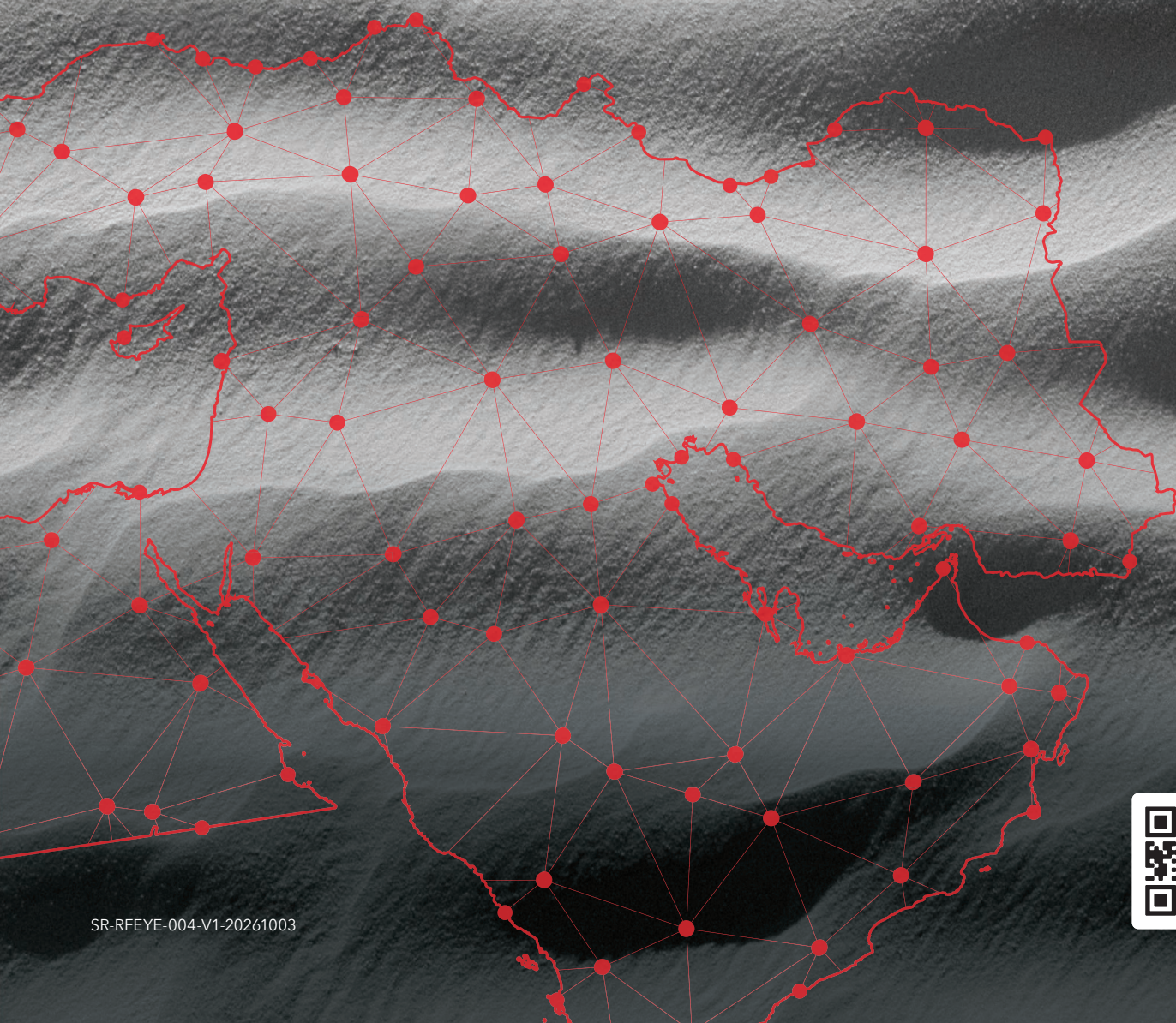


PRAEMONITUS PRAEMUNITUS

FOREWARNED IS FOREARMED

Using wide area, networked, radio frequency sensing to
enhance regional defence and security in the Middle East



An aerial, high-angle photograph of the Middle East, showing the Arabian Peninsula, the Red Sea, and the Persian Gulf. The land is a mix of brown, tan, and green, with visible mountain ranges and coastal features. The water is a deep blue. The sky is a clear, pale blue.

As 2026 unfolds, the Middle East faces an array of defence and security challenges. Insurgencies continue to rage across the region. Vital sea lanes of communications remain at risk from piracy.

FOREWORD

The Middle East, an international crossroads, a tech development hub, and global supplier of resources, will undoubtedly play a central role in the future of the world.

Yet despite the region's strength, several security challenges pose a threat to its stability and prosperity. Suicide drones can disrupt oil refineries, jamming can cause havoc for aviation, and attacks on shipping can threaten lives and trust.

This special report joins seemingly disparate threats across the region and offers a framework for how militaries and security agencies can augment their defences by adding another layer of protection. Wide-area RF sensing is a technological solution that can help exploit modern threats' Achilles heel—dependency on the electromagnetic spectrum.

In this report, Dr Thomas Withington, an expert in electronic warfare, associate fellow at RUSI, and senior non-resident fellow at NATO Defence College, makes the threats we cannot see highly visible.

TABLE OF CONTENTS

Introduction	5
Uninhabited aerial vehicle threats	7
Wide-area, deployed sensing and the UAV threat	7
Airspace Security and Radar Coverage Gaps	9
Enhancing ATC and air defence coverage	10
Maritime Domain Awareness: Red Sea and Coastal Challenges	11
Watching the waters	12
Jamming Detection	13
Pinpointing the problem	13
In building Technical Surveillance Counter Measures	14
Border Security Monitoring	15
Radio at the frontier	15
Conclusions and Recommendations	16

INTRODUCTION

As 2026 unfolds, the Middle East faces an array of defence and security challenges. Insurgencies continue to rage across the region. Vital sea lanes of communications remain at risk from piracy. The maritime environment is characterised by the growing menace of Anti-Ship Missile (AShM) and suicide Uninhabited Aerial Vehicle (UAV) attacks against commercial shipping. Maritime and coastal areas are also exploited by criminals for the smuggling of contraband, people, narcotics and weapons. The illicit use of UAVs, both for acts of violence, and to gather Intelligence, Surveillance and Reconnaissance (ISR) data, remains a cause for concern. The provision of Global Navigation Satellite System (GNSS) Position, Navigation and Timing (PNT) signals, once taken for granted, are now increasingly at risk from deliberate jamming and spoofing. These electronic attacks impact the safety of air and maritime navigation, and commerce. Domestically, countries are at risk from domestic insurgents and foreign espionage. Meanwhile, thousands of miles of land borders across the region are vulnerable to violation by criminal elements.

