INTELLIGENCE BRIEFING | MARITIME SECURITY • ELECTRONIC WARFARE • IRAN

THE INVISIBLE WAR: Iran's Cyberwarfare and Electronic-Warfare Campaign Against Shipping in the Strait of Hormuz

PREPARED BY	Msc. Criminology I Specialist in Intelligence Studies -National and Internal security – Organized crime I Risk Management expert: Pedro Barrueco Perez
PREPARED FOR	Executive and security decision-makers
DATE	24 July 2026
SCOPE	Open-source intelligence assessment; information current through 24 July 2026
CONFIDENCE	High on the existence and operational impact of interference; moderate on comprehensive attribution to Iran

BOTTOM LINE Iran does not need to close the Strait of Hormuz physically to disrupt it. By integrating navigation interference, communications manipulation, selective attacks, vessel seizures, mines, drones and fast craft, Tehran can create a functional blockade—raising uncertainty, insurance costs and operational risk while preserving ambiguity about responsibility.

Executive Summary

The Strait of Hormuz is becoming a laboratory for asymmetric maritime warfare. Commercial ships operating near Iran increasingly face an environment in which their electronic picture cannot be assumed to be true. Global Navigation Satellite System (GNSS) signals may disappear or report false positions; Automatic Identification System (AIS) tracks may become distorted; and unidentified actors may impersonate authorities over bridge-to-bridge radio. These disruptions do not merely inconvenience navigation. In a narrow and congested waterway, they can create collisions, groundings, misidentification, detention and escalation.

The available evidence supports a high-confidence judgment that GNSS/GPS, AIS and communications interference has repeatedly affected commercial shipping in the Persian Gulf, Gulf of Oman and Strait of Hormuz. Official maritime advisories documented significant jamming and spoofing in 2025 and again during the 2026 conflict. The geographic concentration of some interference near Bandar Abbas, Iran's demonstrated electronic-warfare capability and the strategic benefits to Tehran support a moderate-confidence assessment that Iran is responsible for, or deliberately benefits from, a meaningful portion of this activity. Publicly available evidence does not justify attributing every anomaly to Iran; regional militaries also employ defensive jamming, and technical attribution remains difficult (JMIC, 2025, 2026a, 2026b; MARAD, 2026; Reuters, 2025a).

Key Judgments

- Iran is integrating electronic warfare into a broader anti-access/area-denial strategy designed to make the strait unsafe, unpredictable and economically expensive without requiring a sustained conventional naval confrontation. High confidence.
- GNSS jamming and spoofing can degrade or falsify the position and timing data feeding shipboard navigation and AIS. The immediate consequences include loss of situational awareness, false tracks, navigational error and increased collision or grounding risk. High confidence.
- Iran can combine electronic interference with radio warnings, harassment, selective seizures and kinetic systems to shape vessel behavior and impose a de facto or selective blockade. Moderate-to-high confidence.
- The 2019 seizure of the British-flagged Stena Impero remains an important—but not conclusively attributed—case in which anomalous GPS/AIS data may have helped place or depict the vessel inside Iranian waters before its detention. Moderate confidence.
- The term cyberterrorism is too narrow and legally contentious for the full activity. Maritime electronic warfare, cyber-enabled coercion and hybrid maritime operations are more accurate. Cyberterrorism may apply only where intent, political coercion and serious harm satisfy a recognized terrorism definition. High confidence.

Intelligence Question and Analytic Framework

This briefing addresses whether Iran uses electronic warfare and cyber-enabled methods as part of an asymmetric doctrine against commercial and military vessels around the Strait of Hormuz, and how those methods could disrupt maritime operations. The assessment draws on

official maritime advisories, government and military publications, academic and professional studies, shipping intelligence, cybersecurity analysis and reputable news reporting.

TERMINOLOGY Jamming overwhelms legitimate satellite signals. Spoofing transmits counterfeit signals that generate a false position or time. AIS manipulation changes or corrupts reported vessel identity, position or movement. A cyberattack compromises software, networks or data. These mechanisms can be coordinated, but they are not technically identical.

