EIGENRAC

US/Israel-Iran War

Hybrid Warfare: GCC Threat Assessment March 2026

25-03-2026

EIGENRAC MANAGEMENT FZ-LLC

1. EXECUTIVE SUMMARY

This report examines hybrid warfare as it is being actively used against Gulf Cooperation Council (GCC) states right now. It explains what hybrid warfare is, how Iran operates it, and what that means for the security of people and organisations living and working across the Gulf region in 2026.

Hybrid warfare is not a single type of attack. It is the deliberate combination of missiles and UAVs, cyber operations, disinformation, economic disruption, and covert subversion, all used together and timed to amplify each other's effect. What makes it so dangerous is that no single domain tells the full story. A missile strike is made worse by simultaneous cyberattacks that blind emergency services. Disinformation campaigns turn every explosion into a psychological weapon. Sleeper cells map targets before the first shot is fired. The result is a threat that is greater than the sum of its parts.

Iran has built this capability over four decades. Its network of armed proxy groups: Hezbollah in Lebanon, Hamas in Gaza, the Houthis in Yemen, and Iraqi militias, gives the ability to strike multiple adversaries across a wide geography while maintaining plausible deniability.

Since 28 February 2026, following US-Israeli strikes on Iran, the GCC has become a direct battleground. Iran has fired thousands of Unmanned Air Vehicles (UAVs) and ballistic missiles across the six member states, struck oil refineries, financial centres, airports, desalination plants, and residential areas, and activated pre-positioned intelligence cells inside Qatar and other Gulf states. The UAE alone absorbed 314 ballistic missiles and 1,672 drone attacks in under three weeks. Saudi Arabia's Eastern Province oilfields, Qatar's Ras Laffan LNG facility, Bahrain's Bapco refinery, and Kuwait's power infrastructure have all been hit. Dubai's financial district was struck multiple times. Every GCC airport was targeted.

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.

2. HYBRID WARFARE

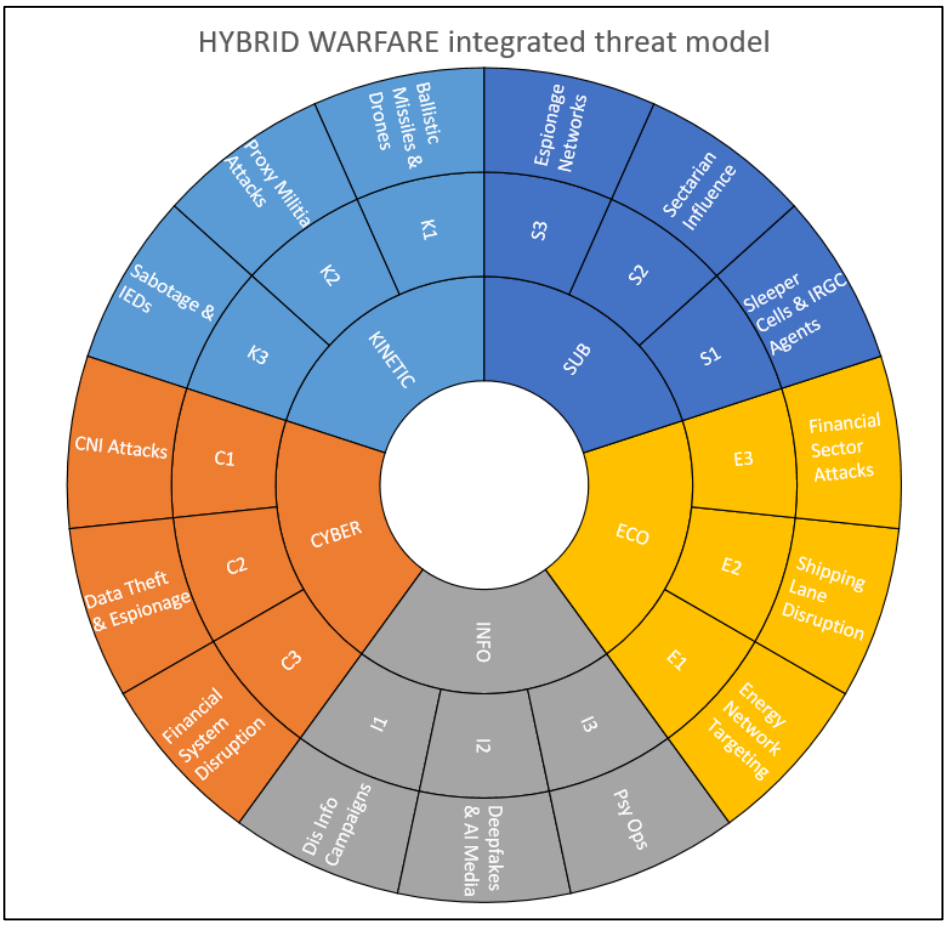
Definition and Origins of Hybrid Warfare

