EIGENRAC

US/Israel-Iran War

Non-Kinetic Hybrid Warfare: GCC Cyber, Information and Economic Operations Threat Assessment April 2026

16-04-2026

EIGENRAC MANAGEMENT FZ-LLC

1. EXECUTIVE SUMMARY

Iran and its aligned actors are running a sustained non-kinetic hybrid campaign against GCC states. They are combining cyber operations, information warfare and economic pressure to disrupt, distract and coerce, either alongside or in place of kinetic action. Cyber activity has evolved from noisy distributed denial-of-service (DDoS) and defacement into more credible claims of intrusions, ransomware and persistent access in finance and government systems, with the UAE and Saudi Arabia most targeted. Information operations, increasingly powered by artificial intelligence and deepfakes, are timed to coincide with cyber events and political developments. Their purpose is to exaggerate damage, confuse audiences and undermine trust in official messaging. Economic pressure is visible in energy export disruption, higher shipping and insurance costs, and episodes of stress in GCC financial markets. For now this remains managed volatility, not systemic crisis, but it demonstrates Tehran's ability to use the Gulf's economic centrality as leverage against perceived US-aligned governments.

Over the next three to six months, the main escalation risk lies in a shift from nuisance and signalling to disruptive cyber actions against energy processing, power generation or desalination infrastructure. Such attacks, if synchronised with information campaigns and renewed kinetic activity, would have both domestic and global impact. Even if missile and drone strikes reduce, pre-positioned network access, information operations infrastructure and economic levers mean the non-kinetic threat to GCC states is likely to remain elevated.

2. CYBER DOMAIN DEVELOPMENTS

Since the 28 February strikes on Iran, hacktivist activity has expanded rapidly. More than sixty groups have mobilised under the Cyber Islamic Resistance banner, claiming hundreds of actions in a short period across over one hundred Telegram channels. These groups are conducting DDoS campaigns, data-wiping attempts and website defacements against government and private-sector networks in the UAE, Saudi Arabia, Bahrain, Kuwait, Qatar and Jordan. Many of these operations are crude and disorganised, designed more to generate noise and divert defensive resources than to deliver strategic effects. Reporting from commercial cyber security providers describes primitive tooling and a lack of consistent tradecraft. In most cases, the impact has been nuisance-level disruption rather than sustained operational degradation.

The UAE has emerged as the most heavily targeted GCC state, allegedly facing up to 700,000 cyberattacks per day and a reported increase of around 175 percent compared to the pre-conflict baseline. Open sources indicate a shift in the UAE from simple DDoS and defacements towards more serious intrusion and ransomware-related claims, particularly against financial, legal and government entities. The group Handala, aligned with Iran, claims to have breached Dubai Courts, Dubai Land Department and the Dubai Roads and Transport Authority, alleging large-scale data theft and destruction. UAE cyber leadership has publicly warned about a move towards automated, AI-enabled attacks that infiltrate networks, move laterally and remain dormant until a “zero hour” trigger, at which point systems could be wiped or taken offline. This suggests intent to establish persistent access that could be used for more disruptive action in future, although the veracity and scale of these specific claims remains unconfirmed.

Saudi Arabia, by contrast, saw fewer early disruption claims but now displays the sharpest growth in cyber-related activity. Reporting shows a rise from a relatively low baseline of posts mentioning Saudi cyber targets to several hundred by early April, with growing emphasis on intrusion attempts, vulnerability testing and ransomware threats rather than simple defacement. Pro-Iranian groups such as the Islamic Cyber Resistance (313 Team) and DieNet have claimed operations against Kuwaiti ministries, Bahraini government portals and airports in Bahrain, Saudi Arabia and the UAE. In Qatar, hacktivist groups claimed attacks on energy-sector websites and state broadcasting infrastructure during the early phase of the conflict, but activity has since shifted towards more generic infrastructure-themed content and threat signalling.

Taken together, these patterns indicate that most current cyber operations are still low-impact and opportunistic, but the environment is becoming more crowded and complex. Iran and its aligned actors are using high-volume, mostly low-grade operations to create the perception of a pervasive cyber onslaught, tie up limited defensive capacity and demonstrate reach. At the same time, selected intrusion and ransomware narratives show a clear ambition to move beyond symbolic hacktivism. There is, however, still limited verified evidence of successful compromise of OT or

industrial control systems in energy, power or desalination, and many large-scale breach and data destruction claims appear inflated for psychological effect. In the near term, the UAE and Saudi Arabia remain the most exposed GCC states in cyber terms, both because of targeting volume and because of the strategic value of their financial, government and aviation infrastructure.

