FOX IT
part of ncc group

ncc group

Middle East Crisis Cyber Update

Global Threat Intelligence Team

12 March 2026

Public Release

Table of contents

Executive Summary

- NCC Group continues to monitor the evolving conflict in the Middle East to assess the security implications for our clients. Our Threat Intelligence team conducts regular reviews in line with best practices and will update detections where required.
- The assessment of Iranian cyber operations remains largely unchanged from the previous report. Iranian state-sponsored cyber threat activity is highly likely to remain focused on supporting direct wartime objectives. Given Iran's limited capacity and increased focused on kinetic operations, it is unlikely to conduct significant cyber-attacks against private entities in the near term.
- Conflict-linked hacktivist activity has expanded in volume, geographic scope, and actor diversity, while tactics remain largely unchanged. DDoS attacks, website defacements, and data leak claims continue to account for most hacktivist activity, with national governments, critical infrastructure, and technology sectors in Israel and the Gulf region remaining the primary targets.
- As previously assessed, clients' risk profiles remain linked to their geographic presence, connections to Israel and the US governments, as well as their host governments' support for strikes against Iran.

Assessment

As previously assessed, cyber threats linked to the current conflict in the Middle East are unlikely to change significantly for organisations outside Iran's traditional targeting scope. However, the risk landscape may broaden as additional governments become directly or indirectly involved in the conflict through political, military, or diplomatic support. Organisations with a presence in Israel, or with commercial or governmental ties to the US government, continue to face elevated risk. In the immediate term, Iranian cyber operations are likely to focus on directly supporting objectives in the ongoing conflict with Israel and the US. However, the risk of cyber disruptions from kinetic targeting in the Gulf region is elevated following Iran's declaration that cloud infrastructure sites in the region are legitimate targets.

Iran and affiliated cyber threat activity continue to focus mainly on high-visibility but low-impact operations. As of the time of writing, reporting indicates that DDoS activity linked to the current conflict accounts for over 60% of claimed attacks. Targets include Israeli government, military, and infrastructure entities, as well as organisations in countries perceived as aligned with Israel or the US, including GCC countries, Jordan, Cyprus, Germany, and Australia. Although technically limited in its impact, such activity can still cause temporary operational disruption and reputational risk.

Mis and disinformation-related activity is also likely to continue increasing as the conflict evolves. Generative AI enables the rapid creation and distribution of manipulated images. Recent media reports pointed to the notable increase in AI-generated and -manipulated imagery, with some content creators monetising such material through advertising. As generative AI imagery becomes increasingly realistic, there is a growing risk that unverified content may be accepted as authentic. This reinforces the importance of approaching conflict-related visual content with caution.

NCC Group Action

Detection Engineering

Our Global Detection Engineering team develops analytics based on (un)expected behaviours and outcomes, rather than against specific signatures belonging to specific campaigns or tools. This enables us to develop detection logic potentially covering currently unknown threat campaigns and techniques. Whilst threat actors and tools will change, our focus on behaviour and outcomes enables us to be proactive in covering emerging threat actors and tools in the future. This provides the best level of future-proof detection coverage for our SOC clients.

We continuously work with our threat intelligence team to review our detections based on changes to our clients' threat landscape. The Middle East crisis does not change this process; however, we are conducting research into Iranian nation state and Iranian threat actors to verify our detection alignment and make changes where required.

Our threat intelligence team continuously identifies and validates Indicators of Compromise (IoCs), which are fed into our IoC hunts. Positive detections of these in client environments are then triaged by our SOC analysts, with escalation deemed appropriate.

Threat Hunting

NCC Group's Global Threat Hunting team is closely monitoring the evolving situation and is actively assessing opportunities to conduct proactive, hypothesis-led hunts for actors linked to the nations involved, as well as those who may seek to exploit the ongoing destabilisation and deteriorating geopolitical conditions in the Middle East. We remain highly alert to any shifts in adversary behaviour and are ensuring our posture reflects the heightened threat environment.

Our threat hunting team is working in close coordination with our Threat Intelligence team to identify, validate, and prioritise relevant threats as soon as practicable. Any resulting targeted hunts will be executed through our established processes and communicated appropriately to impacted clients.

Middle East Crisis

Background

Please see our previous Middle East Crisis Update released on 5th March 2026.

Conflict Development

Since our initial report was published on 5th March, the USA and Israel have maintained expansive air campaigns against Iran. In Lebanon, Israel began striking targets in central Beirut on 8th March.[1] Iran has continued missile and drone attacks across the region, supported by pro-Iranian armed militia groups in Iraq.[2] For Iran, attacks outside of Israel, or on regional targets not clearly linked to US-military assets, have been publicly framed as retaliatory and 'like-for-like'. On 11th March Iran's military leadership declared US/Israeli linked economic and banking interests would be targeted following an attack on an Iranian bank, this reflects a pattern seen with civilian airports, water infrastructure and energy assets. [3] [4] [5] [6] [7] [8] The announcement coincides with the publication by Iranian media of a list of "Iran's New Targets".[9] The list reportedly includes regional office locations and cloud-based infrastructure linked to prominent US companies and Israel, including Google, Microsoft, and Oracle.[10] The implications of a broader, new statement made by Iran's military leadership on 11th March are unclear; Iran committed to moving from 'reciprocal' to continuous attacks.[11]

In addition to the rising human cost and physical damage caused by military activities, regional attacks on oil and gas infrastructure, combined with Iran's effective closure of the Strait of Hormuz to maritime traffic caused a global shock to the energy sector.[12] Oil prices temporarily exceeded levels caused by Russia's invasion of Ukraine in 2022, and other oil-based products such as jet fuel increased nearly doubled in price.[13] On 11th March Iran's military leadership publicly reiterated their commitment to continue disrupting the oil economy; defining any vessel or tanker linked to the "US, [Israel] and their partners" as a 'legitimate target'.[14] It is currently unclear which, if any, (non-partner linked) vessels may be permitted to cross the Strait of Hormuz.

