses on pro-Iran activity by organic and state-backed groups, though it is worth noting that most of these attacks had very limited impact and remain publicly unproven. A limited number, such as Homeland Justice's attack on the Albanian capital city, Tirana, was publicly documented. Cyberattacks on the pro-Israel front, in particular those by the group Gonjeshke Darande against the Iranian Sepah Bank and Nobitex, were overwhelmingly more disruptive and significant. Gonjeshke Darande is suspected of being linked to the Israeli government.

In order to examine the perception hacking and narratives of the pro-Iran activities covered in this report, we have focused on the public claims by these hacktivist actors during the conflict.

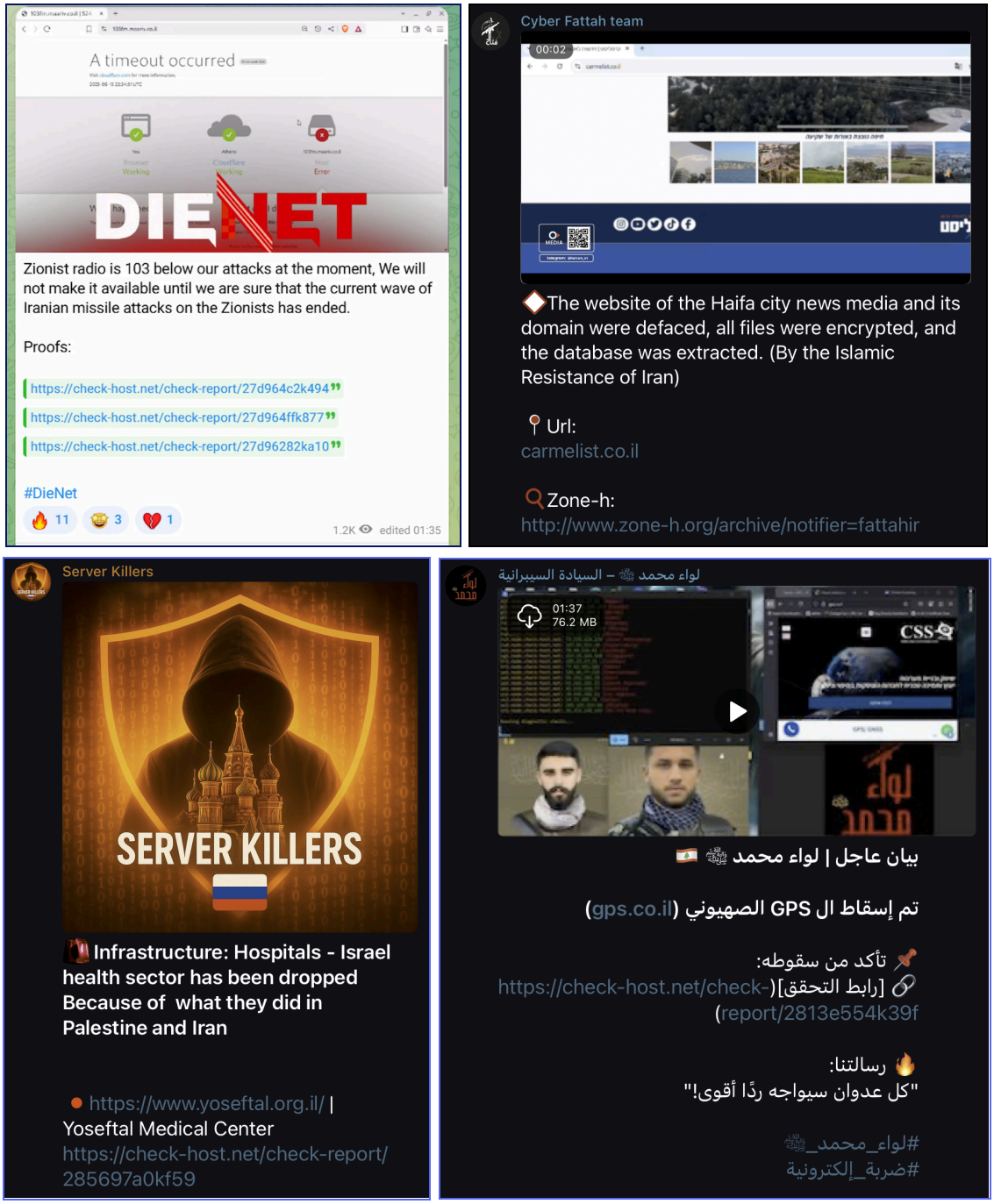
However, as highlighted by cybersecurity companies, APTs and other groups have launched different types of attacks with no public announcement.

