أحمد الطناني | نشر في 13 March 2026,

The Hidden Architecture of Zero Hour: How Iran Built Its Intelligence Networks in the Gulf

The ongoing war between Iran on one side and the United States and Israel on the other has revealed that the conflict has another, far more concealed and consequential dimension one rooted primarily in the realm of intelligence. The nature of the strikes, the precision of certain targeting operations, and the breadth of their geographic scope all suggest that the current confrontation is, at its core, the product of years of accumulated intelligence work. During that time, each side sought to build a vast target bank and penetrate the security and military structures of its adversary in preparation for the moment of confrontation.

Within this context, battlefield indicators and the pattern of targets struck during the war point to growing evidence of an active Iranian intelligence infrastructure in the region. Over the course of years, this network appears to have focused on gathering information, monitoring bases and vital facilities, and cultivating a diverse web of sources. The result seems to be a multi-layered intelligence system that combines technical surveillance, human networks, and cyber intrusions.

From this perspective, the current war has become a test of intelligence

agencies' ability to transform accumulated information into operational power at the moment of conflict. This raises fundamental questions about the nature of the intelligence architecture Iran has built across its regional environment, and the extent to which it can support military operations and sustain an effective target bank against its adversaries.

A Multi-Centered Intelligence Architecture

To understand the role played by Iranian intelligence in managing wars and constructing target banks against its adversaries, it is necessary to examine the nature of its institutional structure. Iran does not rely on a single centralized intelligence agency. Instead, it operates a multi-agency system whose components function in overlapping ways.

This arrangement gives Tehran a broad capacity to collect information through different channels, though it also creates a degree of competition and ambiguity within the intelligence community itself.

The roots of this system date back to the period before the Islamic Revolution. In 1957, Shah Mohammad Reza Pahlavi established the SAVAK intelligence service to protect the monarchy and pursue opposition movements. After the fall of the Shah in 1979, the organization was dismantled.

It was replaced by SAVAMA, which later evolved in 1983 into the Ministry of Intelligence and Security today the country's primary civilian intelligence agency responsible for gathering and analyzing information both inside Iran and abroad.

However, the balance of power within Iran's intelligence community gradually shifted in favor of the Islamic Revolutionary Guard Corps (IRGC), particularly after the events of the Green Movement protests in 2009. In response, the Iranian leadership expanded the security role of the IRGC through a restructuring of its intelligence apparatus.

Three major institutions were established during that process and now form the backbone of the IRGC's intelligence activity: the IRGC Intelligence Organization, responsible for managing intelligence operations; the Intelligence Protection Organization, tasked with counterintelligence and monitoring security breaches; and the IRGC Protection Organization, which handles specialized security missions including protecting leadership figures and sensitive facilities.

Alongside these institutions, Iran's intelligence ecosystem includes other agencies affiliated with the army, police, and judiciary, as well as specialized cyber security units. There is also an intelligence body linked directly to the office of the Supreme Leader.

Together, this multiplicity forms something akin to a broad intelligence

community in which responsibilities are distributed among several institutions operating with varying degrees of coordination and competition.

One notable feature of this system is that most agencies maintain independent counterintelligence units. Their role extends beyond confronting external infiltration; at times, they also monitor other domestic agencies, reflecting a relatively low level of institutional trust within the system.

To manage this complexity, Iran established the Intelligence Coordination Council, which includes representatives from roughly sixteen security bodies. Its purpose is to coordinate intelligence activity and link it to decisions made by the Supreme National Security Council, although overlaps in authority between agencies persist.

Within this multi-layered structure, the Quds Force of the IRGC stands out as the external arm of Iran's intelligence system. It manages regional networks and gathers information beyond Iran's borders, helping build an expansive target bank that spans multiple theaters across the region.

In essence, Iran's intelligence architecture is built on an overlapping institutional model that allows information to be collected through multiple channels. This provides the Iranian state with a wide network of data sources—one of the core pillars on which Tehran relies to construct its target bank during crises and wars.

The Shadow War: The Intelligence Battle Between Iran and Israel

The confrontation between Iran and Israel during the war represents an extension of a long trajectory of indirect conflict. Intelligence warfare has long been a central if largely hidden component of that struggle, gradually evolving into a primary arena of competition between the two sides.