3. INFORMATION DOMAIN DEVELOPMENTS

Iran and its partners are also engaged in a multi-layered information campaign that seeks to shape perceptions of the conflict and to exploit uncertainty. The core aim is not simply to persuade audiences of a single narrative, but to saturate the information environment with conflicting claims such that trust in all sources is eroded. This approach is closely associated with concepts of fifth generation warfare, where the information space itself is a central battlefield.

The current campaign features extensive use of AI-generated content. Analysts have documented more than one hundred distinct pro-Iran deepfake artefacts, and one major investigation identified more than one hundred and ten unique pro-Iran deepfakes circulating over a two-week period. These include fabricated strikes on urban centres and exaggerated damage to infrastructure, such as synthetic imagery of smoke rising from Bahraini high-rise buildings, as well as fake visuals of downed US aircraft. Russian and Chinese state-aligned outlets and proxy accounts have amplified some of these narratives, reposting false claims about successful attacks on US military assets and using them to reinforce broader anti-US messaging.

These information operations are frequently synchronised with cyber incidents and key political events. Banking disruptions are accompanied by rumours of insolvency and impending collapse; airline or airport IT issues are paired with false announcements about closure or mass casualties. The intent is to magnify the psychological and economic effect of relatively small technical events, creating an impression of systemic failure. In the GCC context, this activity plays into an information environment characterised by a large and linguistically diverse expatriate population. Residents consume Arabic, English and a wide range of South and East Asian language media. Authentic and manipulated content coexist across these channels, complicating verification and increasing the likelihood of confusion.

So far, the observable impact in GCC states has been episodic rather than structural. There have been short-term spikes in precautionary behaviour and financial anxiety around specific incidents and rumours, but no sustained, large-scale behavioural shifts. Iran’s information campaign has nevertheless contributed to a wider sense of uncertainty, making it harder for GCC authorities to maintain a single authoritative narrative and increasing the risk that future crises trigger sharper public reactions. As AI tools become more accessible and sophisticated, the barrier to producing convincing deepfakes of GCC leaders, officials and emergency systems will continue to fall, raising the potential for more targeted and damaging information attacks.

4. ECONOMIC PRESSURE AND MARKET EFFECTS

The non-kinetic campaign is also visible in the economic domain. Tehran is pursuing a model of amplified economic pressure in which real and threatened disruption to energy infrastructure, maritime routes and financial systems is used to generate broader market reactions. The key to this approach is the interplay between concrete events and perceptions of risk among traders, insurers and investors.

The Gulf region is a central supplier of refined oil products and LPG to global markets. In 2025, Gulf producers exported roughly 3.3 million barrels per day of refined products and around 1.5 million barrels per day of LPG. Recent attacks and security-driven constraints have taken an estimated three million barrels per day of refining capacity offline in the region. Further afield, refineries outside the Gulf have also reduced throughput due to concerns over feedstock availability, which amplifies the effects on global supply. Disruption around the Strait of Hormuz has reduced LNG flows from Qatar and the UAE by more than 300 million cubic metres per day, equivalent to over two billion cubic metres per week. The Ras Laffan complex, the world's largest liquefaction facility, remains reportedly offline following a strike in early March. These developments underline Iran's ability to generate significant economic effects through limited physical actions and sustained threat signalling, even without continuous kinetic escalation.