Countries can choose to expand and enhance their militaries, border security cadres and domestic law enforcement organisations to counter these challenges. Adequately staffed, trained and equipped local organisations are vitally important. Nonetheless, such a course of action will always entail significant expenditure. As this report explains, one way by which the security of Middle East nations can be enhanced at relatively low cost, is via the deployment of networked, Radio Frequency (RF) sensing Electronic Support Measures (ESMs) across wide areas. The security challenges faced by the region all, in some way, exploit the radio segment of the electromagnetic spectrum. The radio spectrum is an environment where threats reside. By maintaining a detailed view of this spectrum across a specific local, regional militaries and law enforcement can receive timely warnings of potential threats. The act of monitoring the spectrum; detecting, identifying, locating and sharing (henceforth known as processing) threats and then acting upon this information has an important impact: it lessens the freedom of manoeuvre within the radio spectrum these threats can exploit.

The illicit use of UAVs, both for acts of violence, and to gather Intelligence, Surveillance and Reconnaissance (ISR) data, remains a cause for concern. >>

Regional threats include the illicit use of Uninhabited Aerial Vehicles (UAVs). The use of such aircraft by state and non-state actors is a cause for concern and is on the increase. Timely, accurate and comprehensive warning of incoming threats is vital to the Counter-UAV (CUAV) battle. Uninhabited aircraft may traverse tens, or even hundreds, of nautical miles to reach their targets. Processing these targets is paramount to provide air defenders the requisite time to perform an interception if so ordered. However, UAVs can be physically small targets made from non-metallic materials giving them a correspondingly small Radar Cross Section (RCS). Nonetheless, these aircraft are often reliant on a radio link to connect the aircraft to its pilot. Likewise, a radio link may be used to share video imagery, or other ISR data, the UAV is collecting. Detecting these radio transmissions allows the processing of a UAV as a potential target. Unattended, networked RF-sensing ESMs can be distributed across large areas to give comprehensive CUAV coverage. These netted sensors can also be integrated into national and regional Integrated Air Defence Systems (IADS) to provide comprehensive CUAV coverage.

The timely detection of air targets also has relevance for air traffic controllers and air defenders. Conventional, inhabited aircraft make a variety of diverse RF signal emissions. These signals support Air Traffic Control (ATC), navigation and flight safety. At the same time, the Middle East does not enjoy 100 percent coverage of its airspace with Primary and Secondary Surveillance Radars (PSRs/SSRs). Significant parts of the region are bereft of radar coverage which risks hampering flight safety and which could be exploited by aircraft performing illegal, illicit or suspicious flights. By deploying networked ESM sensors across areas bereft of radar coverage, gaps can be filled and the Recognised Air Picture (RAP) enriched. Deploying such sensor networks may be less expensive than new PSR/SSR installations to address paucities of coverage.

While nations across the Middle East face threats from conventional and uninhabited aircraft, the region's waters remain blighted by illegal activity and insurgent attacks. This is problematic given the Middle East's dependence on the Red Sea and Persian Gulf for exports of hydrocarbons, and for the global flow of maritime trade through the Red

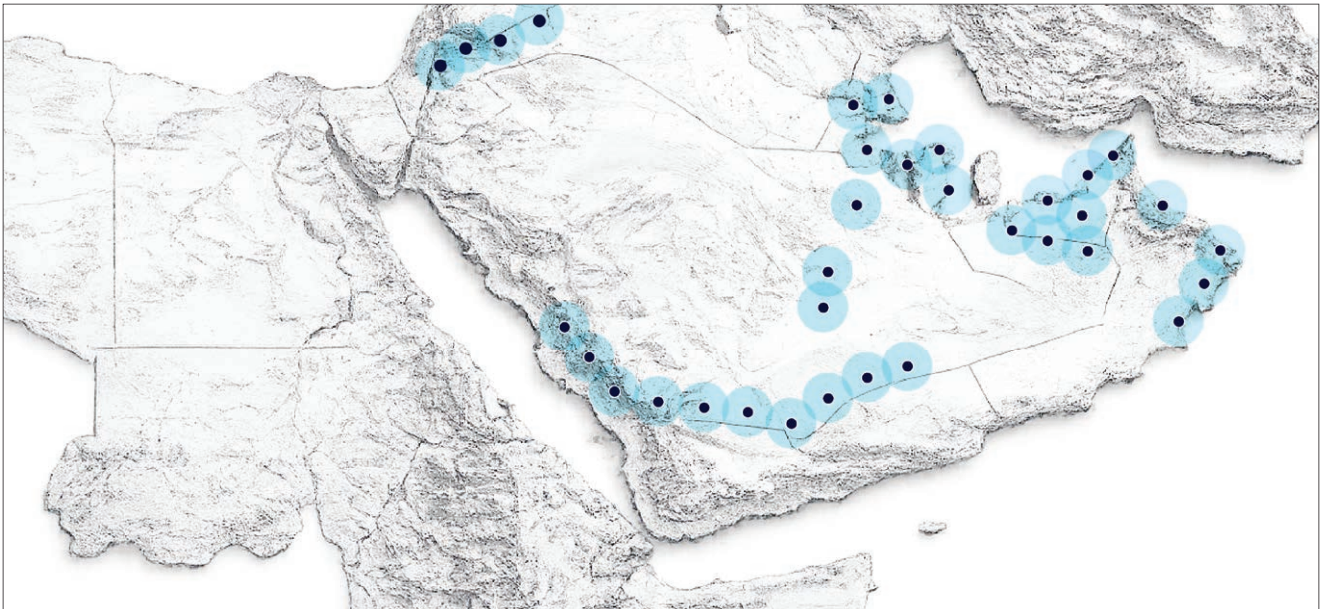


Image 1: Air defense RFeye Sensor deployment across the Middle East

Sea and Suez Canal. Recent years have seen the Red Sea affected by attacks from Houthi insurgents in Yemen against commercial maritime traffic. Commercial and civilian marine traffic is as reliant on RF signals for safe navigation as aircraft. Radio frequency emissions from vessel communications and radar can be detected and exploited by networked, wide area sensing to determine a ship's location and identity. A ship underway but not emitting any radar or communications signals may indicate suspicious behaviour warranting additional investigation by local coastguards or navies. These ESM architectures may have added utility in providing early warning of anti-ship missile attacks against commercial shipping.

Meanwhile the deliberate spoofing and jamming of GNSS PNT signals is on the increase across the Middle East. State and non-state actors alike seek to protect potential targets from attack by GNSS-guided ordnance and suicide UAVs. This jamming and spoofing is seriously impacting the safety of commercial aviation and shipping. GNSS disruption also risks having a serious impact on commerce in the region and beyond. Wide-area, networked RF sensing has the potential to detect and locate sources of deliberate GNSS PNT interference. This can help to identify those performing the jamming as a prelude to further action, diplomatic or otherwise, to encourage its cessation.

