Sleeper Cells: How the Shape of Threats in the Gulf Is Changing

The U.S.-Israeli war on Iran is no longer viewed in the Gulf solely as an external front. Alongside missiles and drones that have pushed Gulf capitals to heighten their alert levels, another trajectory emerged in March one that threatens these states from within.

Several Gulf countries revealed Iranian surveillance groups, financing networks, recruitment attempts, assassination plots, and operations involving the transfer of images and data on sensitive facilities. The question of security has thus shifted from drones to sleeper cells.

What Was Actually Uncovered?

In March alone, four Gulf states announced the dismantling of networks linked to Iran’s Islamic Revolutionary Guard Corps (IRGC) and its ally Hezbollah:

Qatar: Espionage and Drone Sabotage Cells

On March 3, 2026, the Qatar News Agency (QNA) announced the arrest of two cells linked to the IRGC. The first was tasked with gathering intelligence on vital and military facilities inside Qatar, while the second was assigned to carry out sabotage operations using drones.

According to the agency, ten suspects were arrested seven involved in surveillance and three trained in drone operations. Investigations revealed communication devices, sensitive data, and coordination materials in their possession. The suspects reportedly confessed to their ties with the IRGC and to being assigned espionage and sabotage missions.

United Arab Emirates: A Money Laundering Network Under Commercial Cover

On March 20, the Emirates News Agency (WAM) announced the dismantling of a "terrorist" network funded by Iran and Hezbollah, operating in the UAE under the guise of a fictitious commercial entity.

The statement confirmed the network had conducted money laundering operations and financed terrorism, aiming to undermine national security and financial stability by infiltrating the economy.

No details were disclosed regarding the number or nationalities of those arrested. Lebanon's Foreign Ministry condemned what it described as a "terrorist conspiracy" and offered cooperation with Abu Dhabi, while Hezbollah denied any presence or activity in the UAE.

Kuwait: Assassination Plot and Multiple Networks

On March 25, Kuwait's Ministry of Interior announced it had foiled a plot to assassinate state leaders. The State Security apparatus arrested a six-member cell five Kuwaiti citizens and one individual whose citizenship had been revoked following extensive surveillance.

Kuwait announced the arrest of three cells during March, which it said were linked to Iran and Hezbollah.

Authorities also identified 14 additional suspects abroad, including Kuwaitis, Lebanese, and Iranians. Investigations revealed links to Hezbollah and plans targeting "state symbols," alongside efforts to recruit new members. The suspects had reportedly received advanced military training abroad.

This was not the first such case since the outbreak of war with Iran. On March 16, Kuwaiti security forces dismantled a Hezbollah-linked cell of 14 Kuwaitis and two Lebanese nationals. On March 18, ten individuals were arrested for coordinating with foreign entities to provide information on sensitive sites.

Bahrain: Espionage, Financing, and Operational Planning

On March 26, Bahrain's Public Prosecutor referred 14 defendants including one woman in four separate cases to the High Criminal Court. Some of the accused had fled to Iran.

Charges included coordinating with the IRGC to carry out hostile operations

within Bahrain, providing financial support, and transferring funds for such activities.

The charges also encompassed leaking classified information, spreading rumors to incite panic, and photographing sensitive locations to send to Iranian operatives, who allegedly used them to target facilities within the kingdom.

The Public Prosecutor stated that some defendants had received military training in IRGC camps, and that evidence included confessions, witness testimonies, and forensic analysis of electronic devices.

What Are the Patterns of Iranian Threats?

1. From Proxy Networks to Asymmetric Tools

These developments are part of a broader hybrid war that extends beyond conventional military confrontation. For years, Tehran has relied on regional allies and proxies to deter its adversaries, successfully expanding its influence across Baghdad, Damascus, Beirut, and Sana'a.

An analysis by Chatham House on Iran's "forward defense" strategy suggests that heavy reliance on proxies has made these networks vulnerable under mounting pressure, as they now face a comprehensive assault by the United States and Israel.

This context helps explain why Tehran may turn to asymmetric tools such as espionage and covert financing to preserve its deterrence capabilities after sustaining direct military blows.

The Middle East Council on Global Affairs argues that the current war has pushed Iran toward a hybrid model combining aerial missile strikes with cyber, economic, and media tools.

It warns that a prolonged conflict could see Iran escalate cyberattacks against banks, energy firms, and government networks, alongside increased use of disinformation and economic sabotage.