Through interdependencies, the energy crisis has the potential to create a significant disruption to critical supply chains including food and petrochemicals (including agrochemical).[15] For countries heavily dependent on Gulf exports which also lack strategic supply stores this has the potential to risk food, energy and fuel shortages. Despite the physical attacks and high global stakes of the conflict, countries closely tied to and historically willing to support US military operations continue to resist involvement beyond facilitating defensive activities, despite US criticism.[16] [17]

---

[1] https://www.reuters.com/world/middle-east/least-two-killed-strike-hotel-building-central-beirut-security-source-says-2026-03-08/
[2] https://www.reuters.com/world/middle-east/drone-strike-hits-us-diplomatic-facility-iraq-reports-washington-post-2026-03-11/
[3] https://www.reuters.com/world/middle-east/iran-will-target-us-israeli-economic-banking-interests-region-state-media-2026-03-11/
[4] https://www.aljazeera.com/video/newsfeed/2026/3/9/irgc-warns-of-energy-war-after-us-israeli-strikes-on-iranian-assets
[5] https://www.reuters.com/world/middle-east/iran-will-target-us-israeli-economic-banking-interests-region-state-media-2026-03-11/
[6] https://www.reuters.com/world/middle-east/two-drones-fall-vicinity-dubai-airport-iran-crisis-shows-no-sign-easing-2026-03-11/
[7] https://www.aljazeera.com/news/2026/3/8/how-targeting-of-desalination-plants-could-disrupt-water-supply-in-the-gulf
[8] https://www.airwaysmag.com/new-post/tehran-airports-disrupted-mehrabad-imam-khomeini
[9] https://www.aljazeera.com/news/2026/3/11/iran-declares-us-israeli-economic-banking-interests-in-region-as-targets
[10] https://www.aljazeera.com/news/2026/3/11/iran-declares-us-israeli-economic-banking-interests-in-region-as-targets
[11] https://www.reuters.com/business/energy/iran-says-oil-will-reach-200-barrel-warns-continuous-strikes-2026-03-11/
[12] https://www.csis.org/analysis/no-one-not-even-beijing-getting-through-strait-hormuz
[13] https://www.reuters.com/world/middle-east/airlines-begin-hike-fares-due-higher-fuel-prices-shares-stabilise-2026-03-10/
[14] https://www.reuters.com/business/energy/iran-says-oil-will-reach-200-barrel-warns-continuous-strikes-2026-03-11/
[15] https://www.cnbc.com/2026/03/11/strait-of-hormuz-closure-shipping-economy-oil.html
[16] https://www.reuters.com/world/europe/trump-tells-britain-he-does-not-need-its-help-win-iran-war-2026-03-07/
[17] https://www.reuters.com/business/aerospace-defense/romanian-review-us-request-use-local-air-base-iran-operations-2026-03-11/

Despite declared US and Israeli ambitions for the conflict to trigger regime change, and calls from both President Trump and Prime Minister Netanyahu for Iranians to seize power, the Iranian regime is aggressively deterring civil unrest, including protest activity.[18] [19] Inconsistent and non-committal messaging both continue to make it difficult to infer with confidence the conditions which would allow the conflict to be assessed as successful, and brought to an end.[20] [21] From an Iranian perspective, the initial retaliatory acts are reported to have been the result of an early 'fire at will' order when the conflict began and command structures were disrupted. In contrast, Iran is likely now implementing a plan developed over decades for this situation.[22] More recent applied knowledge and drone technology from Russia's war against Ukraine is also relevant. Iran's strategy can be understood as two broad strands:

1) Leveraging its ability to create high impact physical and economic disruption in the region to create sufficient geopolitical pressure on the US and Israel to end the war before the regime falls.

2) Forcing the US, Israel and their allies to use up limited supplies of defensive capabilities against drones and other mass-produced weaponry; allowing Iran to tolerate earlier losses to enable them to apply their military pressure more effectively later in the war - a form of 'asymmetric endurance'.[23]

Global organisations and leaders continue to work to mitigate the impact of the conflict, including diversion of Iraqi oil through Turkish infrastructure, and planning to mobilise global oil reserves.[24] [25]

Iran's current crisis appears to have reinforced, and potentially elevated, the level of control and influence held by the Iranian military, in particular the Supreme Leader's specialist armed force the Islamic Revolutionary Guard Corps (IRGC). Having appeared to have pressurised Iran's political leadership away from a diplomatic approach, early reports that Iran's Supreme Leader Ali Khamenei had been killed early in the war were confirmed by the appointment of the IRGC's preferred candidate; the former leader's son Mojtaba Khamenei.[26] [27] Mojtaba is reported to have served in the IRGC and is described as a hardline cleric currently subject to US sanctions.[28] Reportedly injured in the same strikes which killed his family, and under threat of assassination by both Israel and the US, the new leader has not yet made a public appearance.[29] [30] The IRGC and other military leaders continue to fill the public power void.

Cyber Developments

As of 11th March, more than 300 claimed cyber-attacks have been reported since the beginning of the military operation on Iran. Distributed Denial-of-Service (DDoS) attacks account for over 60% of these claimed attacks, followed by web defacement at 24%.[31] The conflict overall has driven a surge in AI-generated propaganda and fabricated imagery circulating across various social platforms as well which further complicates efforts to conduct credible assessments of incidents as false content blends with legitimate reporting.[32]

Noteworthy cyber activity during this reporting period includes the targeting of an unnamed bank, airport, NGO and a software company in the US and Canada. On 5th March Symantec and Carbon Black released a report that identified the threat activity and attributed it to the MOIS-linked threat actor MuddyWater (aka Seedworm).[33]

---

[18] https://www.aljazeera.com/video/newsfeed/2026/3/11/iran-security-chief-warns-against-anti-government-protests
[19] https://www.aljazeera.com/news/2026/3/7/iranian-authorities-warn-against-fifth-column-as-no-signs-of-war-abating
[20] https://www.theguardian.com/us-news/2026/mar/07/trump-rationale-war-iran-story
[21] https://www.nytimes.com/2026/03/10/us/politics/trump-iran-war-how-long-timeline.html
[22] https://www.bbc.co.uk/news/articles/cz7g2qrz8vdo
[23] https://www.nytimes.com/2026/03/03/world/europe/iran-war-strategy-trump-israel.html
[24] https://www.reuters.com/business/energy/iraq-asks-krg-help-pipe-crude-oil-turkey-sources-say-2026-03-11/
[25] https://www.reuters.com/business/energy/iea-proposes-largest-ever-oil-release-strategic-reserves-wsj-reports-2026-03-11/
[26] https://www.nytimes.com/2026/03/07/world/middleeast/iran-president-pezeshkian-gulf-apology-war.html
[27] https://www.reuters.com/world/middle-east/irans-new-leader-still-silent-was-elevated-by-revolutionary-guards-2026-03-10/
[28] https://www.aljazeera.com/features/2026/3/8/who-is-mojtaba-khamenei-a-contender-for-irans-leadership-amid-war
[29] https://www.reuters.com/world/europe/trump-rejects-settling-iran-war-raises-prospect-killing-all-its-potential-2026-03-08/
[30] https://www.reuters.com/world/middle-east/israel-believes-irans-new-leader-was-lightly-wounded-attacks-senior-official-2026-03-11/
[31] https://socradar.io/iran-israel-cyber-conflict-dashboard/
[32] https://www.bbc.com/news/articles/ckg8wvz427vo
[33] https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us

However, the report notes that the threat activity has been active on the target's network since the beginning of February, predating the current military operation. Another report published by CloudSEK on 6th March found that more than 60 Iran-aligned groups have used AI-assisted reconnaissance tools to scan and map potential targets across US critical infrastructure, focusing on exposed Industrial Control Systems (ICS) using default credentials.[34] Compromise of ICS environment could potentially enable disruptive or destructive cyber-physical attacks against sectors such as energy, water, or transportation. However, as of this writing, no confirmed operational impact associated with this activity has been observed.

