Republic of the Marshall Islands

MARITIME ADMINISTRATOR

11495 COMMERCE PARK DRIVE, RESTON, VIRGINIA 20191-1506
TELEPHONE: +1-703-620-4880 FAX: +1-703-476-8522
EMAIL: marsec@register-iri.com WEBSITE: www.register-iri.com

SHIP SECURITY ADVISORY No. 09-25

To: **Owners/Operators, Masters, Company Security Officers, Recognized Security Organizations**

Subject: **GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) INTERFERENCE**

Date: **6 October 2025**

This Ship Security Advisory (SSA) supersedes SSA No. 04-24.

Vessel operators should be aware of the escalating risks posed by GNSS interference in the following regions:

- Asia (including the East China Sea, South China Sea, Yellow Sea, and Taiwan Strait);
- Baltic Sea (including the Gulf of Finland and Gulf of Gdansk);
- Middle East (including the Arabian Sea, Red Sea, Arabian/Persian Gulf, Gulf of Oman, and Strait of Hormuz); and
- Eastern Mediterranean Sea.

These forms of interference, often linked to geopolitical tensions and electronic warfare activities, disrupt positioning, navigation, and timing information, potentially leading to navigational errors, operational delays, and safety hazards. Incidents of GNSS interference have surged since 2022, with reports of thousands of vessels impacted in 2025.

This SSA provides region-specific threat assessments, followed by comprehensive measures to mitigate the risks posed by GNSS interference. Vessel operators are urged to implement redundant navigation protocols, report incidents promptly, and consult updated navigational warnings from authorities such as the United States (US) Coast Guard Navigation Center (NAVCEN) and the North Atlantic Treaty Organization (NATO) Shipping Centre (NSC).

1.0 Regional Threat Assessments

1.1 **Asia** (including the East China Sea, South China Sea, Yellow Sea, and Taiwan Strait)

.1 **Overall Threat Level: Substantial**, with increasing frequency and sophistication, particularly in the South China Sea and near the Korean Peninsula.

This SSA is evaluated annually by the RMI Maritime Administrator (the "Administrator") and expires one year after its issuance or renewal unless otherwise noted, superseded, or revoked.

Asia, particularly the South China Sea, East China Sea, and waters near the Korean Peninsula, has seen a surge in GNSS interference since 2023, driven by geopolitical tensions over territorial disputes and North Korean activities. Jamming and spoofing have occurred near the Spratly Islands, Taiwan Strait, and Yellow Sea. Automatic Identification System (AIS) spoofing has been reported near Subi Reef and Mischief Reef, and North Korea's jamming from Haeju has disrupted South Korean shipping lanes.

.2 **Associated Risks**: In the South China Sea (handling 30% of global trade), spoofing may cause vessels to deviate into disputed waters, escalating diplomatic tensions. Jamming disrupts AIS and Electronic Chart Display and Information System (ECDIS), increasing collision risks in congested routes like the Malacca Strait. Security concerns include potential military escalations, with North Korean jamming linked to missile tests. Economic impacts involve trade delays and higher insurance costs, while safety risks include false positional data in high-traffic areas.

The interference affects all major GNSS constellations (Global Positioning System (GPS) (US), Galileo (European Union), GLONASS (Russia), BeiDou (China), with multi-constellation jamming and sophisticated spoofing increasing in complexity. These disruptions are often persistent, with daily impacts in high-traffic areas.

1.2 **Baltic Sea** (including the Gulf of Finland and Gulf of Gdansk)

.1 **Overall Threat Level: Severe**, with near-daily occurrences and expanding coverage.

The Baltic Sea, including the Gulf of Finland, Gulf of Gdansk, and areas near Kaliningrad, has emerged as a major GNSS interference hotspot since late 2023, with Russian sources in Kaliningrad Oblast (e.g., Tobol systems and Baltic Fleet) reportedly responsible for daily disruptions.

Gdynia Maritime University and GPSPATRON studies detected 84 hours of interference from June to November 2024, with 29 hours in October 2024 alone, including multi-tone jamming from mobile maritime sources. Finland's Coast Guard notes constant disturbances since April 2024. EASA and GPSJAM.org map persistent jamming from Kaliningrad, impacting over 5,800 vessels in the second quarter of 2025.

.2 **Associated Risks**: In this enclosed sea with heavy traffic and shallow waters, disruptions increase grounding and collision hazards, particularly near ports like Gdansk and Helsinki. AIS anomalies could mislead traffic, while spoofing causes position errors. Safety risks include false alarms and degraded situational awareness, with security implications from Russian hybrid warfare tactics. Economic effects involve port delays and higher operational costs, compounded by NATO-Russia tensions.

1.3 **Middle East** (including the Arabian Sea, Red Sea, Arabian/Persian Gulf, Gulf of Oman, and Strait of Hormuz)

.1 **Overall Threat Level: Substantial**, with potential for escalation amid regional instability.

The Middle East region experiences persistent GNSS interference, exacerbated by conflicts such as those involving Israel and Iran, and Houthi aggression in the Red Sea. Jamming and spoofing incidents have intensified since June 2025, following Israeli airstrikes on Iranian targets and retaliatory actions.

The Joint Maritime Information Centre (JMIC) reports severe disruptions affecting vessels, with circular spoofing patterns observed off Haifa and anomalies near Sudan's coast.

Windward AI data indicates that approximately 970 ships per day were affected in the Arabian Gulf and Strait of Hormuz in June 2025, up from zero in the fourth quarter of 2024 to 890 in the second quarter of 2025. Open-source intelligence points to electronic warfare systems like those near the Port of Bandar Abbas, Iran, as primary sources.