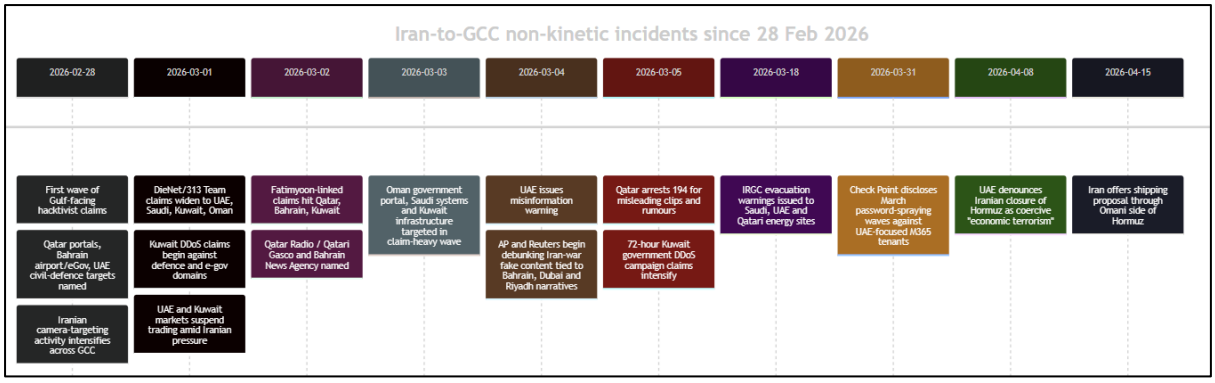
Maritime and logistics pressure around Hormuz and, potentially, the Red Sea has driven up shipping insurance premiums and routing costs. In several cases, the perception of threat against vessels has been enough to disrupt shipping schedules and supply chains. Within the GCC, financial markets have experienced sharp but short-lived episodes of stress. UAE equity exchanges closed temporarily around the start of the missile campaign. Regional indices have fluctuated with escalation cycles, often reacting to news of failed negotiations, new attacks or maritime incidents. Markets in Dubai, Abu Dhabi and Qatar have shown unstable but not catastrophic performance, while oil-linked equities in Saudi Arabia have benefited from higher price expectations. Major financial institutions, including large global banks, have downgraded non-oil growth expectations for some GCC economies, particularly the UAE and Bahrain, where diversification strategies depend heavily on financial services, tourism and foreign investment.

At this stage, the economic impact is best described as managed volatility rather than crisis. However, the pattern is consistent with Iran's broader strategy of non-kinetic warfare: Tehran is demonstrating that it can raise the cost of close alignment with the United States and Israel, and that hosting Western military and financial presence carries tangible economic and political risks. Energy exporters such as Qatar, the UAE and Saudi Arabia, and financial hubs such as the UAE and Bahrain, are the most exposed within the GCC. European and Asian energy importers bear secondary costs, which increases their incentive to press for de-escalation on terms that take Iranian leverage into account.

5. INTEGRATED ASSESSMENT AND OUTLOOK

Iran's non-kinetic campaign in the Gulf has now matured into a coherent three-domain pressure system. Cyber operations distract defenders, probe networks, signal capability and, in selected cases, seek persistent access. Information operations amplify fear, confusion and mistrust, particularly during key incidents. Economic levers exploit both the real and perceived vulnerabilities of the regional energy and financial architecture. These activities complement kinetic operations but can also substitute for them, allowing Tehran to maintain a degree of escalation and coercion below the threshold of open war, and to continue imposing costs even if missile and drone attacks diminish.

In the short to medium term, the intensity and focus of non-kinetic activity will track the overall trajectory of the conflict. Renewed or failed negotiations, major kinetic events and public statements of alignment against Iran by GCC governments are likely to trigger spikes in cyber activity, information campaigns and market volatility. The most serious escalation pathway involves a shift from predominantly nuisance-level and signalling operations to genuinely disruptive attacks on OT and control systems supporting energy processing, power generation and desalination. Such attacks would have higher strategic impact within GCC states and could drive more severe global market responses.



If the conflict de-escalates, non-kinetic activity is likely to fall back to a lower tempo but will not disappear. Tehran has a clear interest in retaining pre-positioned access in key networks, maintaining an information operations infrastructure that can be activated quickly, and leveraging the memory of recent shocks to influence future negotiations. The Gulf will therefore remain exposed to a layered, non-kinetic threat environment even in periods of relative calm.