On 9th March, Israeli media reported that several cyber-attacks attributed to Iran-nexus threat actors have targeted a wide range of organisations in Israel in recent days, citing the Israeli National Cyber Directorate.[35] While further details remain limited, the report stated that the attacks were intended to wipe data and disrupt business activities.

An additional feature of the conflict's cyber dimensions is the targeted exploitation of cameras by both sides. Checkpoint observed Iranian-attributed actors attempting to access Hikvision and Dahua IP cameras across Israel and Gulf states from 28th February, consistent with Iran's assessed tactic of leveraging camera access for battle damage assessment and targeting correction in support of missile operations.[36] Conversely, Israel reportedly hacked Tehran's traffic camera network and used the footage to track the movements of Khamenei's bodyguards and Senior Officials ahead of the February strikes.[37]

Overall, the volume and nature of the observed activity reinforce NCC Group's previous assessment that pro-Iranian cyber operations linked to the conflict would mainly consist of low-impact, high-volume attacks that largely target geographies directly involved in the conflict.

Iranian Government Direct Threat

Since the release of the first report last week, our assessment of Iran's state-sponsored cyber operations remains largely unchanged: Iran's APTs are assessed to have switched to supporting war-time efforts and as the national internet connectivity level remains at 1%, there is little capacity for launching cyber operations using domestic infrastructure.[38] Although state actors likely retain preferential access to remaining connectivity, which may explain how MuddyWater has sustained one of the most significant confirmed operations attributed to an Iranian state-sponsored group in this period. Symantec and Carbon Black's Threat Hunter Team identified activity associated with the group on networks belonging to a US bank, airport, software company and non-governmental organisations in both the US and Canada, as well as the Israeli operations division of one victim, with the activity beginning in February 2026 and continuing in the days following the launch of Operation Epic Fury. Dindoor, a previously unreported backdoor, which leverages the Deno runtime for JavaScript and TypeScript execution was found on the networks of the Israeli-outpost of the software company, the US bank and Canadian NPO; while Fakeset, a python backdoor was used on the US airport and non-profit.[39] Both backdoors were signed with certificates linked to previously identified MuddyWater infrastructure.[40]

While MuddyWater has not been associated with wiper deployment in past campaigns, its presence in these networks predating the conflict means that, should access be retained, the group would be in a position to sustain espionage activities or pivot to disruptive operations as the conflict continues.

Appendix A of this report covers nation state capabilities for Iran, Israel and the US.

[34] https://www.cloudsek.com/blog/ai-the-iran-us-conflict-and-the-threat-to-us-critical-infrastructure
[35] https://www.jpost.com/business-and-innovation/article-889314
[36] https://research.checkpoint.com/2026/interplay-between-iranian-targeting-of-ip-cameras-and-physical-warfare-in-the-middle-east/
[37] https://www.timesofisrael.com/report-israel-hacked-tehran-traffic-cameras-to-track-khamenei-ahead-of-assassination/
[38] https://mastodon.social/@netblocks/116215079677400761
[39] https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us
[40] https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us

Indirect Threats

Cyber Criminals

Traditional cybercriminal actions, like those we may see from financially motivated threat actors or Organised Criminal Groups (OCGs), have not been seen to be a major part of the Iranian response to Operation Epic Fury. Instead, the majority of actions seen in the cyberspace appear to be conducted by state-sponsored actors such as MuddyWater, hacktivists such as FAD Team or hacktivist fronts such as the MOIS-affiliated Handala Hack. These groups are examined in detail elsewhere in this report.

Organisations should be alert, however, to the use of traditional cybercriminal TTPs and the integration of elements of the cybercriminal ecosystem into the arsenals of Iranian state-sponsored and state-aligned actors and hacktivists. Multiple groups have been observed utilising tools commonly seen in cybercriminal campaigns, such as the infostealer Rhadamnthys. Ransomware has also been used to destroy victim organisation's data and to cover the tracks of attackers, and the affiliate model of known ransomware operations such as Qilin have been exploited to obfuscate attackers' identities.[41]

Cybercriminals with no link to Iran remain a threat. Regardless of where they are located, many OCGs will seize upon the conflict to launch attacks of their own. OCGs may choose to recycle old data and attack claims which, due to the chaos resulting from the war, may become harder to verify or attribute with confidence. It is also likely that malicious actors, whether OCGs or state actors outside of Iran, will use the topic of the war as an emotive lure for phishing and spearphishing attacks. These will expand beyond the META region where much of the malicious cyber activity has so far been observed and could impact organisations around the globe.[42]

Hacktivism

Since our last published report, the hacktivist landscape surrounding the US/Israel-Iran conflict has continued to expand in volume and diversification of the actors involved, while core tactics remain the same. Between the previous publication and 12th March, the number of hacktivist groups engaged in activities related to the war has increased from 60 to 84, with DDoS and hack-and-leak claims continuing to dominate reported threat activity.[43] [44] As outlined last week, Iran's domestic connectivity collapsed to roughly 1% of normal levels following US/Israeli strikes on Iran, and this remains the case, which significantly limits the ability of state-aligned operators inside Iran to coordinate, communicate, or publish activity.[45] There are also still fewer groups active compared to the 12-Day War[46] [47], while hacktivists operating from outside of Iran such as NoName057(16) and 313 Team appear to be filling the operational vacuum created by the blackout. It is important to note that Handala Hack's continued activity could be supported by Starlink connectivity as the group's usage of it was observed during the January blackout.[48]

As previously assessed, governments, critical infrastructure and technology sectors in both Israel and the Gulf remain the primary targets for hacktivists, while US entities have seen limited DDoS attempts.[49] For example, on 8th March a pro-Iranian hacktivist group based in Iraq, 313 Team, claimed to have conducted multi-hour attacks against several Kuwaiti governmental websites, while also threatening to conduct large-scale cyber operations against

[41] https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/
[42] https://www.fortinet.com/blog/threat-research/cyber-fallout-after-the-strikes-signal-noise-and-what-comes-next
[43] https://x.com/Cyberknow20/status/2029886368017699003
[44] https://x.com/Cyberknow20/status/2031639381732364644
[45] https://x.com/netblocks/status/2031998313797423299
[46] https://x.com/Cyberknow20/status/1934960115016445952
[47] https://x.com/Cyberknow20/status/2031639381732364644
[48] https://x.com/_CPResearch_/status/2013349461070586054
[49] https://www.intel471.com/blog/israeli-us-strikes-against-iran-triggers-a-surge-in-hacktivist-activity

Bahrain's government infrastructure due to their ongoing support of the adversaries in the regional conflict.[50] [51] Outside of the consistent behaviours observed, severable notable shifts have emerged over the past week.