Hybrid warfare describes the deliberate, coordinated use of military and non-military tools to achieve strategic objectives while remaining below the threshold of formal declared war — exploiting the ambiguity of the "grey zone" between peace and open conflict. It is defined as the simultaneous use of regular arms, irregular tactics, terrorism, and criminal practices. All coordinated to create compounding, multi level effects on the adversary.

NATO formally recognised hybrid threats at its 2016 Warsaw Summit, concluding that Article 5 (the mutual defence clause), could be triggered by a hybrid attack. The US Army's doctrine (TC 7-100) defines hybrid threats as "a dynamic combination of regular and irregular forces, along with criminal elements, working together for mutual benefit," extending the concept to encompass political, social, and non-kinetic instruments.

The Five Domains of Hybrid Warfare

Hybrid warfare operates simultaneously across five interconnected domains. The power of this approach lies not in any single domain but in the **coordinated, timed application** of all five, each amplifying the effect of the others. The HYBRID WARFARE integrated threat model consists of KINETIC (Conventional & Irregular), CYBER (Digital Operations), INFORMATION (Psychological & Narrative), ECONOMIC (Coercion & Disruption), and SUBVERSION (Proxy & Covert Action).



How Hybrid Warfare is Operationalised

The enemy operationalises hybrid warfare through a sequenced and layered approach. In the pre-conflict phase, subversive and cyber elements are pre-positioned: sleeper cells map targets, cyber actors pre-plant malware in critical systems, and information operations seed disinformation narratives. As tensions escalate, economic pressure is applied, disrupting trade routes and energy exports. When the threshold for kinetic action is reached, all domains are triggered simultaneously: missiles strike infrastructure, cyber operations blind communications, and information campaigns flood social media to maximise confusion.

Domain	Primary Tools	Strategic Objective
Kinetic	UAVs, missiles, proxy fighters, IEDs	Physical destruction; stretch defences; impose costs
Cyber	Malware, DDoS, ICS disruption, data wipe	Paralyse infrastructure; blind command systems
Information	Deepfakes, bots, fake alerts, propaganda	Erode public trust; generate panic; shape narrative
Economic	Energy attacks, port disruption, financial targeting	Impose economic pain; signal escalation capability
Subversion	Sleeper cells, espionage, sectarian networks	Internal disruption; pre-targeting; plausible deniability

The critical distinguishing feature of hybrid warfare is ***plausible deniability***. As we see, the aggressor maintains sufficient ambiguity so that the target state cannot justify a symmetric military response without appearing to be the aggressor. Proxy forces and hacktivist groups serve as the deniability layer, while state intelligence directs operations from a distance.

The Iran–Israel Hybrid War: Key Attack Vectors in operations

The Iran–Israel confrontation represents one of the most comprehensively documented examples of hybrid warfare. Across every domain, both actors have deployed sophisticated, timed, coordinated operations:

- **Cyber Domain:** In June 2025, concurrent with Israeli airstrikes on Iranian nuclear facilities, Israeli-linked group *Predatory Sparrow* destroyed data at Iran's state-owned Bank Sepah and disrupted financial infrastructure in coordinated, strategically timed cyber operations. Iran responded by deploying social media botnets, AI-generated deepfakes, and spoofed emergency text messages to Israeli civilians. Fake alerts warning of imminent terrorist bombings, sent to appear from Israel's own Home Front Command and

designed to create panic. Iran's cyber operations expanded over 700% following the mid-2025 conflict, according to cybersecurity assessments[1].