Wide-area, networked ESM coverage can also pay dividends from an internal security perspective. Several countries around the Middle East are grappling with ongoing insurgencies. Foreign espionage may also be a significant problem. Insurgents and intelligence operatives can be monitored via the cellphones that they depend on to remain in contact with fellow cadres. So-called 'International Mobile Subscriber Identity (IMSI)

catchers' provide a mechanism to track a person of interest via their cellphone. In-building monitoring for Technical Surveillance Countermeasures (TSCM) can provide a valuable layer of additional security for sensitive, strategic or classified intelligence protection (military bases, embassies, intelligence HQ, for example). Full spectrum permanent RF spectrum monitoring is now widely deployed across the Middle East to secure zones or whole building interiors and counter drone, electronic eavesdropping and espionage.

Deployed, wide area sensor networks could also help strengthen border security across the Middle East, particularly in areas where frontiers are in sparsely populated or inhospitable areas. Deploying additional border forces always risks entailing a financial outlay for personnel and equipment. A lower-cost alternative maybe found in these sensing networks. Criminal elements keen to smuggle contraband, people, weapons, cash and narcotics illicitly through frontiers depend on radio communications to coordinate their activities. Spartan areas may lack cellphone coverage, but Satellite Communications (SATCOM), for example, may provide an alternative. These, and other, radio signals can be detected by networked ESMs and geolocated. Local border forces can then be deployed for further investigations.

This report will detail the applications for deployed wide-area, networked ESMs in the context of the defence and security challenges faced by nations in the Middle East. Several case studies will be used to explain the relevance of this technology, and the benefits it affords. These benefits not only address local domestic and international security issues but may also help to meet sovereign national security and defence concerns, while reducing reliance on U.S. power.

UNINHABITED AERIAL VEHICLE THREATS

The statistics make for sober reading: between October 2024 and September 2025 the Middle East experienced 417 incidents involving the offensive use of a UAV. As figures from the Tactics Institute for Security and Counter Terrorism, a non-governmental organisation based in London, note these 2024/25 statistics represent a seven-fold increase on the number of similar occurrences between 2023 and 2024.¹ As the institute's report makes clear, a large percentage of incidents involving the offensive use of UAVs has been blamed on Houthi insurgents. The Houthis are a politico-religious group operating in Yemen which claim to represent the Zaidis, the country's Shia Muslim population.² The Houthis are one politico-religious movement which is reported to receive support from the Islamic Republic of Iran. Other groups include Hezbollah, a Shia politico-religious movement based in Lebanon and Hamas, a Sunni Muslim Palestinian movement active in the Gaza Strip on the eastern Mediterranean coast. All these organisations are avid UAV users.³

Reports in late 2025 noted the widespread use of these uninhabited aircraft both by Hezbollah and the Israeli military in southern Lebanon and in the vicinity of the Israel-Lebanon border.⁴ Although the politico-military

power of Hamas has almost certainly been degraded as a result of Israeli Defence Force (IDF) operations since the Hamas-led attacks on southern Israel on 7th October 2023, the insurgent group has continued to use UAVs to support its operations. In June 2025, the IDF noted an upsurge in the use of uninhabited aircraft within the Gaza Strip. Hamas is believed to be using UAVs for ISR gathering and to target IDF units with UAV-delivered weapons or suicide UAVs.⁵

One area of less certainty is the use of UAVs for strike and ISR missions by the Islamic State and Iraq and Syria (ISIS). There appears to be little information in the public domain regarding the extent to which ISIS has embraced the use of uninhabited aircraft for these missions. There is certainly evidence that ISIS has deployed UAVs in the past. One analysis noted that in 2017 the group may have performed over 200 attacks with UAVs in Iraq and Syria theatres.⁶ Military action by a coalition of nations including France, the United Kingdom and the United States are ongoing against ISIS in these countries. There is every possibility that such offensive operations have degraded the group's ability to use UAVs en masse as an attack vector.



There is no single capability that can detect, identify, locate and engage a hostile UAV. Instead, several technologies must be brought to bear in the CUAV fight. >>

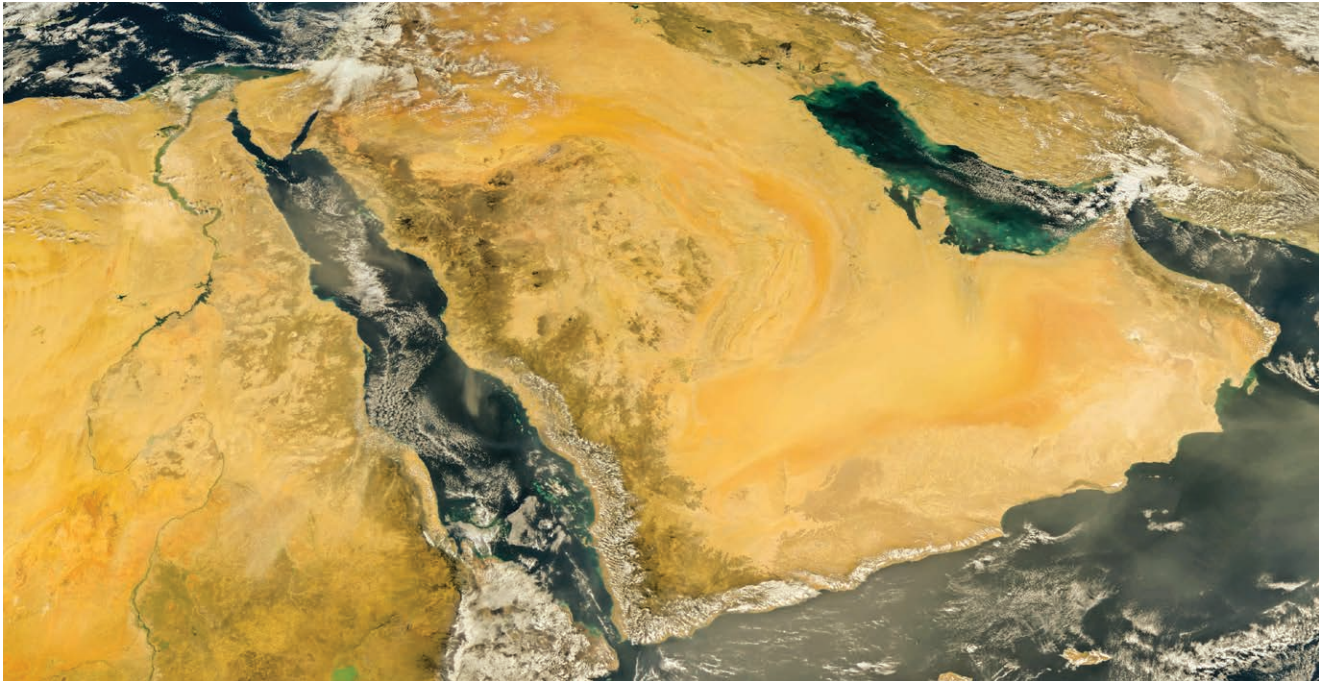


 *Image 2: Satellite image of the Middle East*

Wide-area, deployed sensing and the UAV threat

There is no single capability that can detect, identify, locate and engage a hostile UAV. Instead, several technologies must be brought to bear in the CUAV fight: These capabilities include the processing of UAV targets by radar, ESMs and optronics. ESMs are of particular interest as they can process the radio signals that link a UAV to its pilot. These signals are used to control the aircraft and for the UAV to share its telemetry and the ISR data it is collecting. Many UAVs, particularly those intended for the hobby or commercial markets, have an in-built fail-safe device. Should the aircraft lose the signal linking it to the pilot it will land in situ or return to its point of origin. The same action may also occur if the aircraft loses access to GNSS PNT signals. Most UAV signals use frequencies within the Very/Ultra High Frequency (V/UHF) wavebands of 30 megahertz/MHz to three gigahertz/GHz.