Pro-Iranian and Iran-aligned hacktivists (e.g., some pro-Palestinian groups such as Dark Storm Team)[52] have continued to mostly target Israel and Gulf nations in the past week with familiar tactics earlier observed from them. These include DDoS attacks, website defacements, doxxing and data breaches, with Israeli entities being the most impacted, closely followed by Kuwait, Jordan, Bahrain, Qatar and the UAE.[53] Against this backdrop of low-impact activity, one development stands out as a departure from what was observed last week. Handala Hack, assessed to be operating within the MOIS, plays a central role: alongside unverified claims against critical infrastructure such as Aramco[54], the group seemingly achieved success with a wiper attack on US medtech firm Stryker on 11th March.[55] The attack caused global operational outages across Stryker's environment, with more than 200,000 devices reportedly wiped and systems shut down in offices in 79 countries.[56] This attack marks the first confirmed large-scale destructive operation Handala Hack have successfully executed since the start of the war and demonstrates a level of destructive capability far beyond their earlier, largely unverified claims against high-value targets.

Another development is the re-emergence of the alleged hacktivist, Mr Soul, a persona included in the indictment of CyberAv3ngers, who announced their return to operations after a break in the aftermath of the first US-Israeli strikes on Iran and claimed access to Israel's power transmission infrastructure.[57,58] This illustrates how the conflict also attracts experienced operators known for previously targeting ICS and SCADA systems in both Israel and the US. Additionally, Telegram appears to be playing an increasingly central role in operations as threat actors not only use the platform for framing anti-Western or anti-Israeli narratives as justification for retaliatory hack-and-leak operations and DDoS attacks, but also to share real-time updates on the conflict.[59] To illustrate: hours prior to Bahrain confirming damage to a water desalination facility due to an Iranian drone strike[60], pro-IRGC aligned channels have circulated maps of Bahrain's desalination plants on Telegram noting their strategic importance to the country's water supply.[61] While the timing is notable, it remains unclear whether this activity reflects prior knowledge of the attack or whether it was a simple coincidence, meaning multiple hypotheses should be considered. OSINT analysis of a pro-Iranian Telegram channel, CyberBan, further indicates the channel likely operates as an information-exchange system within the Iranian cyber ecosystem as it amplifies hacktivist personas and operators such as Mr Soul while intentionally minimising references to sanctioned IRGC units like CyberAv3ngers.[62] A possible reason for doing so is that it is part of a broader OPSEC-driven proxy strategy, but this remains unclear. Taken together, these developments may suggest that Telegram is being used as a space for operational signalling within both Iranian cyber and kinetic operations and monitoring such channels may provide early indicators of sectors that may be at elevated risk.

Within the expanding ecosystem, Russian hacktivist involvement has become more visible as well. Similarly to the 12-Day War, pro-Russian collectives are increasingly participating in coordinated operations against Israeli and Western assets, often branding their campaigns under previously used umbrellas such as #OpIsrael.[63] [64] For instance, the Russian Legion Telegram channel has shared on 10th March a message from a group calling itself "Cardinal" who alleges they infiltrated systems connected to Israel's nuclear infrastructure, while not providing any

[50] https://x.com/FalconFeedsio/status/2030705942137070072
[51] https://x.com/FalconFeedsio/status/2030316564692734105
[52] https://x.com/FalconFeedsio/status/2028159882000822755
[53] https://www.intel471.com/blog/israeli-us-strikes-against-iran-triggers-a-surge-in-hacktivist-activity
[54] https://x.com/FalconFeedsio/status/2028774486078816480
[55] https://www.reuters.com/technology/stryker-shares-fall-after-report-suspected-iran-linked-cyberattack-2026-03-11/
[56] https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/#more-73316
[57] https://x.com/Cyberknow20/status/2027959605758963870
[58] https://industrialcyber.co/reports/cyber-retaliation-surges-after-us-israel-strikes-on-iran-as-hacktivists-hit-governments-defense-critical-sectors
[59] https://www.darkowl.com/blog-content/dark-web-reactions-to-the-israel-iran-conflict/
[60] https://www.wsj.com/livecoverage/iran-war-news-updates-2026/card/iran-strikes-desalination-plant-in-bahrain-says-gulf-nation-mwjEnNJK1GgtebiNnUaZ
[61] https://x.com/FalconFeedsio/status/2030541114378440832
[62] https://x.com/FalconFeedsio/status/2030988845710442542
[63] https://x.com/Cyberknow20/status/2024083988176937353
[64] https://www.cybersecuritydive.com/news/pro-russia-actors-support-iran-nexus-hackers/813647/

evidence of the claim.[65] This mirrors established hacktivist patterns as observed with both pro-Russian and pro-Iranian actors: high-volume DDoS claims rather than substantiated breaches intended to generate noise. More significant however is the clear expansion of both pro-Russian and aligned pro-Palestinian hacktivists focusing on Western targets over the past week. Groups such as NoName057(16) and the Bangladeshi pro-Palestinian group, BD Anonymous, have expanded targeting beyond Israel and the US to include Germany, Greece and Cyprus which reflects how the cyberfront is widening to encompass nations indirectly linked to the conflict but geographically distant from it. [66] [67] [68] In addition, over the past days the conflict's spillover reached Australia as pro-Palestinian groups BD Anonymous and RipperSec launched DDoS-attacks against Australian organisations (e.g., the website of Tasmanian police) in response to Australia's military support for the UAE and its decision to grant asylum to members of Iran's women football team.[69] [70] The high-visibility backlash in Iran (e.g., threats to players' families) following the women refusing to sing the national anthem during one of the matches has drawn significant media attention which hacktivists weaponised as part of the anti-Australian narratives.[71] This represents a different kind of targeting expansion, driven not by direct military alignment but rather the reputationally sensitive nature of the incident with regards to the IRGC. It remains unclear however, whether the hacktivist activity is fuelled more by Western media coverage of the asylum decision or by domestic outrage inside Iran. Collectively, these campaigns illustrate how rapid local political developments can be absorbed into the broader hacktivist landscape.

While pro-Iranian and pro-Russian groups are dominating the hacktivist space, anti-Iranian hacktivism has also emerged. As published on their Telegram channel Anonymous – אַנוֹנִימִי has released PII of Basij forces and IRGC personnel obtained via both the Iranian Civil Registry Organization and Sepah bank. In parallel, Anonymous Syria Hackers claimed they breached the database of an e-commerce website resulting in leaked PII, credentials and PayPal account information.[72] [73] Such information can support follow-on operations by other actors, including the targeting of IRGC personnel, doxxing campaigns, credential-based intrusions. At this stage however, it remains too early to assess whether these incidents represent a broader trend from anti-Iran hacktivists towards obtaining PII for further cyber-activity. As with all hacktivist reporting, these claims should be treated with caution until independently verified with technical evidence.