Long before military strikes appeared in public view, the intelligence services of both countries were engaged in a shadow war involving infiltration, espionage, technical sabotage, and assassinations. The central objective was to build a comprehensive target bank while weakening the adversary's ability to protect its military and strategic secrets.

Over the past two decades, Israel has succeeded in achieving deep penetrations inside Iran, reflecting the scale of Israeli investment in espionage infrastructure and cyber capabilities directed against Tehran. One of the earliest and most significant episodes in this campaign was the cyberattack involving the Stuxnet virus in 2007.

The malware infiltrated the Natanz nuclear facility and destroyed roughly 1,000 centrifuges about 10 percent of the devices operating at the time delivering a direct blow to Iran's nuclear program and exposing the vulnerability of its

technological infrastructure to external penetration.

Israeli intelligence operations targeting Iran's nuclear program and military infrastructure continued thereafter. These included the theft of Iran's nuclear archive and cyber sabotage operations targeting key facilities such as drone factories, uranium enrichment centers, and ballistic missile bases. They were accompanied by a campaign of assassinations targeting Iranian nuclear scientists, most notably Mohsen Fakhrizadeh in 2020.

This intelligence war reached a peak during the Israeli operation known as "Rising Lion" during the Twelve-Day War, which demonstrated Tel Aviv's ability to translate years of intelligence gathering into precise strikes against sensitive figures and locations inside Iran.

Iran, for its part, has attempted to develop its own capabilities for counter-infiltration inside Israel. In June 2025, Iranian Intelligence Minister Esmail Khatib announced that Tehran had obtained what he described as a "treasure trove of strategic information" from inside Israel.

According to Iranian officials, the material included sensitive documents related to Israel's nuclear program and its relations with the United States and Europe. Tehran claimed the operation was the result of years of infiltration and recruitment of sources inside Israel.

Israeli security investigations have also revealed a surge in espionage activity linked to Iran within Israeli society. Over the past two years, roughly thirty-five indictments have been filed in espionage cases involving nearly sixty defendants.

These cases suggest a shift in Iranian methods toward recruiting individuals for small, incremental tasks beginning with collecting information or photographing locations before, in some instances, evolving into more sensitive assignments.

Sleeper Cells in the Gulf

Iran's intelligence activities have not been limited to its direct confrontation with Israel or the United States. They have also extended to the construction of a covert infrastructure across its regional environment, particularly in the Gulf region.

Numerous incidents announced by Gulf governments over past decades suggest the presence of espionage networks and cells linked to Iranian intelligence agencies or the IRGC. These networks allegedly operated covertly inside Gulf states to gather information and build a regional target bank in anticipation of any potential confrontation.

Sleeper cells are typically defined as groups operating secretly within a particular society that remain dormant for extended periods before being activated to carry

out specific tasks. These tasks often include gathering intelligence about military facilities and critical infrastructure or conducting security and political influence operations during moments of crisis.

The danger posed by such cells lies in their ability to operate undetected for long periods, making it extremely difficult to estimate their true scale or the scope of their activities.

From this perspective, Iran appears to view these networks as one of its unconventional lines of defense in the event of military escalation against it. The presence of operatives capable of monitoring military bases and vital installations in the Gulf provides Tehran with an important source of information regarding U.S. military deployments and strategic infrastructure across the region.

Several Gulf states have announced in recent years that they had dismantled espionage networks linked to Iran. In Saudi Arabia, authorities revealed in 2013 that they had broken up a spy ring of eighteen individuals accused of gathering information on vital facilities for Iranian intelligence. The United Arab Emirates has also seen multiple espionage cases involving the leakage of sensitive military information to actors linked to Iran.

Kuwait has uncovered spy networks accused of monitoring military installations and locations of U.S. forces within the country—cases that at times prompted sharp diplomatic measures against Tehran. In Bahrain, authorities have also announced espionage cases linked to the IRGC as well as arms smuggling networks and drone operations.

This dimension became even more visible during the recent war. In March 2026, Qatar announced the arrest of two cells linked to the IRGC comprising ten suspects. Some had reportedly been tasked with gathering information about military and vital installations, and maps, coordinates, and technical equipment were seized in their possession.

In light of these incidents, these networks can be seen as part of a broader intelligence infrastructure that Iran has gradually built across its regional environment. Their purpose is to enhance Tehran’s ability to gather precise information that could be used once confrontation erupts.