The Threat Environment

Persistent navigation and communications interference

Warnings to commercial shipping predate the current conflict. U.S. maritime advisories in 2019, 2021 and 2023 cautioned vessels in the Persian Gulf and Strait of Hormuz that they could encounter GPS interference, AIS spoofing, bridge-to-bridge communications spoofing and other forms of jamming with little warning (MARAD, 2019, 2021, 2023). The repetition of these warnings indicates a persistent regional hazard rather than a single isolated episode.

The threat intensified sharply during the June 2025 Iran–Israel confrontation. JMIC reported significant electronic interference throughout the strait and wider Gulf, including activity apparently originating around Bandar Abbas. Shipping analytics indicated that hundreds—and on some days more than one thousand—vessels experienced anomalous positioning. Tankers appeared electronically in impossible locations, including rural Russia and inland Iran (JMIC, 2025; Reuters, 2025a; Financial Times, 2025).

During March 2026, JMIC and UK Maritime Trade Operations assessed the regional operational risk as critical and reported sophisticated GPS jamming and electronic interference affecting navigation and communications around Hormuz. The U.S. Maritime Administration likewise warned of significant GNSS interference, spoofing and jamming and urged vessels to cross-check electronic systems with radar ranges, visual bearings and independent navigation methods (JMIC, 2026a, 2026b; MARAD, 2026).

Operational effects on ships

Method	Immediate effect	Operational consequence
GNSS/GPS jamming	Loss or degradation of position and timing	Manual navigation, route delay, increased collision and grounding exposure
GNSS/GPS spoofing	Plausible but false coordinates	Unnoticed deviation, false territorial-water incursion or misrouting
AIS distortion	Incorrect identity, position, course or speed	Misidentification, flawed traffic picture and unreliable transit analysis
Radio spoofing	False instructions from an apparent authority	Diversion, delay, coercion or movement into a vulnerable area

Network intrusion	Compromised bridge, cargo, communications or port systems	Operational shutdown, data manipulation, extortion or sabotage

Assessment synthesized from MARAD (2023, 2026), NDU Press (2024), Cambridge University Press (2024) and JMIC (2026a).

Evidence and Attribution

The Stena Impero precedent

Iran's July 2019 seizure of the British-flagged tanker Stena Impero is frequently cited as a possible example of combined positioning manipulation and maritime coercion. Lloyd's List Intelligence identified unusual AIS messages consistent with the possibility that GPS data feeding the vessel's AIS had been spoofed. The ship subsequently turned toward, or appeared to enter, Iranian territorial waters and was seized by the Islamic Revolutionary Guard Corps Navy (IRGCN). NDU Press and the NATO Cooperative Cyber Defence Centre of Excellence later used the incident as a case study in the weaponization of position, navigation and timing data (Lloyd's List, 2019; NDU Press, 2024; CCDCOE, 2021).

The case is strategically important but analytically incomplete. Public data do not conclusively identify the transmitter or prove Iranian control of the spoofing. It should therefore be presented as a probable or plausible enabling operation—not as a technically proven Iranian cyberattack.

2025–2026 escalation

The volume and geographic spread of later interference strengthen the assessment that electronic warfare is no longer peripheral to Gulf maritime security. In June 2025, approximately 1,000 vessels were reportedly affected during the sharpest surge. The tanker Front Eagle showed impossible movements in tracking data before colliding with Adalynn near the strait; investigators did not establish jamming as the cause, but the incident illustrated the danger of degraded positional integrity (Reuters, 2025b, 2025c; Financial Times, 2025).

In 2026, maritime advisories described interference across the Arabian Gulf, Gulf of Oman and Hormuz approaches as sophisticated and persistent. Commercial tracking platforms displayed vessels moving in unnatural straight lines or clustering at false coordinates. Such patterns are consistent with large-area jamming or spoofing, but they do not independently identify Iran as the originator (JMIC, 2026a; gCaptain, 2026).