China

Outside of the sphere of actors and belligerents with direct involvement in the ongoing conflict, other nation states are using the unfolding situation as part of their own opportunistic cyber operations. Most notably, the China-attributed APT, Camaro Dragon (Mustang Panda). In the immediate aftermath of the conflict escalation sent conflict-themed spearphishing lures and attempted to deploy PlugX against Qatari targets.[74] In a separate campaign observed in the same time frame, attackers impersonated the Israeli government and sent a .zip archive called "Strike at Gulf oil and gas facilities" to targets which dropped a Rust-based loader that eventually loaded Cobalt Strike. The latter campaign is attributed with a lower confidence to China-nexus actors. Similar activity from Mustang Panda was observed by Acronis after the US capture of Maduro in January 2026. In that case, politically themed ZIP archives containing the LOTUSLITE backdoor were sent to US government and policy related entities.[75] Taken together, these campaigns demonstrate the speed at which China-nexus actors pivot in response to such geopolitical flashpoints.

This tactic is not unique to Chinese actors, however. Such flashpoints create perfect conditions for APTs and cybercriminals alike as targets actively seek out new information and lower their guard. In turn, these crises

[65] https://x.com/FalconFeedsio/status/2031276814426140766?s=20
[66] https://x.com/FalconFeedsio/status/2030931618391822446
[67] https://x.com/FalconFeedsio/status/2030576196363366792
[68] https://x.com/FalconFeedsio/status/2031363006429630824
[69] https://x.com/Cyberknow20/status/2031282240622309431
[70] https://x.com/FalconFeedsio/status/2031732318935916766
[71] https://www.abc.net.au/news/2026-03-10/australia-grants-asylum-to-five-iranian-football-players/106435506
[72] https://industrialcyber.co/reports/cyber-retaliation-surges-after-us-israel-strikes-on-iran-as-hacktivists-hit-governments-defense-critical-sectors/
[73] https://x.com/DailyDarkWeb/status/2029594268864536707
[74] https://blog.checkpoint.com/research/china-nexus-activity-against-qatar-observed-amid-expanding-regional-tensions/
[75] https://www.acronis.com/en/tru/posts/lotuslite-targeted-espionage-leveraging-geopolitical-themes/

become pre-built social engineering kits that offer threat actors real organisations and real events to exploit and targets conditioned to treat urgency as legitimacy.

Appendix A- Nation State Cyber Capabilities

Last updated on March 11th, 2026

Iranian Cyber Capabilities

Iran maintains a sophisticated and mature cyber capability. While not operating at the same level as China or Russia, Iranian aligned groups have demonstrated their capacity to target entities across multiple sectors and regions.[76] Their operations, which are designed to align and further state objectives span espionage, influence, and destruction. While primarily orchestrated by state-sponsored groups backed by both the Ministry of Security and the Iranian Revolutionary Guard Corps, the country's capabilities are multiplied through networks of managed proxy groups, and ideologically aligned hacktivist groups, into a single rapidly mobilisable and plausibly deniable force. This force is further amplified by ideologically independent hacktivist groups and cyber actors, including pro-Palestinian collectives, pan-Islamic groups and anti-Western Russian-aligned entities whose campaigns are driven by their own distinct objectives but converge against Israeli, American and Western targets. In times of war, the actions of such groups become indistinguishable from Iran's managed proxy ecosystem, complicating attribution and inflating the perceived scale of actor involvement in the cyber domain.

State-Supported Cyber Operations

Iran's cyber offensive capabilities are directed through the IRGC, which operates under the authority of the nation's Supreme Leader and the Ministry of Intelligence of the Islamic Republic of Iran (MOIS), which sits under the civilian presidency. [77] Despite this separation, both organisations maintain affiliated state-sponsored APTs with the IRGC overseeing APT42, APT33, APT35 and the MOIS directing APT34 and MuddyWater. Each of which leverages the nation's infrastructure to carry out distinct objectives ranging from espionage and sabotage to influence operations targeting entities including foreign governments, dissidents, and critical infrastructure. Such attribution has been made over the years through technical analysis that draws on shared or reused malware infrastructure, repeated tactics, techniques and procedures, Farsi-language artefacts embedded in code, leaks and indictment from the US Department of Justice identifying specific IRGC and MOIS personnel by name. While objectives and targeting may differ across these various groups, shared TTPs and operational coordination suggest a degree of integration which amplifies the overall capabilities of Iran in the cyber domain. The following paragraphs will present an overview of the main APTs, and hacktivist-fronts attributed to Iran's IRGC and MOIS.

APT34

APT34 is one of the most prominent and well documented Iranian threat actors tied to the MOIS. Active since at least 2014, the group was previously tracked as two separate entities, APT34 and OilRig however overlapping activities led to the two being consolidated into one. APT34 targets map directly to Iran's geopolitical and strategic interests, with previous sectors including government, chemical, energy, telecommunications and financial, with a particular focus on organisations operating in the Middle East. APT34's operations, however, are not restricted to this region, with past campaigns targeting organisations in Europe, North America and parts of Asia also. Due to this focus on geopolitical and strategic interests, APT34's campaigns revolve around long-term access and data collection rather than short-term disruptions.

The group's campaigns emphasise stealth and persistence, blending open-source tools and custom-built malware families across intrusions. Across each phase of the attack chain, APT34 operates methodically. Extensive

[76] https://www.defenseone.com/threats/2026/02/strikes-iran-will-test-us-cyber-strategy-abroad-and-defenses-home/411782/
[77] https://www.csis.org/blogs/strategic-technologies-blog/beyond-hacktivism-irans-coordinated-cyber-threat-landscape

reconnaissance is conducted to identify vulnerable systems and potential access points as well as to provide the research required for the group to create tools tailored to specific target environments[78, 79].

During initial access, the group routinely use social engineering techniques like spear-phishing across different mediums including email and LinkedIn to deliver their payloads. Credential harvesting is done through widely available tools like Mimikatz or LaZagne while persistence is established using scheduled tasks, registry modifications or remote access services like Outlook Web Access. These tactics reflect APT34's overarching commitment to low-profile and low noise generating intrusions which is further committed to using DNS tunnelling and encrypted fallback channels for command and control[80].

Its arsenal is constantly expanding and includes custom exfiltration tools like STEALTHOOK, IIS backdoors and custom webshells. Alongside these, APT34 has an extensive catalogue of historically deployed tools, including Alma Communicator, BondUpdater, Clayslide, DNSExfiltrator, DNSpionage, Fox Pane, GoogleDrive RAT, Helminth, ISMInjector, and keyloggers KEYPUNCH and LONGWATCH, among many others. The breadth of this toolkit reflects group's capability to conduct a wide range of operations spanning reconnaissance, lateral movement, exfiltration, and where required, destruction[81].

APT34's operational flexibility, combined with a customised, modular toolset, reflects its ability to adapt quickly to target environments and ensure it can maintain long-term persistence. As one of Iran's most prolific APTs, the group's operations will likely increase as Iran's conventional military options decrease; however, the group's silence in the days ahead of the strikes on February 28th, as assessed by Anomali indicate that they are likely already involved in pre-positioning operations[82].

MuddyWater

MuddyWater is a MOIS-affiliated actor first observed in 2017, targeting government, telecommunications, energy and private sector organisations primarily in the Middle East, but with past campaigns reaching into Europe and the US also. Historically, this group has operated high tempo campaigns abusing legitimate remote monitoring and management tools like PDQ to blend into normal IT operations, but since 2025 they have shifted towards more targeted and sophisticated intrusions that use custom malware[83].