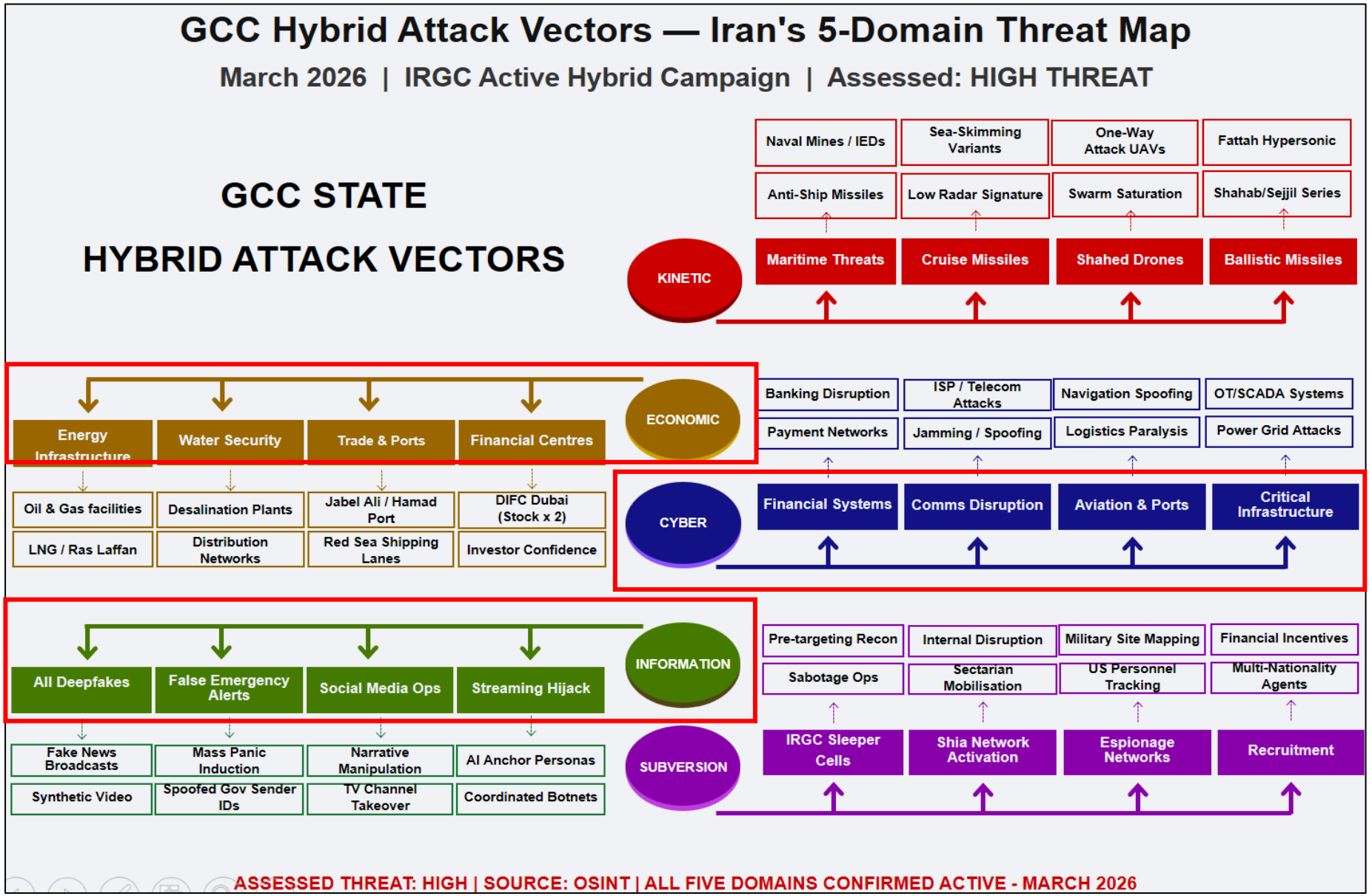
6. KEY WATCH POINTS

There are important gaps in current visibility. Verification of critical infrastructure breaches remains limited; many claims of successful OT compromise or large-scale data destruction are hard to validate and may be overstated. Granular data on the behavioural impact of cyber incidents and information operations on GCC nationals

and expatriate communities is still scarce, making it difficult to judge whether responses are temporary reactions or the start of more enduring shifts in confidence and capital. Finally, the extent and durability of Iranian-linked access in GCC government and critical infrastructure networks is not fully known. These uncertainties will shape both the risk of sudden escalation and the options available to GCC states and their partners as they seek to manage the non-kinetic threat.

Iran's campaign against the GCC is a pre-planned, five-domain hybrid operation and not a reactive strike. The evidence is clear: espionage cells were in place before the first missile was launched; cyberattacks and disinformation were timed to coincide with kinetic strikes; economic targets were chosen to maximise global pressure. All three analytical hypotheses in this report: escalation dominance, deterrence by punishment, and preparation for a sustained guerrilla campaign, are assessed as operating simultaneously. Even if a ceasefire is reached, the underlying threat is not likely to stop. Subversion networks remain in place, cyber implants stay pre-positioned, and information operations continue. The hybrid threat to GCC states is assessed as HIGH and likely to persist through 2026 and beyond.