Organic Hacktivist Activity

In the days following Israel's first strikes on Iran on June 13, pro-Palestine hacktivists groups Arabian Ghosts, Liwaa Mohammed, Unknowns Cyber Team, Golden Falcon, LulzSec Black or DieNet started claiming DDoS attacks against Israeli targets, with a peak in activity on June 14. Targets included the Bank of Israel, media outlets, and government agencies, alongside claims of intrusions and hack-and-leaks.

While attacks continued over the two weeks of the war and after the ceasefire, we registered a second surge of attacks around June 19, when groups targeted Israeli domains seen as linked to critical infrastructure, including railway systems and government and military agencies. Overall, we observed over 100 pro-Iranian groups, including Russian hacktivist groups such as NoName057(16) and ServerKillers, mobilize either through statements of intent or attacks, a number that tracks with publicly available data.

Not all Middle East and North African (MENA) hacktivist groups sided with Iran: anti-Iranian groups organizing around anti-Ba'athist Syrian groups that support the new Syrian government launched DDoS attacks against Iranian domains, including media outlets and government websites, and spread claims of intrusions into technology companies, among others. Prior to regime change in Syria, hacktivist activity by the Syrian Electronic Army, Anonymous Syrian Hackers, and the Islamic Hacker Army, among others, repeatedly targeted the Assad regime, Iran,and Russian infrastructure, for their involvement in Syrian politics. Some Indian pro-Israel groups also launched minor attacks on Iran.



Example attacks from DieNet, Cyber Fattah Team, ServerKiller, and Liwaa Mohammed targeting Israeli websites they consider part of the country's critical infrastructure during the Israel-Iran war.

Known Iranian Hacktivist Personas and State-Backed Groups

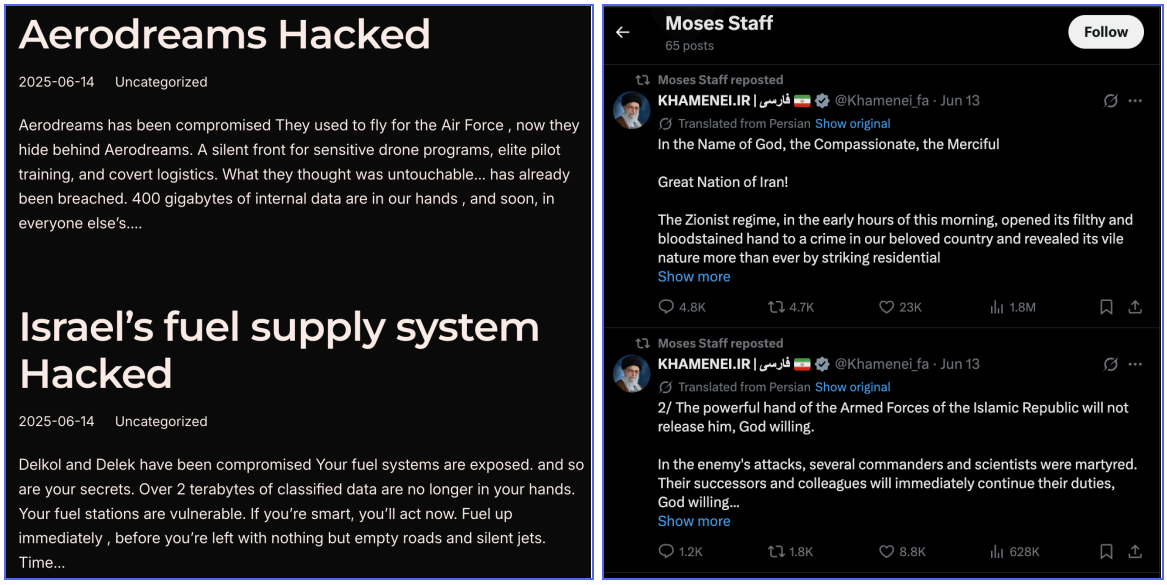
Outside of this organic activity by hacktivist groups with geopolitical and ideological motives, we also observed Iranian hacktivist personas and groups reactivating to spread pro-Iranian content and carry out attacks, or to reframe their ongoing operations as support for Iran. Industry peers linked these groups to the IRGC, the Ministry of Intelligence (MOIS), and others that were

attributed to unknown Iranian actors. Iranian-run and -backed groups mainly relied on their usual techniques, such as claims of data leaks, camera network intrusions, and doxxing companies tied to the Israeli government or military.

