



By: Nawaf Obaid

The Hidden War for Yemen's Islands



For years, the war in Yemen has been portrayed as a struggle over cities, militias, and ceasefires.

That framing misses the most consequential dimension of the conflict: a deliberate effort by the **United Arab Emirates** (UAE), acting through UAE Special Forces–led external operations task forces, to construct a parallel military-intelligence architecture across southern Yemen and its offshore islands.

This was not an auxiliary contribution to the Saudi-led coalition; it was an Abu Dhabi-financed, managed, and commanded system designed to secure long-term control over terrain and maritime chokepoints critical to global trade and military movement.

This architecture was conceived as a multi-domain intelligence, surveillance, and reconnaissance grid, integrating airborne ISR (manned aircraft and unmanned aerial systems), maritime domain awareness platforms, and subsea sensing arrays into a single operational picture.

Its purpose was persistence: continuous custody over air, surface, and subsurface movement across the Bab al-Mandab, the Gulf of Aden, and the western Arabian Sea.

The system's design logic far exceeded any declared counterterrorism or maritime-safety mandate and instead mirrored state-level intelligence enterprises.

Crucially, this was not a passive monitoring construct. It was fused to **UAE Special Forces** task groups, primarily elements of the Emirati Presidential Guard, embedded across islands, ports, and airfields.

These task forces exercised command and operational control over ISR tasking, logistics, sustainment, and data backhaul through command pathways outside approved coalition inventories, allowing Abu Dhabi to operate an independent battlespace picture beyond Yemeni sovereign authority.

That entire framework has now collapsed.

What failed was not a single base or agreement, but the Abu Dhabi-run system linking islands, mainland hubs, and collection sites into a coherent network.

The decisive inflection point was the restoration of Yemeni sovereign control under **Saudi-led coalition enforcement**, followed by physical takeover, technical exploitation, and the removal of non-authorized personnel and systems.

The exposure of this network matters because it reveals intent. Recovered layouts, infrastructure signatures, and system configurations demonstrate preparation for long-term dominance over maritime and air approaches, not temporary coalition support.

The **architecture** was built to endure, to surveil, and to shape the environment—until sovereign enforcement made that persistence untenable.

Mayun (Perim): The Bab al-Mandab platform

Mayun Island was operated as a forward UAE Special Forces–controlled military-intelligence platform overlooking one of the world's most sensitive maritime chokepoints.

Post-Saudi takeover exploitation confirmed the presence of Israeli engineers and intelligence technicians operating alongside UAE personnel, fully integrated into a UAE command chain.

Their role was technical and operational: installation, calibration, sustainment, and operation of advanced ISR infrastructure supporting persistent monitoring of the **Bab al-Mandab**.

Technical exploitation confirmed the installation of advanced Israeli-made air-surveillance systems configured to generate long-range air pictures and cue ISR collection against aircraft and unmanned systems transiting the southern Red Sea.

These sensors were fused with airborne ISR feeds from manned aircraft and drones operating from Mayun and associated hubs, forming closed sensor-to-tasking loops designed for uninterrupted coverage rather than episodic observation.

Mayun was intended to mature into a permanent Emirati Israeli forward operating base, capable of sustaining ISR sorties, drone operations, and interdiction-capable aviation

In parallel, Mayun hosted sophisticated underwater surveillance systems, including seabed-anchored passive and active acoustic arrays configured for submarine detection and classification.

Orientation and recovered signature libraries indicate deliberate monitoring of naval traffic through the strait, including Saudi, Egyptian, NATO, and multinational vessels operating under Combined Task Force mandates.

These systems bore no resemblance to port-security or navigational-safety installations and were clearly configured for strategic intelligence collection.

Recovered planning materials indicate that Mayun was intended to mature into a permanent Emirati Israeli forward operating base, capable of sustaining ISR sorties, drone operations, and interdiction-capable aviation.

Infrastructure signatures—runway reinforcement, hardened support zones, and sustainment facilities—were consistent with long-term basing rather than temporary presence

Socotra and the offshore network

The Socotra Archipelago was operated as a distributed ISR and maritime-monitoring

complex under UAE task force control.