The Center for Strategic and International Studies (CSIS) goes further, describing Iran's strategy as a "multi-domain punitive campaign," noting: "Tehran recognizes it faces militarily superior forces and thus expands the battlefield horizontally by threatening civilian and economic systems in neighboring states."

This campaign includes missiles, cyberattacks, and disinformation aimed at paralyzing ports, refineries, desalination plants, data centers, and financial institutions.

2. Sleeper Cells as an Activatable Tool

Concerns about sleeper cells are not mere media exaggeration. According to an

analysis by the Washington Institute for Near East Policy, U.S. investigations have thwarted 17 Iran-linked plots over the past five years.

One of the most prominent cases involved Ali Kourani, a Hezbollah operative sentenced in New York in 2019, who described himself as a sleeper agent tasked with collecting intelligence on targets in the United States and Canada.

The worst-case scenario would be the activation of dormant Iranian cells in the Gulf and the outbreak of a war on two fronts, internal and external.

Kourani stated that orders to act would come if war broke out between the United States and Iran suggesting Tehran maintains a global network of sleeper cells that can be activated when needed.

Another report by the institute notes that the killing of Iranian leadership figures prompted the Quds Force to warn that its enemies “will not be safe anywhere.” Iran-linked plots have since surfaced in Azerbaijan, Kuwait, Qatar, the UAE, and the United Kingdom, raising concerns in Washington about potential activation of cells inside the United States.

The alignment between these warnings and Gulf announcements suggests that developments in Doha, Kuwait City, Abu Dhabi, and Manama are not isolated incidents.

The Guardian cited experts warning that Iran could activate sleeper cells in the Gulf. Security analyst Bilal Saab cautioned that the worst-case scenario would involve a two-front war external and internal.

He noted indications that dormant cells had already begun moving, with arrests reported in Kuwait and the UAE, warning that the crisis could deepen if the war drags on.

3. The Cyber Dimension and Targeting Digital Infrastructure

The cyber dimension is equally critical. A report by the International Institute for Strategic Studies (IISS) highlights the asymmetry in cyber warfare.

While the U.S. and Israel possess advanced capabilities used to disrupt Iranian communications Iran relies on hacker groups and aligned actors to launch distributed denial-of-service (DDoS) attacks, deface websites, and conduct “hack-and-leak” campaigns to destabilize adversaries.

The report points to attempts to access surveillance cameras in the Gulf to guide strikes, warning that gaps in cybersecurity across some Gulf states increase vulnerability to such breaches.

This helps explain the importance of cells gathering images and coordinates on the ground. The threat is not divided between physical surveillance and digital

intrusion; rather, both operate in tandem within a unified logic of hybrid warfare.

How Has the War Changed the Meaning of Gulf Security?

The reports suggest that the war is no longer confined to traditional battlefields. If prolonged, and if Iran continues its hybrid approach, threats will deepen within Gulf societies in several ways:

1. Expanding Internal Risk

The Guardian notes that the greatest fear is a two-front conflict: Gulf states facing missiles and drones externally, while confronting espionage and sabotage cells internally.

Evidence suggests that cells uncovered in Qatar, Kuwait, the UAE, and Bahrain were tasked with providing coordinates to enhance strike precision or to conduct synchronized sabotage operations.

2. Redefining Security Priorities

As CSIS analysis indicates, Iran's strategy increasingly targets infrastructure energy, communications, transport, and banking.

Experts argue that air defense alone is no longer sufficient. Protecting information systems, monitoring suspicious financial flows, and tightening oversight on recruitment and money laundering activities have become essential reflected in recent arrests across the Gulf.

3. Broader Intelligence Crackdown

Chatham House suggests Iran's reliance on proxy networks has backfired, leaving them exposed and vulnerable to dismantling. However, the Middle East Council on Global Affairs warns that the conflict could evolve into a prolonged war of attrition, heightening risks of miscalculation and escalation.

These risks may push Gulf governments to expand human intelligence operations and regional security cooperation to detect any signs of newly activated cells, while also strengthening cyber response systems, as recommended by the IISS.

The Middle East Council outlines three potential trajectories: gradual escalation, unintended escalation due to miscalculation, or a temporary tactical de-escalation.

If the conflict is quickly contained, Iran may maintain only a limited internal threat. But if the war persists, the likelihood of uncovering additional cells will rise intensifying pressure on social cohesion and leaving the Gulf gripped by the constant fear of infiltration.

رابط المقال: https://www.noonpost.com/en/368602/