The most prolific group was by far Handala Hack, a pro-Palestine hacktivist group consistently amplified by the Iranian media apparatus that Crowdstrike and the anti-government Iranian media outlet Iran International link to the MOIS-run Iranian threat actor Banished Kitten. Handala reactivated hours after Israel's strikes on Iran, following months of silence on social media and on their website. Beginning on June 14, the group started claiming a series of hack and leak attacks on companies linked to the Israeli military, including an Argentinian drone manufacturer.

CyberToufan, which industry peers suspect is backed by unknown Iranian actors, continued its campaign "Enter Upon Them by The Gate," which it claims involves intrusions and hack-and-leak operations targeting military and government contractors. After the war, CyberToufan started mentioning Israel's attacks on Iran despite stating they would remain focused on Gaza. Similarly, Homeland Justice, which Microsoft linked to the MOIS, reactivated after a month of silence and released a post accusing two MEK-affiliated Iranians of "conspiring against the people of Iran" with Israeli officials on June 21. The dox was published amid attacks on the Municipality of Tirana, Albania, in retaliation for hosting MEK refugees, and did not explicitly mention the war, despite its timing.

A group affiliated with the IRGC, Moses Staff, reactivated after eight months of silence on X and began amplifying Supreme Leader Khamenei's content. The escalation also triggered the appearance of groups Graphika assesses to be copycats of Cyber Av3ngers, a group the U.S. government attributed to the IRGC, and the self-proclaimed Iran Cyber Security Group, which defaced a U.S. government website in 2020. The Cyber Av3ngers copycat group amplified another hacktivist group, APT IRAN, which promoted a list of allegedly hacked email addresses from Israeli defense company Rafael. On Telegram, Iran Cyber Security claimed it conducted a "massive cyber attack" on "Israeli financial companies and medical systems."



Left: Handala claiming attacks starting June 14 on Israeli companies. Right: Moses Staff amplifying Khamenei's posts on X.

Case Study: Cyber Isnaad Front

Part one of this report discussed how pro-Iran groups exploited the state media ecosystem and inauthentic social media networks to portray Iran as having the superior hand online. Here in part two, we highlight how they also amplified a new, supposedly independent hacktivist group that emerged during the war. Graphika and industry peers suspect that this group, Cyber Isnaad Front (Cyber Support Front), is an Iranian-linked front.

Overview

During the escalation, one new, seemingly independent group emerged and was repeatedly amplified shortly after its creation. Cyber Isnaad Front presents as an Arabic-language hacktivist group that attacks Israeli companies connected to the Israeli military and government in support of Palestine. We first observed Cyber Isnaad Front when Tasnim News began to amplify it on June 19, 2025. This was two days after Cyber Isnaad Front created its Telegram channel, and a day after it started posting. Another group, Gaza Children Hackers, which, based on its TTPs, we assess with medium confidence is an Iran-run persona, also promoted Cyber Isnaad Front.

Cyber Isnaad's logo is an inverted red triangle that was initially used in Al-Qassam Brigades videos and has since become seen as a pro-Palestine or pro-Hamas symbol, particularly for armed Palestinian resistance online. The Telegram channel bio for Cyber Isnaad links to an "onion" service meaning it is only accessible through the Tor network that makes hosts and users anonymous to each other. The group also administered a now-deleted data-selling account they promoted on their Telegram channel, @DataSellingAdmin.

On their onion website, outside of emphasizing support to Palestine and referencing "Al-Quds martyrs," Cyber Isnaad stated it was created as a "new front" to "lay siege to the criminal regime of Israel in cyberspace" until "full destruction of occupation" in Palestine is achieved. It presented not only as its own group, but also as a broader entity that pro-Palestine hacktivist groups can join to unite against Israel, and designated "any company or entity that supports Israel" as potential targets.