ANNEX A - GCC Attack Vectors — Comprehensive Map (Non-Kinetic Red Boxed)



ANNEX B - GCC Hybrid Non-Kinetic Attacks during Operation Epic Fury April 2026

Gulf Cooperation Council (GCC) Non-Kinetic Hybrid attacks 28 Feb – 15 April 2026

Cyber: Kuwait absorbed one of the densest waves of claim-led DDoS pressure against defence and public-sector websites, while Iranian-linked actors also targeted IP cameras; the publicly visible effect looks mostly nuisance-level rather than a proven deep breach (medium overall; low for many DDoS claims).

IO / Economic: Kuwait-specific Iranian narrative activity was less distinct in open reporting than the cyber and market picture, but economic coercion was clear when KPC declared force majeure and cut output citing Iranian threats to Hormuz and attacks on Kuwait (IO low; economic high).

Cyber: Bahrain faced claim-heavy disruptive pressure against the airport and eGovernment estate, alongside Iranian-linked IP-camera targeting, but again with limited public proof of deep compromise (medium overall; low for many DDoS claims).

IO / Economic: AP documented AI-generated strike exaggeration around a Bahraini high-rise amplified by accounts associated with the Iranian government, while Hormuz disruption forced Alba to shut 19% of aluminium capacity (IO medium; economic high).

Cyber: Saudi banks and some government systems featured in claim-led hacktivist disruption, while Check Point also saw limited Saudi involvement in an Iran-nexus M365 password-spraying campaign, suggesting reconnaissance and access-building more than proven destructive compromise (medium overall; low for many public DDoS claims).

IO / Economic: Reuters debunked AI-generated Riyadh strike imagery, and IRGC evacuation warnings to Samref and Jubail showed clear coercive pressure on the Saudi energy base (IO medium; economic high).

Cyber: Qatar saw claim-heavy disruptive pressure against core government portals and Iranian-linked IP-camera targeting, but little public evidence of deep or lasting compromise (medium overall; low for many DDoS claims).

IO / Economic: The information environment was noisy, with AFP debunking AI imagery around Al Udeid and Qatari authorities arresting 194 people over misleading clips and rumours, while IRGC warnings to Mesaieed and Ras Laffan represented direct energy coercion (IO medium; economic high).

Cyber: Iranian-linked activity combined IP-camera targeting from 28 February with a March Microsoft 365 password-spraying campaign affecting 25+ UAE organisations, while many concurrent proxy-hacktivist DDoS claims against public-facing services remained claim-led rather than confirmed (medium overall; low for many DDoS claims).

IO / Economic: UAE authorities publicly warned against AI-generated and recycled strike footage, and IRGC evacuation warnings to Al Hosn alongside wider Hormuz disruption put direct pressure on UAE energy and maritime flows (IO medium; economic high)

Cyber: Oman saw only low-confidence, claim-led disruptive pressure against the government portal and no clearly attributable destructive Iranian cyber incident in the reviewed open sources (low).

IO / Economic: Oman-specific Iranian IO was sparse in public reporting, but Musandam/Hormuz geography left Oman directly exposed to Iranian shipping coercion, including Tehran's proposal to allow safe passage only on the Omani side of the strait (IO low; economic high).

ASSESSMENT: If the ceasefire weakens or diplomacy fails, a renewed wave of DDoS, portal disruption, credential-access attempts and synthetic-media narratives against the UAE, Saudi Arabia, Qatar and Kuwait is more likely than not, around 70%. The most probable targets are public-sector login estates, visible government portals, finance, aviation, telecoms and energy-adjacent information systems, because those were the repeated target classes in the period reviewed. A large, publicly attributable wiper or OT/ICS sabotage event in a GCC state remains possible but not the base case, around 25%–35%. Iran and Iran-linked actors have the historical capability, and vendors continue to warn about wiper risk and ICS-themed targeting, but the evidence in this period shows more reconnaissance, claim-amplification and burden-shifting than proven destructive execution inside GCC networks.

EIGENRAC