.2 **Associated Risks**: Navigational errors may cause groundings or collisions in congested chokepoints like the Strait of Hormuz, a critical route for global oil trade. A notable incident involved the container ship MSC ANTONIA running aground in the Red Sea on 10 May 2025, due to signal spoofing. Other operational disruptions include unreliable AIS data, which could contribute to misidentified vessel positions and increased collision risks. Safety implications are heightened by potential spillover from military actions, with secondary effects on timing-dependent systems like cargo handling. Economic impacts include route deviations and rising insurance premiums, while security risks involve masking illicit activities such as sanctions evasion.

1.4 **Eastern Mediterranean Sea**

.1 **Overall Threat Level: Substantial**, with frequent and intensifying incidents.

The Eastern Mediterranean Sea, including areas near Cyprus, Syria, Turkey, and the coasts of Israel and Lebanon, has seen a sharp rise in GNSS disruptions since Russia's invasion of Ukraine in 2022, with spillover from Middle Eastern conflicts. Reports from NAVCEN and GPSJAM.org highlight jamming near Port Said, Egypt, the Suez Canal, and Jeddah Port, Saudi Arabia, with over 117 vessels spoofed to Beirut-Rafic Al Hariri Airport on 4 April 2024.

By the second quarter of 2025, interference also affected vessels off Sudan's coast, extending to the Eastern Mediterranean. Israeli air bases have been identified as sources of widespread spoofing, impacting civilian aviation and maritime traffic. The European Union Aviation Safety Agency (EASA) notes persistent jamming and spoofing in this region, often tied to defense against drones and missiles.

.2 **Associated Risks**: In this high-traffic area, disruptions could lead to deviations into hazardous waters or restricted zones, increasing collision and grounding probabilities. AIS spoofing creates false vessel tracks, complicating traffic management and potentially enables illicit operations. Safety concerns include false terrain warnings and system alarms on vessels, while security risks involve broader electronic warfare.

1.5 Black Sea

.1 **Overall Threat Level:** **Severe**, due to ongoing conflict and targeted electronic warfare.

The Black Sea region, particularly near Crimea, ports of Gelendzhik and Novorossiysk, and Ukrainian borders, faces severe GNSS interference attributed to Russian electronic warfare, intensified since the 2022 Ukraine invasion. Open-source intelligence reveals jamming systems near Gelendzhik causing vessels to display inland positions, with 227 cargo ships spoofed to multiple inland sites on 4 April 2024.

Windward AI reports persistent disruptions, including multi-constellation jamming affecting all major GNSS systems.

.2 **Associated Risks**: Navigational inaccuracies in this area of conflict heighten collision and grounding risks, especially in shallow waters. Spoofing could mislead vessels into restricted zones, exacerbating geopolitical tensions. Operational disruptions affect dynamic positioning and timing systems, while safety implications include unreliable AIS in support of collision avoidance. Security risks are acute, with interference potentially concealing military movements or enabling sanctions-related activities by some vessels. Economic impacts include delayed grain and oil shipments, which are critical for global food security.

2.0 Mitigation Measures

To safeguard against GNSS interference, RMI-flagged vessels should adopt the following measures, consistent with industry best management practices and IMO guidelines:

2.1 Implement Navigational Redundancy

.1 Employ alternative positioning sources in high-threat areas, including Inertial Navigation Systems (INSs), celestial navigation, radar parallel

indexing, and visual fixes with landmarks. Cross-verify GNSS data against these to detect anomalies.

.2 Maintain updated paper charts as relevant, and ensure the ECDIS is configured for manual dead reckoning positions and speed log inputs during disruptions.

.3 Integrate multi-constellation/multi-frequency GNSS receivers (e.g., GPS, Galileo, GLONASS, etc. for improved resilience.

2.2 Monitor and Detect Interference

.1 Use receivers with anti-jamming/spoofing features, such as Controlled Reception Pattern Antennas (CRPA), Receiver Autonomous Integrity Monitoring (RAIM), and signal authentication.

.2 Monitor for indicators like sudden position jumps, Horizontal Dilution of Precision (HDOP) values above 2 with inconsistent tracks, discrepancies between radar overlay and ECDIS, or echo-sounder depth mismatches.

.3 Install interference monitoring tools for real-time detection and classification.

2.3 Crew Training and Procedures

.1 Conduct regular drills simulating GNSS interference, including bridge team briefings on response procedures. Train crew to recognize spoofing (e.g., abnormal speed increases) versus jamming (signal loss alarms).

.2 Augment bridge watches in high-threat areas, adding extra officers for manual plotting and radar monitoring. Avoid over-reliance on AIS; turn off overlays if anomalies appear.

.3 Plan routes with buffers around known high-threat areas, consulting Navigational Warnings (NAVWARNs) from the United Kingdom Hydrographic Office (UKHO) or the National Geospatial-Intelligence Agency (NGA), and coordinate with port authorities for daylight arrivals.

2.4 Report and Share Intelligence

.1 Share incident details with the RMI Maritime Administrator (the "Administrator"), UKMTO, and NSC for collective awareness. Refer to MARSEC-210 for contact information.

.2 Participate in regional monitoring networks (e.g., Baltic R-Mode) and any international efforts for resilient position, navigation and timing information.

2.5 Operational Planning and Technology Adoption

.1 Develop a GNSS disruption response plan , including reversion to non-GNSS aids like eLoran or R-Mode where available (e.g., Baltic Sea trials).

.2 Report incidents immediately to NAVCEN and NSC, providing latitude/longitude, time, duration, and screenshots.

.3 Consider installing advanced solutions such as anti-jamming/spoofing systems or independent backup time and location information systems.

3.0 Additional Information

3.1 Updated international industry association guidance on GNSS Jamming and Spoofing has recently been published.

3.2 Vessel operators are encouraged to review this SSA along with industry association guidance and integrate these measures into their operations.