Screenshot of Cyber Isnaad's currently offline onion service explaining their motivations.

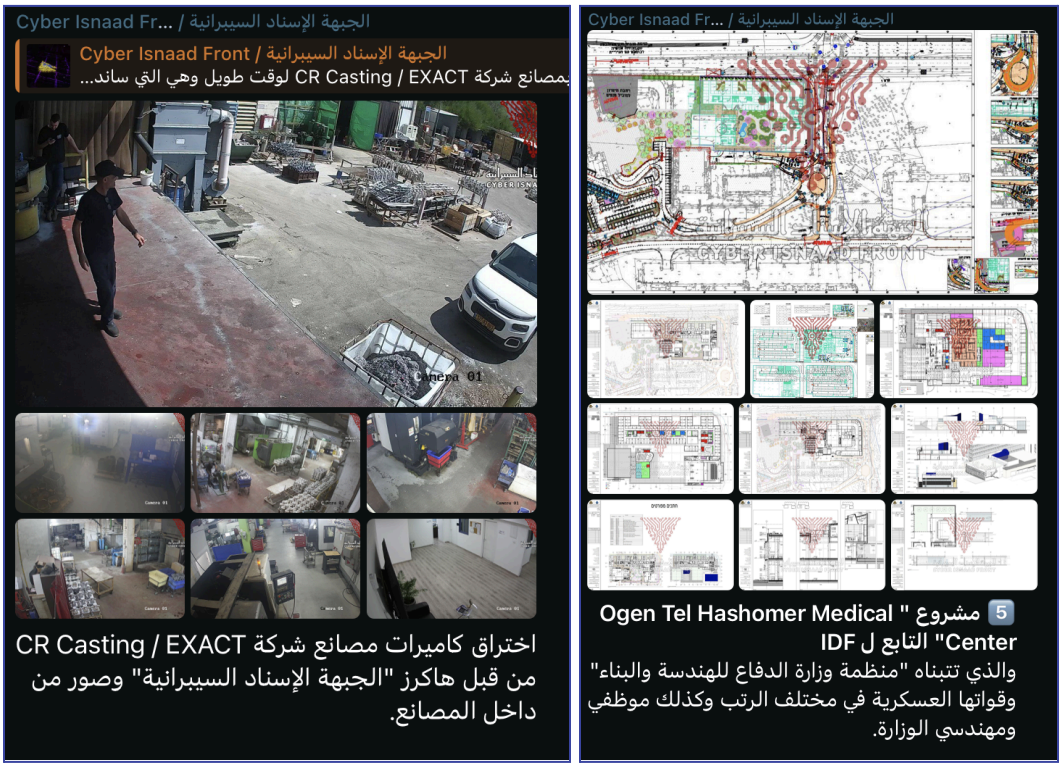
Cyber Isnaad posts in Arabic and claims to be independent. However, based on its techniques, tactics, and procedures, we assess with medium confidence that the group is an Iranian-linked hacktivist persona. We, however, cannot link it with high confidence to a specific nexus of Iranian-run hacktivist activity.

Targeting and Attack Mode

On their Telegram channel and onion website, Cyber Isnaad immediately began promoting data leaks and claims of intrusion against Israeli companies that they consider directly support or have ties to the Israeli military or government. Additionally, they began sharing doxxing attacks on employees of the companies they targeted, as well as security camera network intrusions. All of these are common TTPs among Iranian hacktivist fronts and Iran-backed groups.

In the first days of their existence, the group claimed they broke the "backbone of the Zionist army's communications network" by taking over and destroying the Israeli army's internal communications systems, including satellite and industrial control systems. They released screenshots allegedly showing internal systems from companies such as Gilat, a satellite

network company contracting with the Israeli Ministry of Defense, or blueprints and 3D models of technology developed by the manufacturer CR Casting/EXACT for the Israeli army. These releases were accompanied by posts containing images seemingly stolen from employees' personal devices and security camera screenshots intended to prove the intrusion. Since then, the group has continued to focus on the same type of targets.



Example Telegram posts from Cyber Isnaad Front allegedly showing their intrusion into security cameras belonging to CR Casting/EXACT (left), and claiming to show the blueprints of the Ogen Tel Hashomer Medical Center, affiliated to the IDF. They claim they obtained these through a hack against Bensimon Aluminium Industries.