- **Information Domain:** Iranian operatives, many linked to IRGC psychological operations (PsyOps) units created legions of fictitious social media personas complete with AI-generated profile photos to push coordinated narratives[2]. In the February 2026 escalation, doctored images and synthetic video flooded platforms faster than fact-checkers could respond.

- **Kinetic Domain:** Israel's February 2026 "Operation Roar of the Lion" was paired with the largest known cyberattack in history against Iran[3], reducing Iranian internet connectivity to approximately 4% of normal capacity, blinding IRGC command networks and disrupting coordination of retaliatory missile strikes. This represents the clearest example yet of cyber operations as a force multiplier for kinetic campaigns — collapsing the enemy's command, control, and communications infrastructure in concert with physical strikes.

- **Economic Domain**: Direct targeting of Israeli ports (Haifa, Ashdod), offshore gas platforms (Tamar, Leviathan), and broader cost imposition through sustained conflict — estimated 10–15% of GDP growth foregone. Iran's illicit finance engine, the IRGC's Sepehr Energy Jahan shadow fleet of 180+ sanctioned tankers, oil blending operations through UAE intermediaries, and Mahan Air subsidiaries ferrying Quds Force officers to Hezbollah. A December 2025 WikiIran data leak fully exposed this network.

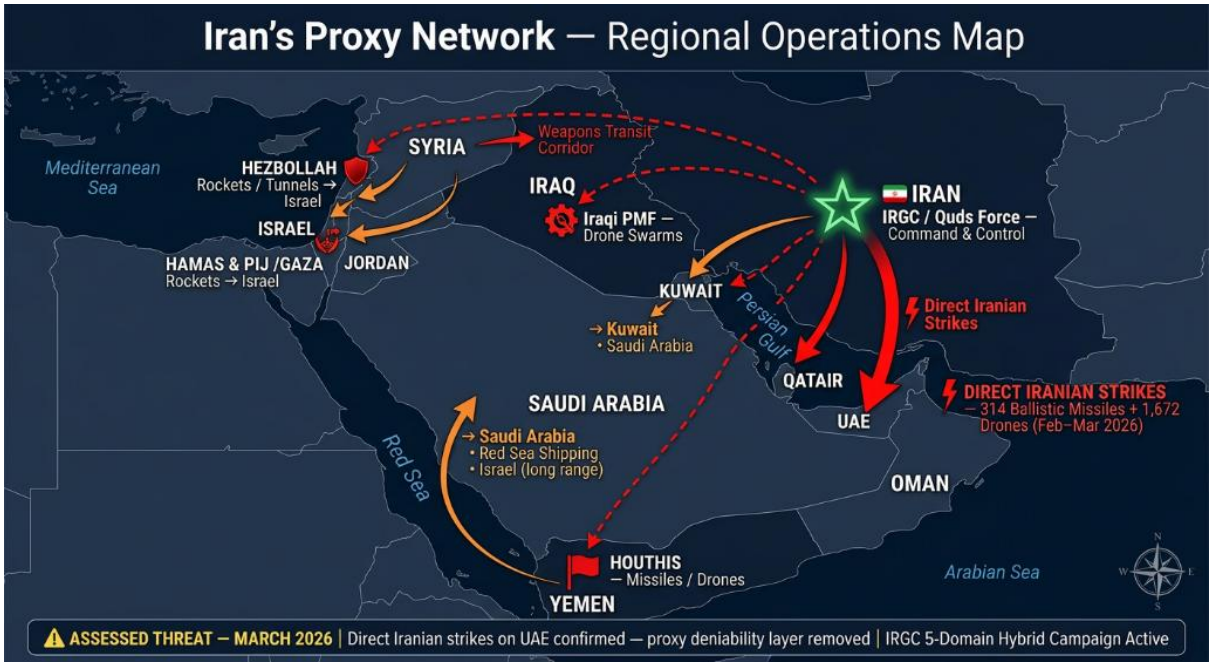
- **Subversion Domain**: Pre-positioned assassination networks globally with 20+ Iran-backed plots disrupted in the UK alone in a single year, including an Israeli Embassy attack plot. Internal purges inside Iran confirming sustained Israeli HUMINT penetration — two agents executed in 2025 for providing intelligence to Israel. Hezbollah as the primary intelligence-collection arm against Israel use tunnel networks doubling as surveillance infrastructure, with the IDF confirming coordinated Hezbollah distraction operations designed to split Israeli defensive focus in March 2026.