MuddyWater's evolution towards a more sophisticated operation is evident in the group's recent campaigns. In October 2025, Group-IB reported on a phishing campaign attributed to the group, in which they compromised a legitimate email account and used it to distribute the Phoenix v4 backdoor to over 100 government entities across MENA, with targets including embassies, and foreign ministries[84]. In December 2025, ESET Research identified a separate campaign primarily targeting critical infrastructure organisations in Israel and Egypt. The campaign deployed MuddyViper, a new backdoor loaded reflectively into memory via a custom loader called Fooder, combined with Sleep API calls to evade automated analysis. This tactic is notably more sophisticated evasion technique than the group's historically noisy tradecraft[85]. In this campaign, operators also deliberately avoided hands-on-keyboard interactive sessions during intrusions to reduce the forensic noise that has historically aided detection of MuddyWater intrusions

More recently, Group-IB identified Operation Olalampo in January 2026, which revealed four new malware variants deployed against organisations in MENA: CHAR, a Rust-based backdoor using a Telegram bot for command-and-control; GhostFetch and HTTP_VIP, novel downloaders; and GhostBackDoor, an advanced persistence implant. Rather than being an isolated campaign, analysis of the Telegram bot used for command and control discovered by Group IB on January 26th 2026, showed that post-exploitation activity went back as far as October 2025. [86] Analysis of the malware itself indicated AI-assisted development also. In a separate campaign, covered by Amazon Threat Intelligence in November 2024, MuddyWater compromised servers hosting live CCTV feeds in Israel which

[78] https://www.levelblue.com/blogs/levelblue-blog/inside-apt34-oilrig-tools-techniques-and-global-cyber-threats
[79] https://socradar.io/blog/dark-web-profile-oilrig-apt34/
[80] https://unit42.paloaltonetworks.com/threat-brief-iranian-linked-cyber-operations/
[81] https://www.levelblue.com/blogs/levelblue-blog/inside-apt34-oilrig-tools-techniques-and-global-cyber-threats
[82] https://www.anomali.com/blog/cyber-threat-briefing-iran-retaliatory-posture
[83] https://www.group-ib.com/blog/muddywater-operation-olalampo/
[84] https://www.group-ib.com/blog/muddywater-espionage/
[85] https://www.eset.com/us/about/newsroom/research/iran-muddywater-critical-infrastructure-israel-egypt-snake-game-eset-research/
[86] https://www.group-ib.com/blog/muddywater-operation-olalampo/

provided coverage of subsequent missile strikes.[87] This campaign, like others demonstrates Iran's use of its APTs as an extension of its kinetic operations.

In the currently evolving conflict, MuddyWater's role as an initial access broker for other Iranian-aligned groups and persistence specialist is particularly significant. Its broad footprint across government and telecommunications networks means access is likely already pre-positioned in targets of interest, available for handoff to more destructive actors or for activation as part of a wider retaliatory campaign.

APT33

APT33 is an IRGC-affiliated actor that first emerged in 2013. Since then, the group's primary focus has been espionage, with persistent targeting of sectors aligned with Iran's strategic interests, namely petrochemical, aerospace, and defence adjacent supply chains, as well as periodic campaigns against the finance, telecommunications, research and government sectors.[88] The geographic scope of these campaigns has primarily focused on organisations in the US, Saudi Arabia and South Korea, with additional targeted countries including the UK, UAE and Belgium.[89, 90] Beyond espionage, APT33 has been attributed to destructive campaigns involving the deployment of wipers, such as Shamoon, which have historically targeted the energy sector in the Gulf region. [91]

For initial access, APT33 relies on spear-phishing, notably by using publicly available job postings to craft targeted career-related messages to lure their victims. Beyond this, the group has also used known vulnerabilities to compromise systems. Post compromise, the group combines commodity malware and custom tools: publicly available tools include Nanocore, DarkComet, QuasarRAT, NetWire, AlphaShell, Mimikatz, PowerSploit, and PoshC2, while custom malwares include TurnedUp, DropShot, ShapeShift, Shamoon and Powerton.[92] Capabilities of these tools include password stealing, C2 command execution, data exfiltration, and installation of additional modules. APT33 also uses Ruler, a lesser-known tool used for remotely interacting with Exchange servers and manipulating client-side Outlook features to enable persistence and lateral movement. [93]

Given APT33's persistent focus on energy and defence supply chains, organisations operating in or adjacent to those sectors should treat the current escalation as a prompt to review exposure, particularly given the group's demonstrated willingness to pivot from espionage to destruction when strategic circumstances demand it.

APT35

APT35 is an IRGC-affiliated actor linked to the organisation's Cyber Unit 13, whose operations date back to 2014.[94] With a focus on conducting long-term operations focused on strategic intelligence collection, the group targets US and Middle Eastern military, diplomatic and government personnel, organisations in the media, energy and defence industrial base, and engineering, business services and telecommunications sectors.[95, 96] In October 2025, a leaked dataset containing operational and logistical documents was published on GitHub and assessed with high confidence of belonging to APT35.[97] The leak offered insights into the group's organisational structure, personnel, tooling and active campaigns. Such visibility of APT internal workings is rarely gained.

While many of APT35's campaigns are identity-centric and favour social engineering over the use of malware, the group also possesses a mature exploitation capability, rapidly weaponising N-day vulnerabilities in common enterprise applications to gain access to environments of interest. [98, 99] Additionally, for initial access, the group

---

[87] https://www.darkreading.com/threat-intelligence/iran-muddywater-new-malware-tensions-mount
[88] https://cloud.google.com/blog/topics/threat-intelligence/apt33-insights-into-iranian-cyber-espionage
[89] https://www.boozallen.com/insights/cyber/tech/apt33-hunt-report.html
[90] https://attack.mitre.org/groups/G0064/
[91] https://www.trellix.com/blogs/research/the-iranian-cyber-capability/
[92] https://www.boozallen.com/insights/cyber/tech/apt33-hunt-report.html
[93] https://attack.mitre.org/groups/G0064/
[94] https://dti.domaintools.com/research/threat-intelligence-report-apt35-internal-leak-of-hacking-campaigns-against-lebanon-kuwait-turkey-saudi-arabia-korea-and-domestic-iranian-targets
[95] https://unit42.paloaltonetworks.com/iranian-attackers-impersonate-model-agency/
[96] https://www.trellix.com/blogs/research/the-iranian-cyber-capability/
[97] https://dti.domaintools.com/research/threat-intelligence-report-apt35-internal-leak-of-hacking-campaigns-against-lebanon-kuwait-turkey-saudi-arabia-korea-and-domestic-iranian-targets
[98] https://www.cloudsek.com/blog/an-insider-look-at-the-irgc-linked-apt35-operations
[99] https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/

uses spear-phishing emails which redirect victims to impersonated websites for credential harvesting and token theft, alongside watering hole attacks and supply chain compromise. Post compromise, APT35 deploys a combination of custom backdoors and commodity tooling, including Sponsor, Soldier, BellaCiao, DownPaper, Mimikatz, and PsExec, to maintain persistence and exfiltrate sensitive data. [100]

Given APT35's focus on long-term access against government and defence-adjacent targets, organisations operating in or with visibility into regional strategic decision-making should treat the current situation as elevating their exposure to this group.