During these alleged attacks, Cyber Isnaad also sometimes releases "Wanted Person" posters doxxing the targeted companies' employees for contributing to the Israeli Defense Forces' acts of terrorism in Gaza, and for lending their services to the Israeli military apparatus. This is a TTP we previously observed from Iran-linked hacktivist personas. These images are featured on the group's Telegram channel, but Cyber Isnaad's onion domain also has a dedicated "Most Wanted" section.

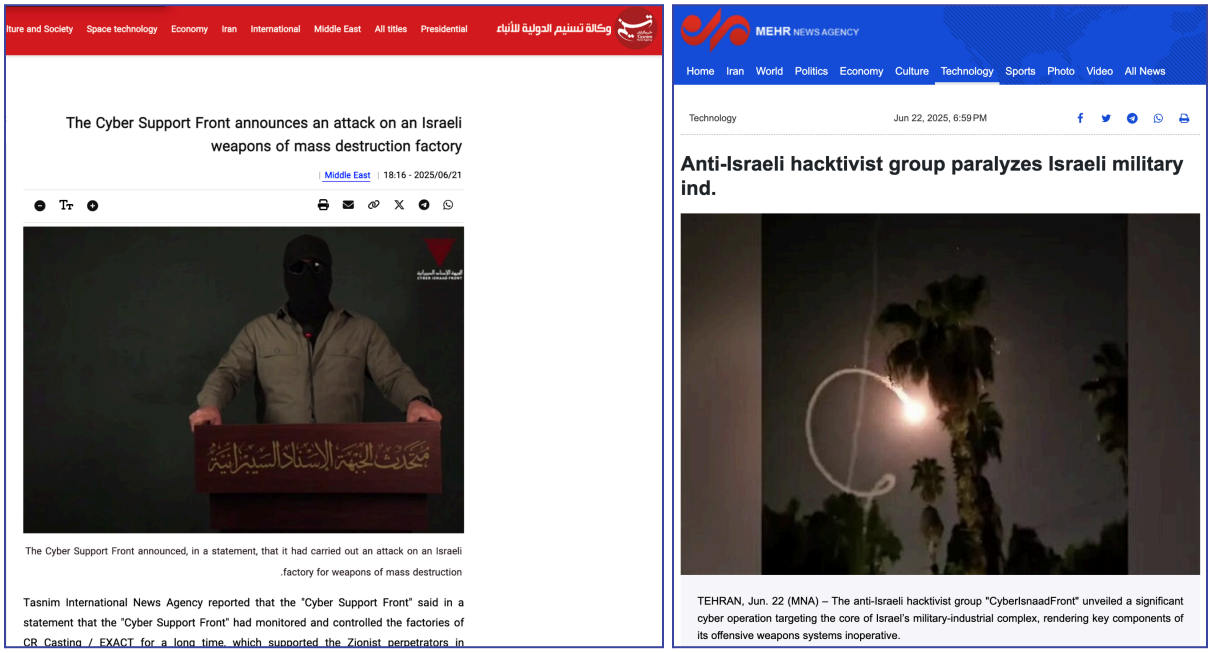
State Media Amplification and Continued Outreach

Almost immediately after Cyber Isnaad's creation and initial claims of attacks, the Iranian state media ecosystem began amplifying the group's claims of attacks, reinforcing suspicions of links between the hacktivist group and the Iranian state. This is a common TTP among state-backed groups in Iran, but also in Russia, among groups attributed to Russian intelligence services, such as Russian Angry Hackers Did It (RaHDit, also known as Nemezida).