[1] https://trendsresearch.org/insight/ai-and-the-evolution-of-asymmetric-cyber-warfare-insights-from-the-2025-israel-iran-conflict/
[2] https://www.mitsloanme.com/article/how-the-current-conflict-is-accelerating-ai-powered-information-warfare/
[3] https://www.jpost.com/israel-news/defense-news/article-888271

3. IRAN'S HYBRID WARFARE MODEL — ARCHITECTURE AND DOCTRINE

The Proxy Network as the Foundation[4]

Iran's hybrid warfare architecture is built on four decades of investment in non-state proxy organisations that combine political, paramilitary, and social functions. The formation of Lebanese Hezbollah in 1982 served as the prototype: Iran would build organisations with deep roots in local communities, providing military training, weapons, and financing while maintaining operational direction through the IRGC Quds Force. This model was subsequently replicated across the region with **Hamas and Palestinian Islamic Jihad** in Gaza, the **Houthis** (Ansar Allah) in Yemen, the **Popular Mobilisation Forces** (PMF) in Iraq, and various Syrian-based networks.



Proxies provide Iran with strategic depth, the ability to project power and impose costs on adversaries far from Iranian territory, without the risks of direct military confrontation or international attribution.

As the Middle East Forum has documented[5], this approach compensates for Iran's conventional military limitations while creating multiple simultaneous pressure fronts that stretch adversary defences.

---

4 **Red proxy nodes** in Lebanon (Hezbollah), Gaza (Hamas/PIJ), Yemen (Houthis), and Iraq (PMF / Kataib Hezbollah), each with their primary attack methods annotated. **Orange attack vectors** showing the direction of threat projection — northward toward Israel, northeast toward the GCC states, and into the Red Sea corridor.

5 https://pdfs.semanticscholar.org/706f/2338d6d895c5a9acfccb429fec1250990d99.pdf

4. THE HYBRID THREAT TO GCC NATIONS — 2026 ASSESSMENT

From Proxy Shadow to Direct Strike

The GCC's exposure to Iran's hybrid warfare has undergone a real shift in 2026. What was previously a campaign of indirect pressure such as the Houthi Red Sea attacks disrupting shipping lanes, cyber probing of energy infrastructure, and covert espionage networks, has escalated into direct, large-scale kinetic and non-kinetic assault across all six GCC member states. At **ANNEX A** is a plan of Iran's GCC attack vectors .

On 28 February 2026, following US-Israeli strikes on Iran, Tehran launched coordinated missile and drone attacks across the Gulf. By 17 March, Iran had fired 314 ballistic missiles, 1,672 drone attacks, and 15 cruise missiles at the UAE alone. By 21 March, Saudi Arabia had recorded 575 drone and 49 missile strikes since February 28. Qatar, Kuwait, and Bahrain all reported sustained aerial attacks targeting airports, military installations, and energy infrastructure. Concurrent with the missile campaign, Qatar announced the arrest of two IRGC-linked espionage cells[6] and 10 individuals assigned to spy on vital facilities and conduct sabotage operations. At **ANNEX B** – is map of GCC Hybrid Attacks during Operation Epic Fury March 2026.