APT42

APT42 is an IRGC-IO-affiliated actor operating under the internal intelligence subdirectorate tasked with the surveillance of individuals considered foreign or domestic threats to Iran. Targets from past campaigns have included journalists, academics, think tank researchers, diplomats, NGO staff, and diaspora communities who APT42 used to obtain long-term access to personal communications, shared drives, and cloud environments. With a heavy reliance on social engineering, operators invest weeks or months into cultivating relationships with targets by masquerading as news outlets, NGOs and legitimate services before delivering malicious links or payloads.[101, 102]

Since 2024, APT42 has used custom phishing kits to impersonate popular email providers like Gmail, Outlook, and Yahoo, to target individuals while attackers pose as security professionals to steal credentials and two-factor authentication codes via WhatsApp and email.[103] In cases where data extraction using social engineering isn't sufficient and host-level device access is required; the group has been observed deploying custom backdoors like NICECURL and TAMECAT. [104]

In comparison to other APTs with more evidently disruptive or destructive objectives APT42 is less focused on infrastructure compromise but instead on compromising individuals. A single account breached by the group belonging to high-value targets like policy professionals, defence contractors, or executives with access to sensitive communications can offer intelligence of equivalent or greater value than what could be gleaned through network intrusion, with the additional advantage of leaving less artefacts. As Iran actively seeks intelligence on US, Israeli and allied decision-making in the current situation, APT42's modus operandi makes it an elevated threat to personnel operating in government, defence, and critical infrastructure, where information gathered could be used to influence Iran's own strategic decision making.

Iranian Hacktivist Personas

Handala Hack

Handala Hack is assessed to be hacktivist persona managed by the MOIS-linked group, Void Mantichor, that emerged in 2022.[105] Incorporating hacktivist tactics to achieve Iranian state interests, the group's past campaigns have focused on the exploitation of exposed services, credential theft, social-engineering, and direct deployment of destructive malware against Albanian, Israeli and Gulf State targets. In comparison to Iran's other hacktivist personas, Handala Hack maintains a higher level of operational sophistication, combining state-directed destructive capability with a highly active public-facing propaganda operation across Telegram and leak sites.[106]

In alignment with their destructive capabilities, Handala Hack's intrusions prioritise impact over stealth; exfiltrated data is published to their public facing channels likely to inflict psychological pressure; and wiper malware is deployed to maximise operational disruption to the targeted systems.[107] The group often pairs custom wipers like CaddyWiper and ZeroCleare with commodity malware and tools like Rhadamanthys infostealer, which provides additional capabilities to Handala Hack while[108]complicating attribution. Handala Hack's intrusions follow a

[100] https://www.trellix.com/blogs/research/the-iranian-cyber-capability/
[101] https://www.wiz.io/academy/threat-intel/what-is-apt42
[102] https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations
[103] https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/
[104] https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations
[105] https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/
[106] https://brandefense.io/blog/void-manticore-apt-2025/
[107] https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/
[108] https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/

common attack chain where spear-phishing is used for initial access, followed by data exfiltration before wiper deployment. This combination maximises impact by ensuring that stolen data can be weaponised in later information operations regardless of whether the destructive payload succeeds.[109]

Handala Hack has demonstrated a notable capacity to sustain its operations amidst internet disruptions and infrastructure degradation. Following internet restrictions in January 2026 imposed in response to mass protests the group's campaigns initially fell silent before resuming and operating from Starlink[110] to target regional entities. CheckPoint confirmed that according to their own data, Handala Hack's use of Starlink continued until at least February 28 and suspect that it continues. [111] [112]

As Iran's conventional military options continue to degrade, destructive cyber operations have the potential to become one of its primary remaining offensive capabilities. While Void Manticore's target scope has historically centred on Israeli and Albanian organisations, the current conflict environment elevates the risk of scope expansion to include US and Gulf state targets directly. Such an assessment is supported by the March 11th attack on US medical technology manufacturer, Stryker, allegedly involving wiper deployment that disrupted global operations and displayed internal branding associated with Handala Hack.[113] [114] While the group claimed responsibility for this attack, Stryker has yet to corroborate this. Should this be corroborated, the Stryker incident confirms the group's operational capacity remains functional. As such, organisations in sectors previously targeted by Handala Hack, including energy, healthcare, government, and defence, particularly those with supply-chain relationships in Israel or the Gulf, should treat the threat from this group as elevated.

Agrius

Agrius is a MOIS-linked actor first seen in 2020 who conducts destructive wiper and fake-ransomware operations against Israeli organisations across multiple industries and regions under a hacktivist cover.[115] [116] Compared to other hacktivist personas, Agrius is more developed and boasts a more sophisticated toolset. Their attacks carry two distinct hallmarks, both of which highlight the group's priority on impact: exfiltrated data is leaked to social media or Telegram channels; and wiper deployment to inflict maximum damage to systems.[117]

Agrius intrusions involve exploiting internet-facing web servers, deploying ASPX webshells, and using living-off-the-land techniques for lateral movement before deploying wiper malware or fake-ransomware to destroy data with ransom demands included as deliberate misdirection to obscure their state direction.[118] Outside of custom wiper and exfiltration tools, Agrius uses publicly available software as part of its arsenal. During the twelve-day war, in June 2025, Agrius-linked infrastructure was observed actively scanning for vulnerable cameras across Israel, likely for supporting post-attack damage and battle-damage assessment for Iranian military planners.

As Iran's conventional military options degrade, destructive operations have the potential to become one of its primary remaining offensive capabilities. While Agrius' target scope was previously limited to Israeli organisations, there is potential for the scope to expand and include the US and Gulf states.[119] Organisations in sectors that Agrius has previously targeted, such as technology and higher education, and that have supply chain relationships in Israel, should consider these threats from this group as elevated risks.

---

[109] https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/
[110] https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/
[111] https://www.firstpost.com/tech/how-irans-handala-hackers-are-using-elon-musks-starlink-for-cyberattacks-amid-internet-blackout-ws-e-13985806.html
[112] https://www.forbes.com/sites/thomasbrewster/2026/03/02/iran-hackers-use-elon-musk-starlink-to-stay-online/
[113] https://www.irishexaminer.com/news/munster/arid-41808308.html
[114] https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/
[115] https://www.truesec.com/hub/blog/iran-uses-hacktivism-as-cover-for-destructive-cyber-attacks
[116] https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/
[117] https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/
[118] https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/
[119] https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026

Cyber Av3ngers and DarkBit

Both Cyber Av3ngers and DarkBit are state-enabled hacktivist personas used by Iran to provide plausible deniability for disruptive and destructive operations. Both have been identified by SentinelOne.[120]

By operating under hacktivist brandings, Iran lowers the threshold for attribution and complicates political response to these operations. The TTPs, targeting, and overall capabilities observed behind both personas, as well as Agrius, such as destructive wiper deployment, ICS/OT exploitation, and coordinated Telegram amplification, go beyond the capabilities commonly demonstrated by independent hacktivist groups, making them more consistent with state-level resourcing.