A single ESM placed on a vantage point like a mast, high building or elevated terrain may be able to detect a UAV via this radio signal from ranges of tens of kilometres, if not more, depending on the signal strength. A single ESM will provide a Line-of-Bearing (LOB) to the UAV. A LOB may be useful in warning that a UAV may be inbound but provide

precious little additional information. Instead, two or more ESMs placed a measured distance apart can use techniques like Angle of Arrival (AOA) or Time Difference of Arrival (TDOA) (requiring at least four ESMs for geolocation in three dimensions) to determine a UAV's location and follow it over time. With this information, air defenders can then decide what action to take against the aircraft. The more ESMs that are deployed over a specific area, the more precise the information that can be obtained about a single UAV, or even a swarm of such aircraft. The networking of these ESMs is imperative to ensure they can share the data they are collecting with ease. This information may be sent across radio, satellite communications, fibre optic and/or conventional telecommunications to Command and Control (C2) systems which will perform the requisite TDOA/AOA calculations. The more ESMs deployed across a specific area, the denser the CUAV coverage. Such deployments can be scaled up to cover large swathes of territory. For example, it is thought that the entire front between Russia and Ukraine in the latter theatre, circa 1,250 kilometres (800 miles), is covered with UAV detection systems, including ESMs.⁷ The CUAV battle is a clear demonstration of one mission where networked sensors deployed across large areas greatly enrich air defence situational awareness.

AIRSPACE SECURITY & RADAR COVERAGE GAPS

Like UAVs, inhabited air traffic relies on the electromagnetic spectrum, particularly to ensure safe navigation. As noted above, UAVs will use a radio link connecting the uninhabited aircraft to its pilot. It is this link that can provide air defenders with a mechanism to process these targets and determine if they are hostile. Civilian aircraft, and military aircraft not flying combat missions, similarly rely on RF signals.

Contemporary aircraft emit several voice and data signals for ATC, flight safety and navigation. For example, VHF radio signals on a waveband of 118MHz to 136.975MHz are used for two-way communications between aircraft and ATC. As VHF is chiefly restricted to LOB ranges, Beyond LOS (BLOS) communications, such as when an aircraft is flying across large stretches of ocean or Arctic areas, relies on High Frequency (HF: three megahertz to 30MHz) radio. BLOS links are also facilitated with SATCOM L-band (1.616GHz to 1.6265GHz/ 1.5GHz to 1.6GHz) frequencies used by the Iridium and Inmarsat constellations.

Aircraft are routinely equipped with SSR transponders. These transponders respond on a frequency of 1.030GHz to a challenge transmitted by an SSR using a 1.090GHz signal. The SSR is often collocated with a PSR. The 1.030GHz and 1.090GHz frequencies are also used by aircraft traffic collision avoidance systems to broadcast their position to other aircraft in the locale. Finally, aircraft radar altimeters transmitting on frequencies of 4.2GHz and 4.4GHz inform pilots of their altitude above the ground. Flight safety is further enhanced by weather radar which maybe carried by some aircraft to provide advanced warning of difficult conditions. Weather radar routinely uses frequencies of 9.345GHz and 9.375GHz.⁸

Finally, air radio navigation systems like VHF omni-directional range and instrument landing systems are passive as the aircraft only receives a signal that is being transmitted from somewhere else. Conversely, an aircraft's Distance Measuring Equipment (DME) is active, which can provide a valuable source of RF intelligence. The aircraft will send out radio pulses on frequencies



Image 3: Area of the Arabian Peninsula where the Empty Quarter is located



A challenge faced by air traffic controllers and air defenders is the detection and processing of inhabited airborne targets. >>

between 960MHz and 1.215GHz which is received by a DME station. The station pauses for 50 microseconds/ms and transmits a signal back to the aircraft. The aircraft's DME receiver computes the entire duration of the outgoing radio signal, the 50ms delay and the return signal from the DME station. The receiver subtracts the 50ms delay and divides the remaining time by two to calculate the distance of the aircraft from the DME station. This calculation is based on the fact that radio signals travel at the speed of light; 161,595 knots-per-second/299,274 kilometres-per-second.⁹

Enhancing ATC and air defence coverage

As with UAV detection and processing, a challenge faced by air traffic controllers and air defenders is the detection and processing of inhabited airborne targets. While the Middle East region has 100 percent ATC coverage, in that national ATC authorities are responsible for overlapping sections of airspace, PSR/SSR coverage is less comprehensive. Estimates from the International Civil Aviation Organisation (ICAO), the United Nations organisation responsible for international civil aviation regulation, safety and

sustainability, state that between 67 percent and 73 percent of airspace in the region has PSR/SSR coverage.¹⁰

One way of closing ATC and air defence surveillance coverage gaps is to deploy networked ESMs to detect and process the RF signals from aircraft discussed above. These ESMs could be deployed across areas where radar coverage is sparse or non-existent. By deploying several of these RF sensors, precise details regarding an aircraft's position, altitude and speed could be defined through techniques like TDOA and AOA. Information regarding targets could be encoded into standard protocols such as ASTERIX (All Purpose Structured Eurocontrol Surveillance Information Exchange) and shared with air traffic controllers and air defenders. It would even be possible to deploy these sensor networks across challenging and inhospitable locations by networking them using radio, conventional telecommunications, fibre optic and/or SATCOM links. Deploying networked, wide-area RF sensors to close radar coverage gaps may also have a financial incentive as such an approach may be less expensive than deploying PSR/SSRs to provide missing coverage.

MARITIME DOMAIN AWARENESS: RED SEA & COASTAL CHALLENGES

Given that they fly at altitude, conventional aircraft and UAVs can be detected at range. To put matters into perspective, RF signals from an airliner flying at 30,000 feet/ft (9,144 metres/m) could potentially be detected by an ESM on the ground at circa 211 nautical miles/nm (390km). Even a UAV flying at an altitude of 328ft (100m) could be detected by the same ESM at a range of 22nm (41km). A network of passive ESM sensors is used to provide wide area air defence monitoring. This network, accompanied by tactical and mobile sensors can provide valuable 'air corridors' for detection and location of threats. However, caveats should be observed that signal detection depends on the sensitivity of the ESM, the gain of its receiving antenna, the gain of the transmitting antenna, environmental and meteorological conditions and the strength of the transmitted signal. The ability to detect targets at altitude cuts both ways as networked ESMs carried by UAVs or conventional aircraft can potentially provide long RF detection ranges, depending on the aircraft's altitude.