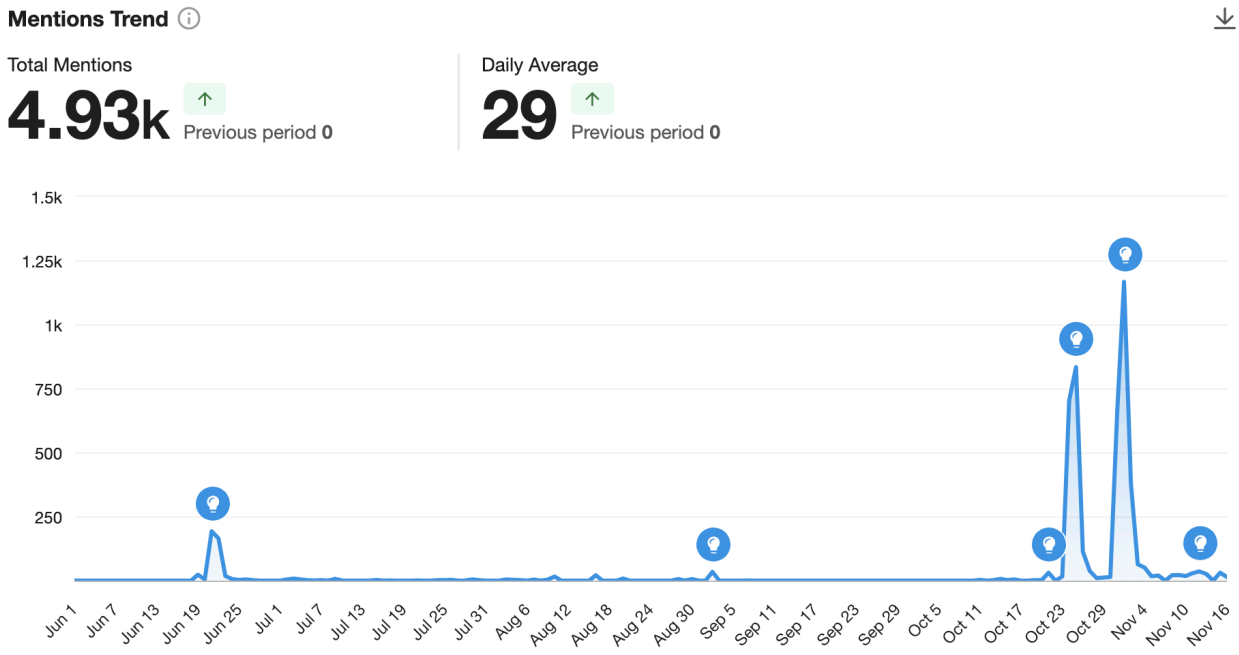
The Iranian media ecosystem started promoting Cyber Isnaad on June 19, with Tasnim posting a tweet presenting the group and teasing the release of information about their operations. After that, outlets active on both X and their own websites, including Tasnim and Mehr News agencies, started reporting on Cyber Isnaad's claims. The Iranian influence operation Attack Alarm also repeatedly amplified Cyber Isnaad.

Our analysis of mentions of Cyber Isnaad on social media and in the media showed that while state media amplification and endorsement remained contained during the war, it increasingly contributed to Cyber Isnaad's popularity. We measured this through media and social media mentions using the social listening tool Meltwater.

While it is worth noting that there is a direct correlation between state media mentions and Cyber Isnaad's online visibility, increasing numbers of pro-Iranian actors amplifying their content also played a role. Engagement with X accounts tied to Cyber Isnaad, which they created in July 2025, remains minimal.



Iranian state news agencies Tasnim and Mehr amplified Cyber Isnaad shortly after the group emerged.