Attribution assessment

Indicator	Assessment	Weight
Geographic concentration	Interference has been observed near Iran's coast and Bandar Abbas, a major Iranian naval hub.	**Supports**
Capability and doctrine	Iran publicly trains for electronic warfare and fields relevant maritime, drone and coastal systems.	**Supports**

Strategic benefit	Interference increases risk, conceals activity and discourages transit without requiring overt closure.	**Supports**
Historical behavior	Iran has seized, harassed and selectively targeted commercial vessels to create leverage.	**Supports**
Regional countermeasures	Other states also jam signals to protect forces from drones and missiles.	**Limits**
Technical opacity	Open sources rarely provide transmitter geolocation, waveform data or forensic access.	**Limits**

Analytic judgment based on the totality of publicly available reporting; not a technical attribution finding.

Iran's Asymmetric Maritime Doctrine

Iran's conventional navy cannot match the United States in a fleet-on-fleet engagement. Its answer is an asymmetric model built around geography, dispersion, surprise and cost imposition. The Office of Naval Intelligence describes the IRGCN as emphasizing asymmetric doctrine in the Persian Gulf. Its toolkit includes fast attack craft, coastal missiles, mines, submarines, drones, distributed sensors and the ability to harass or seize merchant vessels. Professional and academic studies similarly characterize the IRGCN as seeking to exhaust a superior opponent, complicate decision-making and control escalation below the threshold of decisive war (Office of Naval Intelligence, 2017; Fondation pour la Recherche Stratégique, 2024; Levy, 2026).

Electronic warfare is a natural extension of this doctrine. It is relatively inexpensive, scalable and difficult to attribute in real time. Its effects can be amplified through physical pressure: a vessel whose navigation picture is degraded is more vulnerable to radio deception, fast-craft interception, drone surveillance, boarding or accusations that it violated Iranian waters.

ANALYTIC JUDGMENT Iran's objective is not necessarily to make every ship lose navigation. It is to make every captain, insurer and naval commander doubt whether the electronic picture can be trusted. That uncertainty itself becomes a weapon.

Cyberterrorism or Electronic Warfare?

Calling the campaign cyberterrorism may be rhetorically powerful, but it risks conceptual imprecision. Most GPS jamming is electronic warfare because it attacks the electromagnetic spectrum rather than penetrating a computer network. Spoofing occupies a boundary area: it injects false data into digital navigation systems but may do so through radio-frequency transmission rather than network intrusion. AIS manipulation can arise from spoofed GNSS data, altered transponder inputs or deliberate identity deception.

Cyberterrorism normally requires a politically or ideologically motivated cyber operation intended to intimidate or coerce, typically involving serious harm, disruption or fear. The available evidence more clearly supports the labels maritime electronic warfare, cyber-enabled

coercion, gray-zone operations and hybrid maritime warfare. Cyberterrorism could become appropriate if investigators demonstrated deliberate Iranian cyber intrusion intended to cause civilian casualties, catastrophic vessel accidents or terror-driven coercion.

Threat Outlook: Next 6–12 Months

- Interference will probably remain episodic but surge during military escalation, naval exercises, convoy operations or threats against Iranian coastal infrastructure.
- Iran is likely to combine electronic interference with selective enforcement: warning some ships, permitting favored traffic and threatening vessels linked to adversarial states.
- AIS data will become less reliable for intelligence and commercial risk assessment as vessels disable transmitters, manipulate identity messages or operate under degraded GNSS conditions.
- A major collision or grounding caused—or believed to have been caused—by spoofing could trigger rapid escalation even if attribution remains uncertain.
- Iranian partners may adapt similar techniques in the Red Sea and Bab al-Mandeb, extending the electronic threat across a wider network of maritime chokepoints.