Detecting targets at range is an important consideration for maritime domain awareness and coastal security. Of all the Middle East nations only Jordan and Iraq do not have extensive coastlines. The rest have long stretches of coastline either on the Mediterranean, the Red Sea, the Arabian Sea or the Persian Gulf. One nation, the Kingdom of Saudi Arabia, has coastlines on both the Red Sea and the Persian Gulf. Taken together Bahrain, Egypt, Iran, Iraq,

Israel, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, the United Arab Emirates (UAE) and Yemen have a combined coastline of approximately 7,496nm (13,883km). All these countries have maritime Exclusive Economic Zones (EEZs) which, combined, comprise an area of circa 627,515 square nautical miles (2.2 million square kilometres).¹¹

The Middle East is also home to two important shipping routes, chiefly from the Indian Ocean, via the Red Sea, through the Suez Canal and into the Mediterranean. Likewise, the Persian Gulf remains a major conduit for global hydrocarbons traffic from regional oil and gas fields, and refineries to the outside world. As of 2025, circa 100 vessels move through the Strait of Hormuz where the eastern Persian Gulf meets the Gulf of Oman. This figure includes up to 16 large tankers daily, with all tankers carrying up to 20.5 million barrels of Brent Crude daily, equating to 25 percent of all seaborne traded oil and 34 percent of the global oil market. Twenty percent of the world's liquified natural gas is moved from terminals in Qatar and the UAE for exports daily.¹²

It is noteworthy that global commercial maritime traffic through the Red Sea declined in 2025. According to figures produced by the United Nations Conference on Trade and Development, circa 25 commercial vessels traverse the Red Sea daily. This is a dramatic reduction from around 75 commercial ships which navigated this stretch of water daily in the past. For example, a 90 percent drop in



Image 4: The Gulf of Aden and the Red Sea

container vessel traffic was seen in the Red Sea compared to levels of similar shipping seen in 2023. Rates of tanker and bulk carrier movement have similarly declined by 37 percent and 46 percent respectively.

Reductions in Red Sea commercial maritime traffic have been blamed on violent actions by Houthi extremists targeting shipping from the coast of Yemen. Between September 2024 and September 2025, thirteen commercial vessels were targeted by Houthi attacks. These attacks were performed using ASHMs, ballistic missiles, UAVs, uninhabited surface vessels, gunfire and rocket propelled grenades. Two of the attacks, both performed in July 2025, resulted in two vessels, the MV Magic Seas and Eternity C, being sunk.¹⁴

Alongside insurgent maritime threats, areas of the Red Sea and Persian Gulf continue to experience piracy and transnational crime. Narcotics, weapons and people smuggling continue to be major regional concerns. The multinational Combined Task Force 150, a coalition of navies patrolling the Horn of Africa and North Arabian Sea, seized 16 tonnes of narcotics worth around \$2 billion in 2025. The World Bank and United Nations Office on Drugs and Crime both noted increases of weapons trafficking into the Middle East in 2025, particularly via Yemen. Tens of thousands of migrants are believed to have been trafficked into the Middle East, chiefly from Ethiopia and Somalia using this stretch of water.

Watching the waters

Marine traffic depends on the radio spectrum for navigation. This dependency creates RF signals which networks of coastal ESMs, together with electronic support measures on vessels and aircraft, can exploit to detect suspicious marine traffic. Positioning ESMs on coastlines provides a means by which the RF environment, at least to the twelve nautical mile (22km) limit of a country's territorial waters, can be monitored. An ESM's receiving antenna positioned atop a 30m (98ft) mast would provide sufficient coverage to this distance. Obviously, the LOS range of an ESM receiving antenna can be increased by locating these on hills, cliffs or mountains near coastlines. Larger EEZs can be monitored using ESMs on vessels, inhabited aircraft and UAVs. It may also be possible to deploy ESMs and their receiving antennas on buoys.

RF signal data collected and processed by commercial radio frequency sensing satellites can also help to enrich the local Recognised Maritime Picture (RMP). Once again, it will be imperative that the data collected by these assets can be sent with ease to command centres to help populate national, or regional RMPs. While coastal ESMs can be networked using conventional telecommunications, microwave, cellular and/or fibre-optic links, electronic

support measures monitoring larger EEZs will probably need to share their data using V/UHF radio and/or SATCOM.

In terms of exploitable maritime traffic RF signals, vessels tend to rely on VHF maritime mobile band communications on frequencies of 156MHz to 174MHz which handles voice and data traffic. Vessels displacing over 300 tonnes, and all passenger ships, are mandated by the International Maritime Organisation's International Convention for the Safety of Life at Sea to use Automatic Identification System (AIS) transponders. AIS transmissions on frequencies of 161.975MHz and 162.025MHz share

details of a vessel's identity, location and voyage. BLOS and distress communications are provided by Medium Frequency (MF: 2.182MHz) and HF links. Like commercial air traffic, vessels at sea can employ L-band and Ku/Ka-band (14GHz uplink/10.9GHz to 12.75GHz downlink and 26.5GHz to 40GHz uplink/18GHz to 20GHz

downlink) SATCOM. It may be possible for ESMs to exploit UHF signals on frequencies of 450MHz to 470MHz which are used for onboard, handheld communications between crewmembers. In addition to MF signals, emergency position-indicating radio beacons (406MHz) and homing beacons (121.5MHz) can help locate vessels in distress. Regarding navigation, ships and marine craft may use S-band (2.9GHz to 3.1GHz) and X-band (9.2GHz to 9.5GHz) radars.

A lack of RF emissions from a maritime target may indicate a suspicious vessel. ESM information can be overlaid onto maritime radar tracks to provide information on a vessel. This is how AIS works by populating standard RMP tracks with information on individual vessels. A maritime track that is not emitting any AIS, communications and/or radar signals may indicate a ship that is trying to remain 'dark' i.e. not identifiable. Such a situation may be enough to warrant further investigation by coastguard or naval vessels.

Networked, wide-area RF sensing may also help provide early warning of ASHM attack. Several types of weapons employed by Houthi insurgents against shipping in the Red Sea rely on active RF emissions to reach their targets. For example, both the Al-Mandab-1/2 ASHMs rely on X-band Active Radar Homing (ARH) seekers to detect the metal hull of the targeted ship during a missile's end game. It is thought that the Rubezh (North Atlantic Treaty Reporting name SSC-3 Styx) and Sayyad ASHMs deployed by Houthi insurgents also rely on X-band ARH seekers. Netted, wide area ESMs within range may not only be capable of detecting X-band ASHM ARH emissions, but may also be capable of triangulating the missile's location if four or more networked ESMs are within range. If such information can be delivered early enough, it may provide the targeted vessel enough warning to take evasive action, or to prepare for impact.

Detecting targets at range is an important consideration for maritime domain awareness and coastal security. >>

JAMMING DETECTION

Marine and air navigation is at risk from deliberate GNSS PNT signal disruption which has become a growing problem in the Middle East in recent years. State and non-state actors around the region have found GNSS PNT jamming and spoofing to be a favoured method for protecting strategically important areas and politico-military and/or industrial installations from being targeted by GNSS-guided ordnance and/or UAVs.