Elevated sites, shoreline installations, and port-adjacent nodes were configured to provide persistent coverage over the Gulf of Aden and Arabian Sea.

A base on Abd al-Kuri Island and supporting infrastructure on Samhah enabled logistics, access control, and system sustainment.

Redundant power, hardened shelters, and secure communications were consistent with long-term collection and command continuity, not transient coalition activity

Post-takeover **Saudi and Yemeni inspection** identified integrated air-maritime ISR suites, including coastal radar, electronic-collection receivers, UAV ground-control elements, and data-fusion nodes.

Redundant power, hardened shelters, and secure communications were consistent with long-term collection and command continuity, not transient coalition activity.

Mainland hubs and system integration

The island network was reinforced by mainland hubs—Al-Rayyan Airport in Mukalla, Balhaf in Shabwa, Mocha Port, and Al-Anad Air Base in Lahj—used as Abu Dhabi-run operational nodes.

These facilities enabled sustainment, personnel rotation, ISR tasking, and data relay, allowing island-based systems to operate continuously within a single **UAE-controlled operating picture**.

Command responsibility and foreign personnel

This architecture was **Abu Dhabi-financed and commanded**. UAE officers exercised operational control, while foreign personnel were integrated into the system.

Post-takeover Saudi coalition verification confirmed the presence of foreign mercenaries from multiple European and Latin American countries for site security and operational support, alongside Israeli technical personnel embedded with UAE Special Forces task elements to operate advanced ISR systems

Technical exploitation and findings

Joint exploitation by Saudi, Yemeni, and Egyptian military engineers uncovered systems absent from authorised coalition inventories and built around software incompatible with GCC, **NATO**, and CENTCOM ecosystems.

On Socotra, concealed installations at elevated sites were configured for persistent wide-area monitoring, while coastal zones revealed submerged acoustic sensors designed for advanced maritime signature analysis.

Architecture analysis confirmed multi-INT fusion chains combining geospatial, signals, electronic, acoustic, and UAV-derived intelligence, enabling long-dwell tracking of surface combatants, submarines, and aircraft.

This configuration is consistent with state-level intelligence collection rather than counterterrorism operations.

Dismantlement and aftermath

Once sovereign Saudi coalition enforcement was restored, the system's vulnerabilities became decisive.

Island sites were shut down, surveillance nodes dismantled, and mainland hubs cleared of Abu Dhabi-run functions.

The network's value lay in connectivity and persistence; once those were broken, the architecture collapsed.

What this means for Saudi Arabia—and for Yemen

What ultimately emerged from the dismantling of this architecture was not a vacuum but a consolidation of authority.

Saudi Arabia has now assumed full strategic ownership of the Yemen theatre, not only militarily but also in **sovereign and security terms**, placing Yemen's islands, ports, airfields, and maritime approaches firmly under a Saudi-led coalition framework.



Saudi Arabia has now assumed full strategic ownership of the Yemen theatre, not only militarily but also in sovereign and security terms

This was not expansion; it was containment. Yemen was veering toward fragmentation through parallel, externally managed systems operating beyond accountability.

By dismantling unauthorised military-intelligence infrastructure and reasserting coalition discipline, Riyadh halted that trajectory, restored coherence, and assumed ultimate responsibility for stability across the Arabian Sea, Bab al-Mandab, the Gulf of Aden, and adjacent approaches—preventing Yemen from sliding into a patchwork of foreign-run enclaves embedded with permanent surveillance and control mechanisms.

What was dismantled in southern Yemen was

not an auxiliary coalition footprint but an Abu Dhabi-run, financed, and managed military-intelligence enterprise, incorporating foreign mercenaries and Israeli technical participation to establish persistent ISR dominance across one of the world's most strategic maritime corridors.

It was designed to endure. It did not. The collapse of this architecture restored Yemeni sovereign control over islands, ports, airfields, and chokepoints—and placed the burden, authority, and responsibility for Yemen's security squarely where it now resides, within a Saudi-led coalition framework capable of enforcing order rather than multiplying fragmentation.

Dr Nawaf Obaid is a Senior Research Fellow at the Department of War Studies, King's College London.