Indicators and Warnings

- Sudden clusters of vessels appearing at identical inland or airport coordinates.
- Multiple ships reporting simultaneous loss of GPS, Galileo, BeiDou or timing data.
- AIS tracks showing impossible speeds, straight-line convergence or abrupt geographic jumps.
- Radio instructions from unidentified entities claiming to represent Iranian, U.S. or coalition authorities.
- Iranian exercises deploying EW equipment, reconnaissance drones or communications units near Bandar Abbas, Qeshm, Abu Musa or the Nazeat Islands.
- Increased IRGCN patrols synchronized with GNSS anomalies or restrictions on particular flags, owners or cargoes.
- Vessels transmitting nationality or ownership messages intended to signal neutrality or protected status.

Implications and Recommendations

For ship operators

- Treat GNSS and AIS as inputs to be verified, not as a single source of truth. Cross-check radar, visual bearings, depth soundings, inertial systems and independent receivers.
- Establish bridge procedures for loss, drift or contradiction of position data; drill manual plotting and degraded-navigation scenarios.
- Verify unusual VHF instructions through known reporting channels and record audio, time, frequency and claimed identity.
- Preserve electronic logs, screenshots, receiver alarms and raw AIS/GNSS data to support later attribution.

- Coordinate route, insurance, naval liaison and crisis-communications decisions before approaching the strait.

For governments and maritime-security organizations

- Expand regional sensor networks capable of geolocating interference sources and distinguishing jamming from spoofing.
- Create a protected mechanism for operators to submit raw navigation and radio-frequency data quickly.
- Issue common attribution standards that separate confirmed Iranian activity from conflict-related defensive jamming.
- Develop resilient position, navigation and timing alternatives, including terrestrial backups and authenticated signals.
- Integrate electronic-warfare incidents into maritime escort, deconfliction and crisis-escalation planning.

Conclusion

The invisible contest around the Strait of Hormuz is already affecting real ships, crews and markets. Iran's most effective maritime weapon may not be a missile or mine, but uncertainty: uncertainty about a ship's position, the identity of the voice on the radio, the reliability of a digital track and the origin of the interference. Used alongside drones, mines, coastal missiles, fast craft and vessel seizures, that uncertainty allows Tehran to translate limited conventional naval power into disproportionate strategic influence.

The evidence does not support attributing every GPS anomaly in the Gulf to Iran, nor does it justify treating all electronic warfare as cyberterrorism. It does support a more disciplined conclusion: electronic and cyber-enabled disruption has become an important component of the asymmetric contest for Hormuz. For commercial shipping, the operational requirement is therefore clear—navigate as if the digital picture may be manipulated, preserve evidence and prepare to operate safely when satellite navigation cannot be trusted.

References

Cambridge University Press. (2024). “Maritime cyber threats.” In Marine Technology, Ocean Development and the Law of the Sea. https://www.cambridge.org/core/books/marine-technology-ocean-development-and-the-law-of-the-sea/maritime-cyber-threats/C1455D83F2AE46587371DFA8EB92E815

Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2021). Cyber interference against vessels in the Persian Gulf and Gulf of Oman (2019). https://cyberlaw.ccdcoe.org/wiki/Cyber_interference_against_vessels_in_the_Persian_Gulf_and_Gulf_of_Oman_(2019)

Financial Times. (2025, June 17). Visual analysis: GPS interference raises risk of accidents in Strait of Hormuz. https://www.ft.com/content/ac3c571f-2c4e-4c57-b582-21e2b27170f8

Fondation pour la Recherche Stratégique. (2024, May 6). The IRGC Navy’s long-term strategy of asymmetrical warfare. https://www.frstrategie.org/en/publications/notes/irgc-navy-s-long-term-strategy-asymmetrical-warfare-2024

gCaptain. (2026, March 10). Electronic fog of war: GPS spoofing distorts ship traffic near Hormuz. https://gcaptain.com/electronic-fog-of-war-gps-spoofing-distorts-ship-traffic-near-hormuz/