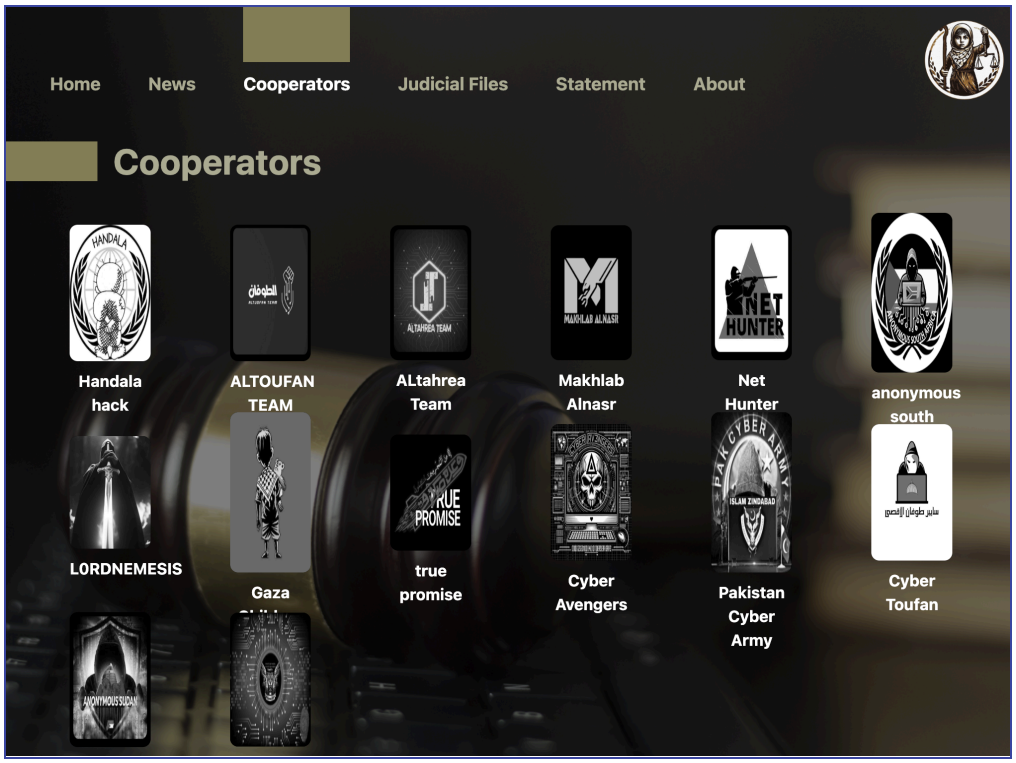


Meltwater query results for "Cyber Isnaad Front" OR "CyberIsnaadFront" OR "الجبهة الإسناد السيبرانية" OR #CyberIsnaadFront OR #الجبهة_الإسناد_السيبرانية between June 1 - Nov 16. Spikes of mentions correspond to state media coverage.

Overlap With Iranian-run Personas and Groups

Outside of media amplification, Cyber Isnaad was also repeatedly promoted by another hacktivist group that Graphika tracks, Gaza Children Hackers. Based on the TTPs of this group, which include hack-and-leaks against contractors or companies connected to the Israeli military and government, CCTV intrusions, doxxing, and amplification and cooperation with IRGC-attributed personas, we assess with medium confidence that it is a state-run or -backed group, though we cannot link it to a specific entity. This group, which first emerged in October 2023, belongs to a network of activity adjacent to the Cyber Court, a cluster of personas that the U.S. has attributed to the IRGC-linked actor Emmeret Pasargad, and which operated under the company name Cyber Group Aria Sepehr Ayandehsazan (ASA). Similar to Handala Hack and more recently Cyber Isnaad, groups belonging to this nexus of activity enjoyed repeated and immediate state media amplification.

While we assess Gaza Children Hackers to be separate from the Cyber Court cluster based on their behavior and TTPs, Cyber Court promoted the group's alleged hack against Israeli companies in May 2024, and lists it as a "cooperator" on their websites, alongside other personas attributed to Iran by industry peers. Some seemingly unrelated groups are listed as "cooperators," but, unlike Gaza Children Hackers, were not promoted on Telegram.



Cyber Court promoted Gaza Children Hackers on their website and on Telegram.