Target Category	Specific Examples	Strategic Rationale
Energy Infrastructure	Saudi Eastern Province oilfields, Kuwait Mina Al-Ahmadi refinery, Qatar Ras Laffan LNG complex	Attack global energy supply; impose economic pain on GCC and international community
Financial Centres	Dubai International Financial Centre (struck twice)	Signal capability to paralyse Gulf economic hub; undermine investor confidence
Ports & Logistics	Jebel Ali (UAE's busiest port), UAE ports (evacuation warnings issued)	Disrupt global trade; demonstrate reach into economic lifeblood
Desalination Plants	UAE and Saudi water infrastructure	Existential civilian pressure — water is non-substitutable
Military & US Bases	Al Dhafra (UAE), Prince Sultan (Saudi), Al Udeid (Qatar)	Degrade US/GCC air defence response; demonstrate deterrence
Aviation	Hamad International Airport (Qatar), Dubai International, Abu Dhabi Zayed Airport	Disrupt evacuation; paralyse economic activity; generate civilian panic
Residential/Civilian	Palm Jumeirah (Dubai), Corniche (Abu Dhabi)	Psychological impact; population displacement; undermine regime confidence

The Internal Threat: IRGC Subversion Networks

Investigations across multiple GCC states have uncovered clandestine IRGC networks pre-positioned before the kinetic campaign began. These networks comprise

[6] https://www.thenationalnews.com/news/gulf/2026/03/04/qatar-says-irans-irgc-sleeper-cells-arrested/

individuals from diverse nationalities (including Arab, South Asian, and Shia Gulf residents) recruited through ideological and financial incentives. Their reported activities include:

- Photographing coordinates of military installations, oil refineries, and critical infrastructure.
- Filming and distributing near-real-time footage of Iranian drone and missile strikes before official announcements thus providing Iran with battle damage assessment and psychological warfare content simultaneously.
- Providing location data on US military community residential clusters in Qatar, the UAE, and Kuwait.
- Conducting pre-operational surveillance of designated bombing targets.

The GCC laws governing espionage during wartime prescribe capital punishment, and concurrent prosecutions are underway across multiple states. The disclosure of these networks confirms that the kinetic campaign was preceded by months, if not years of subversive pre-positioning, the hallmark of sophisticated hybrid warfare doctrine.

Why GCC States Face a Distinctive Vulnerability

GCC states face a combination of structural factors that amplify their exposure to hybrid threats:

- **High dependence on critical infrastructure:** Desalination plants supply most drinking water; LNG and oil facilities are essential to both national revenue and global energy markets. These are high-value, hard-to-defend targets.
- **Large expatriate populations:** The majority of residents in UAE, Qatar, Kuwait, and Bahrain are expatriates. A population that is highly mobile, diverse in nationality, and susceptible to information operations and panic-induced departures.
- **Air defence attrition:** Missile defence systems have performed effectively against ballistic threats and UAVs. However sustained attacks deplete stocks at the cost of expensive interceptors compared to cheap Shahed UAVs.
- **Geopolitical exposure**: GCC states host US military installations that make them implicit participants in the Iran-US confrontation, regardless of their own declared neutrality.
- **Demographic imbalance and internal fault lines:** Iran has historically exploited Shia communities and ideological sympathisers within GCC states for subversion and intelligence collection.

5. ASSESSED THREAT LEVEL AND HYPOTHESIS - GCC REGION

Iran has conducted thousands of drone and missile strikes against GCC states since February 28, 2026, with energy infrastructure, financial centres, airports, desalination plants, and civilian areas all confirmed as targets. IRGC espionage cells have been dismantled in Qatar, with concurrent investigations ongoing in Bahrain, UAE, Saudi Arabia, and Kuwait. Three hypotheses explain Iran's current hybrid posture:

- **Hypothesis 1 — Escalation Dominance (STEMPLES[7]: Military, Economic):** Iran is demonstrating that it can impose unacceptable costs on GCC states hosting US forces, seeking to coerce them into pressuring Washington to halt operations. The coordinated targeting of energy and financial infrastructure signals economic warfare as the primary lever.