The International Air Transport Association reported that deliberate GNSS PNT interference had increased by 175 percent in 2024, compared to the previous year. By the middle of 2024, around 1,500 flights per day were reporting incidences of GNSS PNT disruption over and around Iran, Iraq and Israel. Incidences of deliberate GNSS PNT disruption increased once more in 2025, this time by 500 percent. In the maritime environment 3,000 vessels experienced similar disruption in the Red Sea and Strait of Hormuz.¹⁷

GNSS PNT jamming and spoofing has both a safety and commercial impact on those targeted: Spoofing, where the timing element of an incoming PNT signal can cause a GNSS receiver to display false and/or misleading information to the user, risks degrading that user's situational awareness. This may cause potentially catastrophic navigation errors. To be fair, commercial aviation and shipping rarely relies on GNSS alone for navigation. Nonetheless, the loss of a reliable PNT signal through deliberate action is likely to increase bridge or cockpit stress. Capabilities like the Automatic Dependent System – Broadcast SSR architecture used in aviation and AIS rely in part on incoming PNT

signals received by the aircraft or ship. These signals are converted into coordinates which are transmitted to ATC and maritime control centres to give details of an aircraft or ship's identity, voyage and other behaviours. Transmitting this information, derived as it is from an incoming GNSS PNT signal, is particularly important when a ship or aircraft is beyond radar range.

GNSS PNT disruption can also have a commercial impact: Some airports rely on GNSS PNT signals to provide aircraft with approach vectors to land. Diverting a long-haul airliner to another airport because of such disruption can cost up to \$100,000 in extra fuel burn, landing fees, and accommodation and replacement flights for passengers. Global 'just in time' supply chains can be significantly inconvenienced should GNSS PNT jamming and spoofing slow vessels down or affect major international shipping lanes. It is noteworthy that when the MV Ever Given container ship was grounded in the Suez Canal in March 2021, she delayed over \$9 billion of goods per day until refloated. Some insurance companies may also demand higher premiums for vessels navigating areas where GNSS PNT jamming/spoofing is a major problem.¹⁸

Pinpointing the problem

Detecting, identifying and locating sources of deliberate GNSS PNT interference is imperative for two reasons: First, GNSS users within range of the jammer can be warned that PNT signals may be corrupted, compromised and/or unavailable. Fortunately, GNSS constellations like the United States' Global Positioning System, the European Union's Galileo, the People's Republic of China's Beidou and Russia's GLONASS constellations all transmit their PNT signals on a relatively narrow waveband of 1.1GHz to 1.6GHz. Deployed, wide-area, networked ESMs thus only need monitor a comparatively small slice of the radio spectrum to ascertain if jamming/spoofing is being performed. PNT jamming signals are often noticeably higher in strength compared to genuine PNT transmissions as they try to 'wash out' the comparatively weak PNT signals that reach Earth after a long journey through space. A relatively powerful PNT signal can be an initial indication that something is wrong. It may be relatively easy to spot a spoofing signal by comparing the GNSS PNT signal's output with what a clean signal should look like. As before, networking these ESMs will allow users to triangulate the point-of-origin of the jamming/spoofing signal. Second, with the point of origin determined, it may then be possible to use this evidence to make formal diplomatic representations to a state actor performing the GNSS disruption to request its cessation. Similarly, law enforcement and/or military action could be taken against non-state actors attacking GNSS PNT signals.

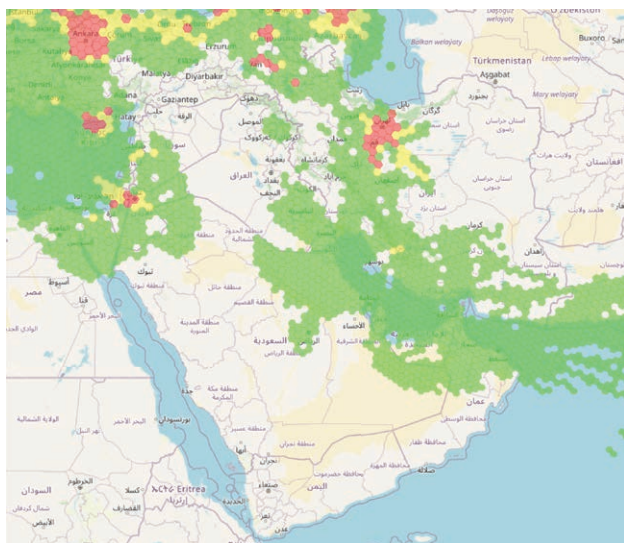


Image 5: Level of reported GPS interference across the Middle East on 04 February, 2026

IN BUILDING TECHNICAL SURVEILLANCE COUNTER MEASURES

Much of this report has hitherto focused on external threats to Middle East nations in the form of airborne and maritime threats. Nonetheless, governments, businesses and wealthy individuals in the region face security challenges from unauthorised surveillance. Covert operatives depend on the radio spectrum to conduct technical surveillance to steal secrets from defence, government and energy agencies, which need robust protection from hidden internet-of-things devices and smart technologies.

Covert listening devices can exploit the radio spectrum to share the Communications Intelligence (COMINT) they are collecting. This introduces a potential vulnerability which can be exploited by counterintelligence teams. Covert listening devices will record sounds, such as speech, within range. This sound is converted into electromagnetic signals; thence into radio waves. These radio waves are transmitted to whoever is performing the eavesdropping and collecting the COMINT. Older listening devices would use VHF signals which could penetrate walls and other structures. However, these systems needed relatively large antennas and were hence harder to hide and use covertly. Contemporary devices use UHF frequencies notably in the Global System for Mobile Communications band of 880MHz to 1.99GHz. These devices may also transmit their COMINT using Wi-Fi radio signals across a 2.4GHz to five gigahertz waveband, or via Bluetooth. Listening devices may transmit COMINT in real-time or using burst transmissions.

Real-time transmission provides near instantaneous intelligence to the eavesdropper, although can be relatively easy and quick to detect as the device will transmit whenever a sound is made in its locale. A counterintelligence team performing a sweep with a spectrum analyser should be able to detect local transmission spikes when the device is active with relative ease. Burst transmissions are harder to detect as the team will need to be performing the sweep at exactly the moment the listening device is making a transmission. This moment may last but a fraction of a second. The downside for the eavesdropper is that a burst transmission does not provide COMINT in real time.

For these reasons it may be prudent to deploy an array of ESMs around a building that continually hunt for, and analyse, signals that could be synonymous with listening devices performing real-time, or burst, transmissions. The networked sensors could simply alert a counterintelligence team when a signal of interest has been discovered, even if it is a burst transmission. Using several sensors may make it relatively easy to pinpoint where the device is located so that it can be removed. Employing an unattended network of sensors saves the expense in time and money of having a counterintelligence team regularly sweep a specific building or installation for listening devices.