The leadership vacuum created by the 28th February strikes further complicated this picture, as the command structure overseeing these personas has likely been disrupted, increasing the likelihood for decentralised and unpredictable proxy activities, as fronts used for psychological impact and as a force multiplier alongside Iran's formalised APT ecosystem.[121]

Iran Conclusion

Iran's cyber capabilities, while clustered under strategic objectives, are not a single team with a single playbook; they reflect a layered system operating across multiple verticals simultaneously. As described in the profiles above, Iran pursues espionage, disruption and destruction through different actors, against different targets, in different sectors and different regions, using methods that are not mutually exclusive. An organisation that hardens its network against MuddyWater's initial access tradecraft may still lose sensitive communications through an APT42 campaign targeting a senior employee's personal account. Similarly, an organisation monitoring APT34's DNS tunnelling may still face an Agrius wiper delivered through supply chain compromise. While these groups have historical targeting patterns, in the current situation, where Iran's conventional military options are diminishing, its reliance on cyber capabilities as the primary focus of its offensive operations could increase. Such load bearing may stretch operations and push its APTs beyond their established target sets, as the personnel behind them struggle to balance competing operations that are ultimately geared towards the regime's grand strategic objective: self-preservation.

Israeli Cyber Capabilities

Israel maintains a well-developed cyber capability for a nation of its size, consisting of a deeply integrated military, intelligence, and private sector ecosystem. At its centre is Unit 8200, the signals intelligence and cyber warfare directorate of the Israel Defence Forces. Comparable to the NSA and GCHQ, Unit 8200 is the largest unit in the IDF and provides roughly 80% of the intelligence collected across Israel's various agencies.[122] The unit also serves as the entry point for young technical specialists into the Israeli defence ecosystem, many of whom transition to the country's high-tech sector after service, creating a feedback loop between military capability and commercial innovation that includes some of the world's most prominent cybersecurity companies such as Check Point, CyberArk, and Palo Alto Networks.[123]

Israel's current cyber structure rests on three pillars: Unit 8200, the C4I Directorate (Cyber Defence Division), and the civilian Israel National Cyber Directorate (INCD). The Mossad and Shin Bet, responsible respectively for foreign operations and domestic counterintelligence, also carry out cyber activities. Within the IDF, a Cyber Innovation Unit focuses on developing new tools and solutions in collaboration with the private sector.[124] This entire system is supported by a national technological ecosystem comprising over 80 cyber and surveillance-related companies. The civilian component of cyber defence is represented by the INCD, established in 2018 as the primary body responsible for critical infrastructure security, incident response coordination, and public education.

On the offensive side, Israel has demonstrated a sustained willingness to use cyber operations as an instrument of statecraft, most notably as the co-developer of Stuxnet, the malware that destroyed an estimated 1,000 Iranian

[120] https://www.sentinelone.com/blog/sentinelone-intelligence-brief-iranian-cyber-activity-outlook/
[121] https://fortune.com/2026/03/01/cyber-retaliation-iran-hack-corporate-security/
[122] https://politicsociety.org/2025/09/24/the-evolution-of-israeli-intelligence-in-the-technological-and-military-context/?lang=en
[123] https://defence24.com/geopolitics/cyber-forces-israel
[124] https://defence24.com/geopolitics/cyber-forces-israel

centrifuges at the Natanz nuclear facility between 2008 and 2010[125]. Israel has continued offensive cyber operations against Iranian infrastructure in the years since, targeting port logistics, fuel distribution networks, and financial systems[126]. During the twelve-day war of June 2025, cyberattacks surged by 700% within 48 hours of the opening of hostilities, with the suspected state-linked group Predatory Sparrow wiping data from Bank Sepah and destroying an estimated 90 million dollars in cryptocurrency held on the Nobitex exchange.[127] [128]

US Cyber Capabilities

The US is assessed to possess the most technically advanced cyber capabilities of any nation state, with recent operations demonstrating their willingness to deploy them alongside kinetic strikes or conventional force. While specifications on the components making up the US cyber ecosystem are limited, past military operations have offered insights into their capabilities.

During Operation Midnight Hammer in June 2025, US Cyber Command (CYBERCOM) supported conventional operations by digitally disrupting Iranian air missile defence systems[129]. While the specific nature of this cyber operation was not disclosed, it prevented Iran from launching surface-to-air missiles against US aircraft entering Iranian airspace and CYBERCOM flagged the activity as one of the most complex operations taken against Iran, in the organisation's sixteen-year history. CYBERCOM received similar praise for its role in the January 2026 Operation Absolute Resolve, where the organisation supported by US Space Command used cyber weapons to disable Venezuelan defenses enabling the extraction of Maduro[130]. A former CYBERCOM legal counsel summarised the nation's current posture bluntly: "We really don't do military operations without cyber support anymore. There is a cyber component for everything we do, even if it seems really unsophisticated".[131] The use of CYBERCOM in high-stakes operations such as Midnight Hammer and Absolute Resolve points to the organisation's maturity and established capabilities.

Despite the US boasting a mature offensive cyber capability, its own defensive cyber readiness can be questioned due to recent developments. CISA, the federal agency responsible for cyber threats and alerting both public and private sectors to emerging and ongoing operations has seen a sharp reduction in staff and funding as Trump's administration decreased the workforce by one third[132]. However, experts assert that despite experiencing resourcing issues other national security agencies including the FBI and NSA retain full operational capacity, which can partially offset the reduction in CISA's public-private coordination role in tracking and responding to cyber threats.[133]

[125] https://zendata.security/2026/03/02/cyber-warfare-in-the-us-israel-vs-iran-conflict-roaring-lion-epic-fury/
[126] https://www.picussecurity.com/resource/blog/predatory-sparrow-inside-the-cyber-warfare-targeting-irans-critical-infrastructure
[127] https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/
[128] https://cybersecuritynews.com/predatory-sparrow-group-attacking-critical-infrastructure/
[129] https://therecord.media/iran-nuclear-cyber-strikes-us
[130] https://breakingdefense.com/2026/01/venezuela-150-aircraft-cyber-effects-maduro-operation-how-it-happened-caine/
[131] https://defensescoop.com/2025/06/23/cyber-command-supports-attack-iran-nuclear-facilities-midnight-hammer/
[132] https://www.defenseone.com/threats/2026/02/strikes-iran-will-test-us-cyber-strategy-abroad-and-defenses-home/411782/
[133] https://defensescoop.com/2025/06/23/cyber-command-supports-attack-iran-nuclear-facilities-midnight-hammer/