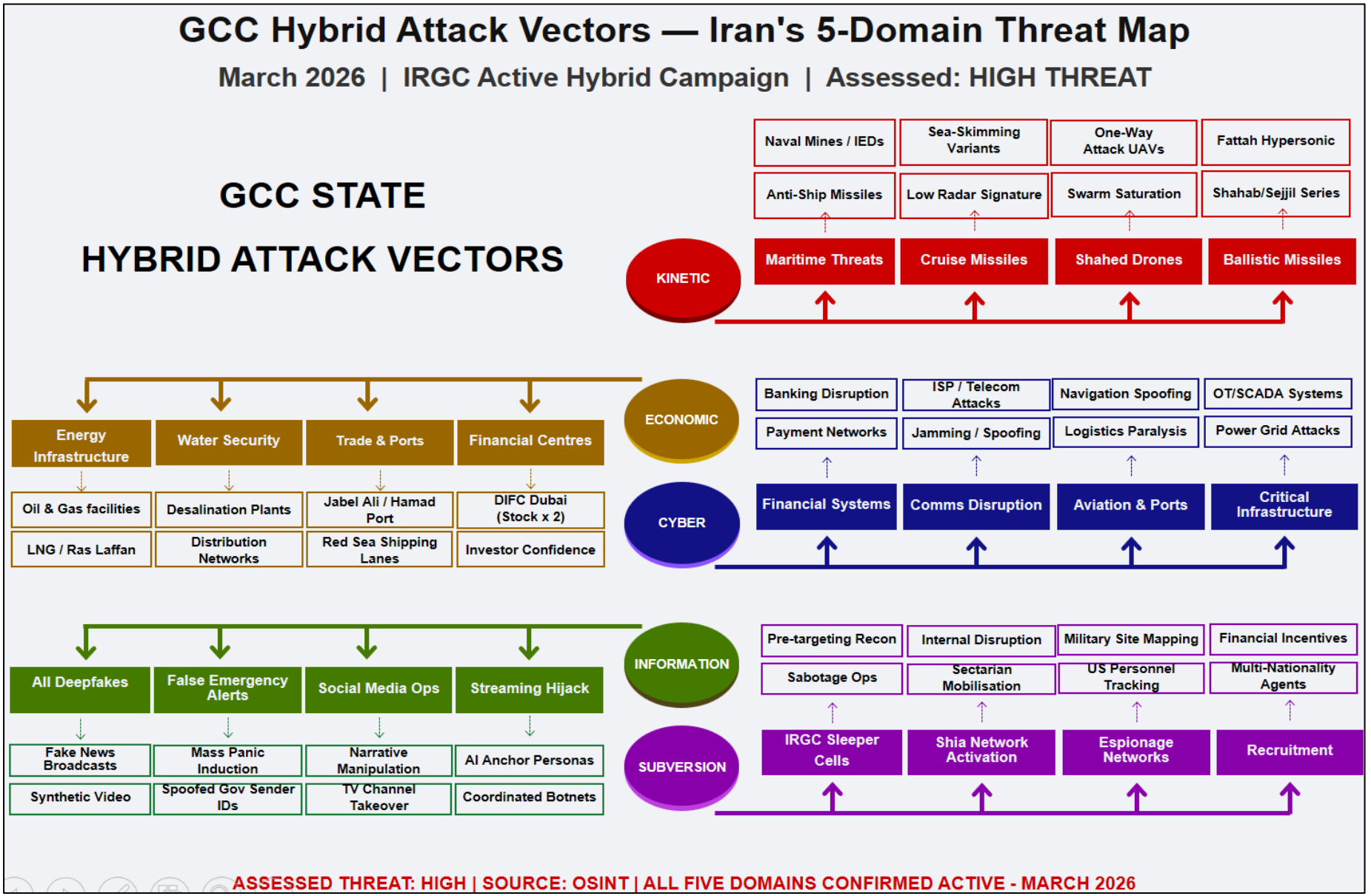
- **Hypothesis 2 — Deterrence by Punishment (STEMPLES: Political, Military):** With its proxy network degraded and direct military confrontation ongoing, Iran is signalling to GCC governments that continued logistical support for US operations carries sovereign risk. An attempt to fracture the US-GCC security architecture through cost imposition rather than military victory.