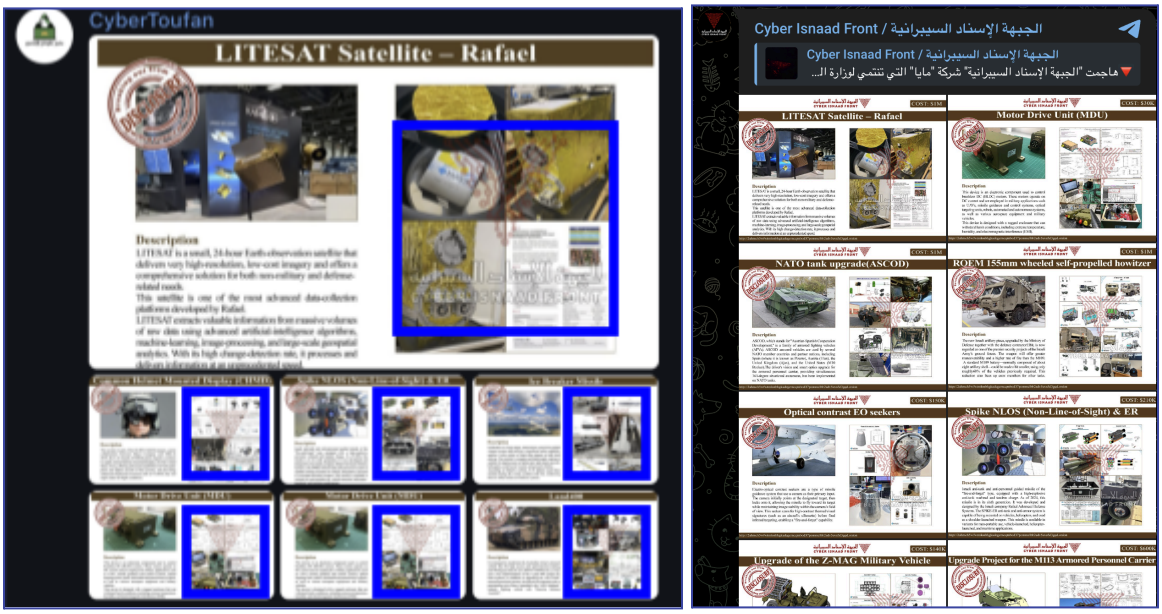
Gaza Children Hackers reactivated after two months of silence and started amplifying and promoting Cyber Isnaad Front on June 23 in a post stating that Gaza Children were "now related" to Cyber Isnaad, and that "all of our operations, activities and etc. are in relation with this Cyber Jihadi Group." From there on, Gaza Children Hackers started attributing attacks on Israeli targets to themselves and Cyber Isnaad, and started posting videos using both their logo and Cyber Isnaad's to announce new attacks. In August 2025, Gaza Children Hackers appeared to resume autonomous activity. For its part, two months later, Cyber Isnaad began acknowledging Gaza Children Hackers, promoting their content and statements that bore both groups' logos.

In November 2025, another group Microsoft assesses is Iran-sponsored, Cyber Toufan, gained significant media attention, particularly in Australia, for publishing documents they claimed to have stolen from Israeli defense companies Rafael and Elbit by breaching the company Maya Engineering. However, these were recycled claims, made previously by Cyber Isnaad in October 2025, when the group claimed it had exfiltrated "important and exclusive information related to the manufacture of parts of military air equipment" belonging to Rafael and Elbit.

The images released by CyberToufan as part of the supposed hack, which were initially published by Cyber Isnaad without attracting attention, bear Cyber Isnaad's logo and were widely reused in international media.

While Cyber Toufan claimed "they received" the data, they cropped the images to remove top mentions of Cyber Isnaad and the pricing of the documents. At this stage, we cannot assess whether the two groups are directly connected or whether Cyber Toufan opportunistically stole

content from Cyber Isnaad; Cyber Isnaad did amplify, on social media, Australian media reporting covering the hack wrongly attributed to Cyber Toufan, cutting all mentions of Cyber Toufan and simply repeating that they were responsible for the hack.



CyberToufan promoting cropped documents stamped with Cyber Isnaad's logo (left) in November. Cyber Isnaad promoting the initial release of these documents in October (right).

Estimative Language Legend

Assessments of Likelihood

Graphika uses the following vocabulary to indicate the likelihood of a hypothesis proving correct. If we are unable to assess likelihood due to limited or non-existent information, we may use terms such as "suggest."

Almost No Chance	Very Unlikely	Unlikely	Real Chance	Likely	Very Likely	Almost Certain(ly)
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence Levels: Indicators of Sourcing and Corroboration

Graphika uses confidence levels to indicate the quality of information, sources, and corroboration underpinning our assessments.

Low Confidence	Medium Confidence	High Confidence
Assessment based on information from a non-trusted source and/or information we have not been able to independently corroborate.	Assessment based on information that we are unable to sufficiently corroborate and/or information open to multiple interpretations.	Assessment based on information from multiple trusted sources that we are able to fully corroborate.

Graphika

About Us

Graphika *is the most trusted provider of actionable open-source intelligence to help organizations stay ahead of emerging online events and make decisions on how to navigate them. Led by prominent innovators and technologists in the field of online discourse analysis, Graphika supports global enterprises and public sector customers across trust & safety, cyber threat intelligence, and strategic communications spanning industries including intelligence, technology, media and entertainment, and global banking. Graphika continually integrates new and emerging technologies into our proprietary intelligence platform and analytic services, empowering our customers with high-precision intelligence and confidence to operate in a complex and continuously evolving information environment.*

For more information or to request a demo, visit our website.