Joint Maritime Information Center (JMIC). (2025, June 22). Week 25 regional dashboard, 16–22 June 2025. UK Maritime Trade Operations. https://www.ukmto.org/-/media/ukmto/products/jmic-week-25-dashboard-16-june---22-june-2025.pdf

Joint Maritime Information Center (JMIC). (2026a, March 8). Advisory note: Regional maritime threat environment. UK Maritime Trade Operations. https://www.ukmto.org/-/media/ukmto/products/update-008---jmic-advisory-note-08_mar_2026_final.pdf

Joint Maritime Information Center (JMIC). (2026b, March 24). Update 023 to JMIC advisory note. UK Maritime Trade Operations. https://www.ukmto.org/-/media/ukmto/products/update-023---jmic-advisory-note-24-mar_final.pdf

Joint Maritime Information Center (JMIC). (2026c, April 12). Update 031 to JMIC advisory note. UK Maritime Trade Operations. https://www.ukmto.org/-/media/ukmto/products/update-031---jmic-advisory-note-12-april_final.pdf

Levy, D. (2026). The doctrine of the Iranian Revolutionary Guard Corps Navy: An advanced practitioner of asymmetric naval warfare. Journal of Strategic Studies. https://doi.org/10.1080/01402390.2025.2598757

Lloyd’s List. (2019, August 16). Seized UK tanker likely ‘spoofed’ by Iran. https://www.lloydslist.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran

National Defense University Press. (2024, February 15). Position, navigation, and timing weaponization in the maritime domain. Joint Force Quarterly, 112. https://ndupress.ndu.edu/Joint-Force-Quarterly/Joint-Force-Quarterly-112/Article/Article/3678180/position-navigation-and-timing-weaponization-in-the-maritime-domain-orientation/

Office of Naval Intelligence. (2017). Iran’s naval forces: A tale of two navies. U.S. Navy. https://www.oni.navy.mil/Portals/12/Intel%20agencies/iran/Iran%20022217SP.pdf

Reuters. (2025a, June 16). Shipping disruption surges around Hormuz amid Israeli-Iranian conflict. https://www.reuters.com/world/uk/ukmto-warns-rising-electronic-interference-gulf-strait-hormuz-2025-06-16/

Reuters. (2025b, June 17). Oil tankers near Iran appear to be in rural Russia as signals jammed. https://www.reuters.com/world/middle-east/oil-tankers-near-iran-appear-be-rural-russia-signals-jammed-2025-06-17/

Reuters. (2025c, June 17). Two oil tankers collide and catch fire near Strait of Hormuz. https://www.reuters.com/world/middle-east/uk-maritime-firm-says-it-is-aware-incident-east-uaes-khor-fakkan-2025-06-17/

U.S. Maritime Administration (MARAD). (2019). Advisory 2019-012: Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, and Red Sea—Threats to commercial vessels. https://www.maritime.dot.gov/msci/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels

U.S. Maritime Administration (MARAD). (2021). Advisory 2021-001: Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea, Gulf of Aden, and Indian Ocean. https://www.maritime.dot.gov/msci/2021-001-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-gulf-aden-and-indian-ocean

U.S. Maritime Administration (MARAD). (2023). Advisory 2023-011: Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Gulf of Aden, Bab al-Mandeb Strait, and Red Sea. https://www.maritime.dot.gov/msci/2023-011-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-gulf-aden-bab-al-mandeb-strait-red

U.S. Maritime Administration (MARAD). (2026, March 13). Advisory 2026-004: Persian Gulf, Strait of Hormuz, and Gulf of Oman—Iranian attacks on commercial vessels. https://www.maritime.dot.gov/msci/2026-004-persian-gulf-strait-hormuz-and-gulf-oman-iranian-attacks-commercial-vessels

Westbrook, T. (2023). Radiofrequency interference strategies targeting marine navigation systems. Journal on Baltic Security. https://journalonbalticsecurity.com/journal/JOBS/article/114