In this sense, sleeper cells represent one component of the Iranian target bank that has been constructed over years in preparation for a potential conflict.

Confirmed Strikes and Active Pursuit

An examination of the pattern of Iranian strikes against the American military presence in the region particularly in the Gulf suggests that the first wave was

primarily drawn from a pre-prepared target bank consisting of known and publicly declared U.S. bases.

This implies that Iranian intelligence efforts initially focused on confirming coordinates, identifying deployment points, and increasing strike accuracy against fixed and relatively well-known facilities.

This network includes major U.S. bases across the Gulf and the surrounding region from the headquarters of the Fifth Fleet in Bahrain to Al Udeid Air Base in Qatar, Camp Arifjan and Ali Al Salem Air Base in Kuwait, Al Dhafra Air Base in the UAE, and Prince Sultan Air Base in Saudi Arabia, in addition to U.S. sites in Jordan and Iraq.

However, some strikes went beyond targeting publicly known bases to hit air defense batteries, radar installations, and early warning facilities sites that do not all fall within the conventional scope of known military bases.

This suggests that the Iranian target bank underwent continuous updating based on a combination of aerial surveillance, satellite imagery, signals interception, and possibly human intelligence gathered on the ground.

This pattern also aligns with Western assessments suggesting that Iranian strikes expanded to include military, oil, hotel, and port facilities in the Gulf indicating an attempt to disrupt the network of American deployment and positioning rather than focusing solely on major military installations.

While strikes against fixed bases point to the existence of a prepared target bank, some developments during the war suggest that Iran also possessed albeit to varying degrees the capability to track mobile or semi-covert targets. The Washington Post reported that an Iranian drone struck a hotel in Manama, injuring two employees of the U.S. Department of Defense.

Similarly, a source told CNN that the CIA station in Riyadh was targeted by a drone during an attack on the U.S. embassy there. The Washington Post had earlier reported that the station sustained damage during the attack, though the CIA declined to comment.

Israel’s public broadcaster Kan also reported that Israelis were injured after an Iranian drone struck an apartment near one of Israel’s representation offices in Abu Dhabi. Hebrew-language sources confirmed that a suicide drone directly hit an apartment housing Israeli residents in the heart of the UAE capital, causing severe material damage.

Taken together, these incidents suggest that some strikes were based on more precise intelligence, pointing to a multi-layered intelligence effort employing different tools and methods. The significance of this pattern is further

underscored by U.S. warnings to its citizens in Bahrain that hotels could become targets for attacks, indicating that the threat was no longer confined to traditional military bases but had extended to alternative spaces of residence and movement bringing the conflict closer to the logic of active pursuit rather than conventional bombardment of fixed installations.

In this context, Iran's Tasnim News Agency reported that IRGC intelligence had urged people "not to host Americans in hotels and to stay away from places where they are present," adding: "We will monitor Americans and target them."

Multiple narratives have also circulated including official Iranian statements and reports in Western media about attacks targeting American intelligence facilities that had not been publicly acknowledged. While no clear official confirmation has been issued by Washington, the possibility suggests that some Iranian strikes were aimed at the intelligence nerve centers directing part of the war in the region.

These indicators collectively point to a tangible operational effort by Iranian human intelligence on the ground. Human sources remain the most capable means of tracking temporary deployment sites, individual movements, and unofficial workplaces—information that cannot be fully obtained through technical tools or remote surveillance alone.

Accordingly, the most plausible picture is that Iran operated on two parallel levels: first, striking a pre-prepared target bank of known American bases and facilities; and second, updating this bank during the war through technical surveillance and human infiltration. This allowed, in some cases, for more precise strikes against radar sites, locations of residence or movement, and facilities directly connected to American and Israeli military and intelligence activities.

Taken together, these developments reveal how much of what had been managed in secrecy for years surfaced during the war. Intelligence emerged as one of the most decisive factors shaping the confrontation not only in directing strikes but also in amplifying their costs and complicating the calculations of the adversary.

Despite the heavy security blows Tehran suffered before and during the conflict, it nevertheless demonstrated an ability to leverage its intelligence tools to deliver security-oriented strikes that disrupted part of the strategic equation even if they remained within a ceiling of capabilities below those of the United States and Israel.