BORDER SECURITY MONITORING

Taken together Egypt, Iran, Iraq, Israel, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, the UAE and Yemen had a combined land border of 22,931km (14,248 miles). Of this combined border length, up to 19,000km (11,800 miles), or 83 percent of the total, runs through desert, arid, mountainous and uninhabited areas. At the same time, many of these countries experience violations of their borders by people traffickers, smugglers, insurgents and other criminal elements. The border between Iran and Iraq experiences critical levels of money and narcotics trafficking. The frontier between Saudi Arabia and the UAE experiences people and narcotics trafficking, while that between Israel and Lebanon sees violations by insurgents and weapons trafficking. Egypt, meanwhile, experiences border violations by people traffickers moving migrants towards the European Union.²⁰

Many nations in the region are caught in a double bind: On the one hand, their borders can experience significant illegal activity, and on the other hand, local geography can make these borders hard to fortify. One option is to significantly enhance and enlarge border security forces. However, recruiting, training and equipping additional personnel can be a significant financial burden. Instead, it may be more prudent to invest in wide area networks of unattended ESMs that continually monitor the radio spectrum in their locale for suspicious signals. Once suspicious activity has been detected, local border forces can take a closer look at the situation, either by deploying a UAV or dispatching a patrol to the area of interest. The same passive sensor networks can be connected to C2 for national defence, air defence and homeland security intelligence.

As discussed above, criminals, like insurgents, depend on communications. Cellphones are one option to remain in contact, but sparsely populated areas, may be devoid of coverage. To put matters into perspective, the Empty Quarter which covers 650,000 square kilometres (250,966 square miles) of Oman, Saudi Arabia, the UAE and Yemen is estimated to have under five percent of cellphone coverage.

Radio at the frontier

A lack of cellular coverage forces people to use alternative options to keep in touch. Perhaps the most ubiquitous of these is SATCOM. Individuals can use satellite phones which may use a constellation like Iridium, Inmarsat or Thuraya (1.525GHz to 1.660.5GHz/3.4GHz to 6.725GHz);



Image 6: Multiple borders in the Middle East that experience border security violations

the latter providing good coverage over the Middle East and Africa. Other systems include Garmin InReach and Zoleo which provide two-way text messaging across the Iridium network. Enhancements like the Smartphone Satellite SOS capability installed in some recent smartphones enable emergency location and text messaging when the phone is out of standard cellular coverage. Some V/UHF civilian handheld radios may allow LOS communications in areas where cellular coverage is lacking. Handheld radio may be particularly useful, for example, if smugglers on one side of a border need to communicate with their counterparts on the other. Similarly, HF radio may provide longer-range BLOS links.

Unattended, networked ESMs monitoring these frequencies in isolated border areas could provide 'early warning' of suspicious behaviour near the frontier. Deploying several ESMs, and their receiving antennas, allows a signal of interest to be geolocated. Given how sparsely populated many of the border areas in the Middle East are, even the detection of a radio signal in an otherwise uninhabited area could trigger further investigation. Deploying a wide area sensing network near a border may have a deterrent effect deterring those wanting to violate the frontier from doing so lest they get caught. One alternative for such individuals is simply to not use any form of radio communications when near a border. However, this course of action risks making the illegal activity much harder to coordinate and more protracted to perform. An additional benefit is that the V/UHF frequencies deployed, netted sensors can monitor could support other tasks like the CUAV mission.

CONCLUSIONS & RECOMMENDATIONS

The Middle East faces an array of diverse defence and security challenges. Regional peace and prosperity depend on threats being detected and addressed in a timely fashion. The region's combined airspace is at risk from illicit UAV use. Its high seas are vulnerable to insurgent and illegal activity. Gaps in ATC coverage can be exploited by those bent on doing harm. Aviation and maritime safety, and hence regional prosperity, are at risk from deliberate GNSS PNT disruption. Domestic security is threatened by insurgent activity and espionage. Border areas in isolated, sparse locations can be vulnerable to criminal exploitation.

At first blush, it may appear that this complex set of interlocking threats can only be addressed by increasing military, border security and law enforcement expenditure. The traditional approach of recruiting and retaining skilled professionals, and equipping them accordingly, will always be important when combating such dangers. Nonetheless, technology has an important role to play in making these organisations ever more effective.

Wide-area, networked radio frequency monitoring can process threats at pace. All the security challenges listed above depend on exploiting the radio spectrum in some shape or form. Detecting, identifying, locating and sharing RF-derived threat information is instrumental in

achieving a timely response. A timely response may help prevent a manageable security challenge escalating into something worse.

These networks can be relatively inexpensive to procure and deploy. The training burden for personnel is light, thanks to the intuitive nature of contemporary and future ESMs and other RF sensors. Wide area sensor networks can perform work that may have required scores of personnel to do in the past. These networks can be monitored remotely and share their data with larger national, or regional IADS, vessel traffic services and/or law enforcement authorities. Furthermore, the networks' very deployment may have a deterrent effect against those who would otherwise have used the radio spectrum in the furtherance of illicit or illegal activities.

The Latin expression *Praemonitus Praemunitus* ('Forewarned is Forearmed') was a relevant maxim for the ancient warriors of Rome as they sought to counter the threats the empire continually faced. The term is relevant today for a region that faces a myriad of threats to its peace and prosperity. Fortunately, as this report has illustrated, monitoring the radio spectrum can help ensure countries around the region remain forewarned and forearmed as defence and security challenges continue.

ABOUT THE AUTHOR



Dr. Thomas Withington is an award-winning analyst and writer specializing in electronic warfare, radar and military communications; a Research Associate at the Royal United Services Institute and a Senior Non-Resident Associate Fellow at the NATO Defense College. He has written widely on these subjects for a range of specialist and general publications. He also works as a consultant and adviser in these areas for several leading government and private sector clients. Furthermore, Dr. Withington provides regular commentary on security and defense aspects of electromagnetic spectrum use for major media organizations around the world.