- **Hypothesis 3 — Preparation for Sustained Guerrilla Campaign (STEMPLES: Social, Technical, Economic):** The activation of internal subversion networks (sleeper cells, sectarian mobilisation) alongside kinetic strikes suggests Iran may be building the conditions for a protracted, multi-domain campaign that transitions from conventional missile attacks to internal sabotage once ballistic missile stocks are depleted.

ASSESSMENT: All three hypotheses are compatible and highly likely operating simultaneously. The most significant indicator is the confirmed activation of IRGC internal networks *before* the kinetic campaign began. This is likely a pre-planned, multi-domain operation, not a reactive strike. The hybrid threat will almost certainly persist beyond any ceasefire. Subversion networks, pre-positioned cyber implants, and information operations infrastructure will highly likely remain active. GCC civilians face an elevated, multi-vector threat environment that is assessed as **likely to persist through 2026** even if kinetic hostilities pause.

[7] Socio, Technological, Economic, Military, Political, Legal, Environmental, Security

ANNEX A - GCC Attack Vectors — Comprehensive Map

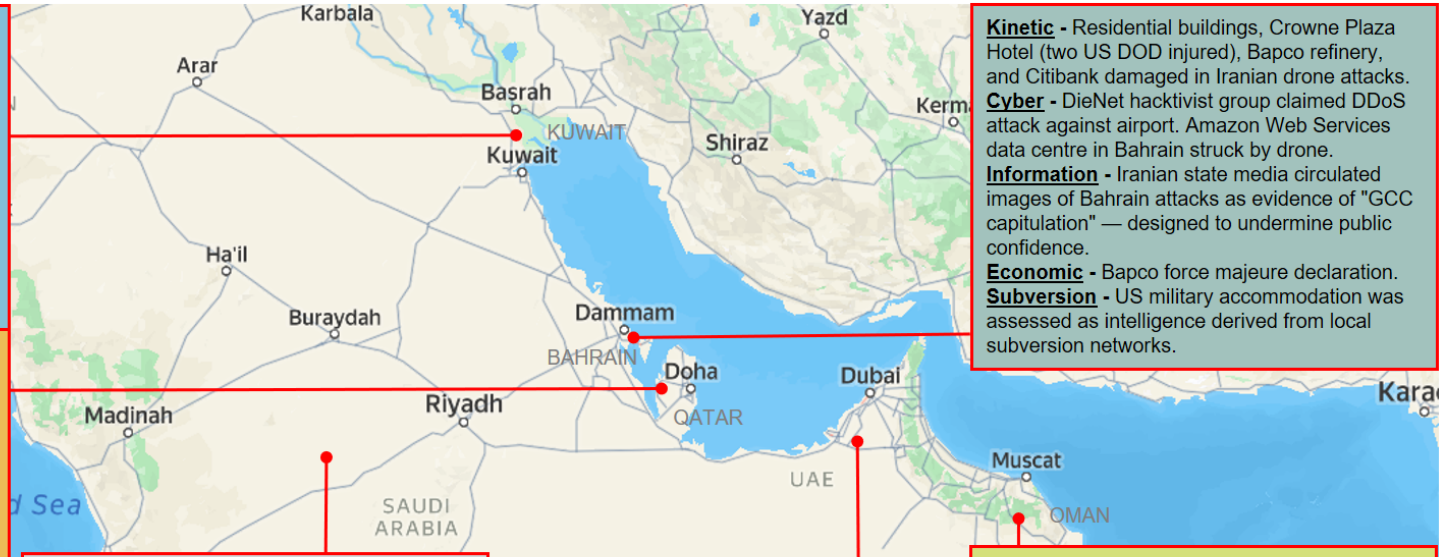


ANNEX B - GCC Hybrid Attacks during Operation Epic Fury March 2026

Gulf Cooperation Council (GCC) Hybrid attacks 28 Feb – 24 March 2026

Kinetic - International Airport; Subiya Power Station; Residential buildings, fire damage caused by drone debris.
Cyber - 313 Team hacktivist collective (pro-Iranian) DDoS and disruption against banks.
Information - Iranian information operations amplified the suspension of Kuwait Stock Exchange as economic collapse.
Economic - Subiya Power Station fire created electricity supply concerns.
Subversion - Shia networks in Kuwait assessed as active by regional security services