REFERENCES

- 1 'Drones, AI and Cyber-Jihad: The Future of Terrorism in the Middle East', 28th September 2025 @ <https://tacticsinstitute.com/middle-east/drones-ai-and-cyber-jihad-the-future-of-terrorism-in-the-middle-east/>, consulted 21st January 2026.
- 2 'Who are the Houthis and why is the US targeting them?', 25th March 2025 @ <https://www.bbc.com/news/world-middle-east-67614911>, consulted 21st January 2026.
- 3 'What is Hamas and why is it fighting with Israel in Gaza?', 14th October 2025 @ <https://www.bbc.com/news/articles/clyv7w3gdy2o>, consulted 21st January 2026.
- 4 Ali, MH, Najem, M, 'An Automated Occupation in South Lebanon', 4th November 2025 @ https://carnegieendowment.org/middle-east/diwan/2025/11/an-automated-occupation-of-south-lebanon?lang=en&utm_source=chatgpt.com, consulted 21st January 2026.
- 5 Bohbot, A, 'Rising Hamas drone activity sparks concern among IDF reservists', 5th June 2025 @ <https://www.jpost.com/israel-news/article-856621>, consulted 21st January 2026.
- 6 Doctor, AC, Rapid Review: The Logic of Terrorist Use of Unmanned Aerial Systems, Enabling Factors, and Barriers to Exploitation, (Omaha: University of Nebraska, 2025), page 8.
- 7 Conversation between the author and a Ukrainian CUAV expert, December 2025.
- 8 International Civil Aviation Organisation, Handbook on Radio Frequency Requirements for Civil Aviation, Second Edition, (Montreal: International Civil Aviation Organisation, 2021); Civil Aviation Authority, CAP 452: Aeronautical Radio Station Operator's Guide, (London: Civil Aviation Authority, 2016); US Department of Transportation, 'US Radio Frequency Bands Supporting Surface and Aviation Transportation', date unknown @ <https://www.transportation.gov/sites/dot.gov/files/docs/subdoc/441/usradiofreqbandssupportingtransportationexcel051020190240pm4000dpicmykprntwatermarkrev.pdf>, consulted 29th January 2026.
- 9 Civil Aviation Safety Authority Australia, 'Operational Notes on Distance Measuring Equipment', date unknown @ <https://www.casa.gov.au/sites/default/files/2021-09/operational-notes-of-distance-measuring-equipment-dme-booklet.pdf>, consulted 29th January 2026.
- 10 International Civil Aviation Organisation Middle East Region, Air Navigation Report 2024, (Montreal: International Civil Aviation Organisation, 2024), pages 7-8.
- 11 Flanders Maritime Institute, 'Maritime Boundaries Geodatabase: Maritime Boundaries and Exclusive Economic Zones', date unknown @ <https://www.marineregions.org/about.php>, consulted 2nd February 2026; Sea Around Us Project, 'Fisheries, Ecosystems and Biodiversity', 2nd February 2026 @ <https://www.seaaroundus.org/data/#/eez>, consulted 2nd February 2026; US Department of State, 'Limits in the Seas', date unknown @ <https://www.state.gov/limits-in-the-seas>, consulted 2nd February 2026.
- 12 International Energy Agency, 'Strait of Hormuz', June 2025 @ <https://iea.blob.core.windows.net/assets/760ed8e8-38b6-4418-b527-6d8976da72e4/StraitofHormuzFactsheet.pdf>, consulted 2nd February 2026.
- 13 United Nations Conference on Trade and Development, 2025 Review of Maritime Transport: Staying the course in turbulent waters, (New York: United Nations Publications, 2025), pages 33-62; International Monetary Fund, 'Port Watch', 2nd February 2026 @ https://portwatch.imf.org/datasets/42132aa4e2fc4d41bdaf9a445f688931_0/, explored, consulted 2nd February 2026.
- 14 Armed Conflict Location and Event Database, 'Interactive Map: Red Sea attacks', 2nd February 2026 @ <https://acleddata.com/platform/interactive-map-red-sea-attacks>, consulted 2nd February 2026.
- 15 Combined Maritime Taskforce 150, 'Public Release, November 19th 2024/8th January 2026 Update', date unknown @ <https://combined-maritimeforces.com/>, consulted 2nd February 2026; United Nations Office on Drugs and Crime, World Drug Report 2025, (New York: United Nations Publications, 2025), pages 42-48; United States Department of State, 2025 Trafficking in Persons Report, (Washington DC: US Department of State, 2025), pages 12-15.
- 16 Confidential discussion with anti-ship missile expert, 29th January 2026.
- 17 Joint Maritime Information Centre, 'JMIC Weekly Dashboard for the Middle East: Week 41 2025', 12th October 2025 @ https://mscio.eu/media/documents/JMIC_Week_41_Dashboard_06_October_-_12_October_2025_.pdf, consulted 2nd February 2026; Obiowo, C, 'Air-craft navigation system disruptions surge by 175% in 2024 - IATA', 26th February 2025 @ <https://nairametrics.com/2025/02/26/aircraft-navigation-system-disruptions-surge-by-175-in-2024-iata/>, consulted 2nd February 2026; 'Maritime GNSS Interference Worldwide: A Cumulative Analysis 2024', 24th October 2025 @ <https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/>, consulted 2nd February 2026.
- 18 Harper, J, 'Suez blockage is holding up \$9.6 billion of goods a day', 26th March 2021 @ <https://www.bbc.com/news/business-56533250>, consulted 2nd February 2026; 'GPS Jamming: A growing threat to aviation security', 15th September 2025 @ <https://internationalfinance.com/magazine/technology-magazine/gps-jamming-a-growing-threat-to-aviation-safety/>, consulted 2nd February 2026; 'Maritime GNSS Interference Worldwide: A Cumulative Analysis 2024', 24th October 2025 @ <https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/>, consulted 2nd February 2026; Maritime Administrator Republic of the Marshall Islands, Ship Security Advisory No. 09-25: Global Navigation Satellite System (GNSS) Interference, (Reston, VA: Republic of the Marshall Islands, 6th October 2025).
- 19 Central Intelligence Agency, 'The World Factbook - Land Boundaries', 2025 @ <https://www.cia.gov/the-world-factbook/field/land-boundaries/>, consulted 3rd February 2026.
- 20 United Nations Refugee Agency, 'Global Trends', 12th June 2025 @ <https://www.unhcr.org/global-trends>, consulted 3rd February 2026; Mansour, R, Al-Shakeri, H, 'The shape-shifting axis of resistance', March 2025 @ <https://www.chathamhouse.org/2025/03/shape-shifting-axis-resistance>, consulted 3rd February 2026; Menmy, DT, 'How is Iraq still a source of dollar smuggling to Iran and other neighbouring states?', 30th June 2025 @ <https://www.newarab.com/news/whats-driving-forward-us-dollar-smuggling-iraq-iran>, consulted 3rd February 2026.

SILVUS
TECHNOLOGIES
a Motorola Solutions Company

RFeye[®]

Silvus Technologies, a Motorola Solutions company, builds mission-critical capabilities that enable defense and security organizations to understand the electromagnetic environment, maneuver through the spectrum, and maintain an operational advantage in contested conditions. Through an interoperable ecosystem of industry-leading RFeye™ sensors, resilient tactical communications, and advanced electronic warfare capabilities, Silvus extends SIGINT to dismounted operators and uncrewed platforms—empowering forces to sense threats, connect forces, and command the spectrum. Together, these capabilities deliver the situational awareness and decision advantage needed to achieve spectrum superiority.



SILVUS
TECHNOLOGIES
a Motorola Solutions Company

Silvus Technologies UK Ltd
Unit 1, Bourn Quarter
Wellington Way
Cambridge
CB23 7FW

Silvus Technologies and RFeye are trademarks or registered trademarks of Silvus Technologies Inc. Copyright© 2026 Silvus Technologies. All rights reserved. No part of this document may be reproduced or distributed in any manner without the prior written consent of Silvus Technologies. The information and statements provided in this document are for informational purposes only and are subject to change without notice.



UK Certificate number: F5576625