Kinetic - Ballistic missiles and drones; Al Udeid Air Base, food storage warehouse, Ras Laffan LNG complex, Hamad International Airport, Qatar Navigation tankers and LNG shipping.
Cyber - AI-manipulated satellite image falsely claiming complete destruction of a US radar at Al-Udeid Air Base. CloudSEK logged DDoS against Qatari financial institutions and QatarEnergy digital infrastructure.
Information - Iranian state media disinformation campaign targeting Al-Udeid, false satellite image was shared via IRGC Telegram channels and reached regional mainstream media.
Economic - Qatar Stock Exchange (QSE) benchmark index dropped 4.3%. Qatar Navigation fell 5.6%; Qatar Gas Transport retreated 6.7%. Ras Laffan production halted.
Subversion - Arrest of 10 IRGC-linked operatives assigned to intelligence collection on military infrastructures, and drone operations for sabotage. Assessed as pre-positioned before 28 February strikes.



Kinetic - Missiles and drone strikes targeting Riyadh and the Eastern Province. Ras Tanura oil facility targeted.
Cyber - Pro-Iranian hacktivist group DieNet DDoS attacks on Riyadh Bank and Sharjah Airport.
Information - IRGC-linked Tasnim claimed 650 US troops killed in the Gulf — Saudi and regional media struggled to counter the false claims.
Economic - Saudi TASI index experienced sustained sell-off; foreign capital exited petrochemical, banking and real estate sectors.
Subversion - Shia community networks within the Eastern Province active intelligence-sharing.

Kinetic - Highest Iranian ballistic missile and drone campaign. Airports, Ruwais refinery, DIFC and Fujairah Port targeted.
Cyber - UAE reported over 1,000 cyberattacks from Iran. DieNet hacktivist group DDoS attack.
Information - Hundreds of AI-generated and manipulated posts circulated on X within minutes of each missile strike.
Economic - UAE suspended stock exchange trading (Abu Dhabi Securities Exchange and Dubai Financial Market).
Subversion - IRGC-linked individuals confirmed filming and distributing near-real-time footage.

Kinetic - Residential buildings, Crowne Plaza Hotel (two US DOD injured), Bapco refinery, and Citibank damaged in Iranian drone attacks.
Cyber - DieNet hacktivist group claimed DDoS attack against airport. Amazon Web Services data centre in Bahrain struck by drone.
Information - Iranian state media circulated images of Bahrain attacks as evidence of "GCC capitulation" — designed to undermine public confidence.
Economic - Bapco force majeure declaration.
Subversion - US military accommodation was assessed as intelligence derived from local subversion networks.

Kinetic - Drones recorded targeting Oman through the least-affected GCC state. Fuel tank struck at Salalah.
Information - Iranian messaging framed Oman strikes as "spillover" — consistent with Iran's interest in preserving Oman as a diplomatic channel.
Economic - Strait of Hormuz security concerns (Iran's mine threats) directly threaten Oman's Port of Salalah transshipment business and fishing industry.
Subversion - Iranian and US messaging sought to exploit Oman's neutral position as a pressure point on both sides.

US-Israeli "Operation Epic Fury / Roaring Lion" strikes on Iran on 28 February 2026, Iran launched a multi-domain retaliatory campaign across all six GCC states. The first time Iran has conducted direct, sustained kinetic attacks against Gulf sovereign territory at scale. As of 23 March, Iran had launched thousands of drones and ballistic missiles against GCC states, with the largest concentration targeting the UAE. Concurrent cyber, information, subversion, and economic operations confirm this as a fully operational five-domain hybrid campaign.

EIGENRAC