Beazley Logo

Article

Navigating spoofing: Securing the future of maritime resilience

Maritime operations are sailing into a digital storm

The industry’s dependence on Global Navigation Satellite Systems (GNSS) for positioning, navigation, and timing (PNT) has created critical vulnerabilities that few can afford to ignore. Civilian GNSS signals are low-power, unauthenticated, and alarmingly easy to disrupt - a vulnerability that adversaries are already exploiting.

In politically charged waters (from the Baltic and Black Seas to the Red Sea and the Arabian/Persian Gulf) reports of jamming and spoofing attacks are increasing.

This is a growing operational reality that extends across navigation systems and the Automatic Identification System (AIS). And the consequences stretch far beyond simple signal loss: delays, collision risk, operational legal costs and fines.

GNSS interference: when safe passage goes adrift

GNSS interference is a direct threat to safety and operational continuity. When jamming strikes (where there is no signal), the fallout is immediate: positions vanish, Electronic Chart Display and Information Systems (ECDIS) default to dead reckoning, alarms can blare, and timing-dependent communications and systems falter. In restricted waters, that disruption can delay or abort operations, cause congestion, resulting in financial loss. These disruptions can also compound navigational risk, leading to grounding, collisions, traffic separation scheme breaches and environmental risk.

But the real danger lies in what you don’t see. Spoofing (fake GPS signals) and meaconing (delayed real GPS signals) are silent saboteurs. By injecting false yet plausible data, they trick GNSS receivers into reporting phantom positions. Autopilots, dynamic positioning systems, and AIS logic start making decisions based on inaccurate information.

Collision avoidance calculations can fail. ECDIS displays become erratic. Meaconing goes further, rebroadcasting authentic signals with a delay, creating a flicker between truth and fiction that undermines trust in navigational input.

And when trust collapses, AIS becomes a liability. Compromised GNSS means AIS broadcasts false positions and timestamps. When this false position is recorded as reality, the operational consequences can be significant. For example, vessels recorded as entering sanctioned waters can create liabilities that are not easily rectified, rendering a vessel untradable and often incurring significant costs and legal fees.

Turning the tide on disruption

The signal environment is increasingly contested, and maritime operators who rely on a single layer of defence are increasing their risks. However, resilience is achievable through a layered, disciplined approach.

Start with the fundamentals: multi-constellation, multi-frequency receivers. When one source is compromised, these systems keep positioning alive. Pair that with anti-jam antennas to suppress horizon-based jamming. Even something as basic as smart antenna placement, using ship structures to shield against low-angle interference, can make the difference between continuity and chaos.

Detection matters just as much as defence: Commercial GNSS receivers with spoofing and interference alerts give crews early warning of anomalies like sudden signal strength shifts or timing jumps, which are critical for fast response. Adding receiver autonomous integrity monitoring and advanced integrity checks to verify signal consistency and expose spoofing attempts before they corrupt navigation logic.

In terms of contingency: GNSS receivers have the capability to track multiple signal providers (such as GPS, Galileo, GLONASS) across multiple frequencies, improving resilience. This allows continuous checks within systems reducing the likelihood of impact on Position Navigation Timing (PNT) systems.

Finally, true resilience is rooted in culture: Beyond physical system enhancements, disciplined incident reporting under IMO guidelines ensures interference events feed into Safety Management Systems, which then feed into flag state and SOLAS reporting mechanisms, strengthening the entire sector's intelligence.

Anchoring certainty in cyber coverage

The Association of Average Adjusters (AAA) has brought much-needed attention to a lack of clarity in maritime insurance in a recent discussion paper: the ambiguity surrounding coverage for GNSS spoofing and jamming. Most traditional marine policies use language to exclude cyber where there is intent to do harm. However, in practice, these signal attacks often affect whole regions and aren't necessarily aimed at any one vessel. This broad language means ship operators can't always be sure their losses will be covered, making it more

important than ever to have insurance that’s designed to protect in today’s digital maritime world and the increasing geopolitical uncertainty.

Bottom line

GNSS vulnerabilities can’t be eliminated, but they can be contained. The maritime sector must piece together a mosaic of resilient receivers, intelligent monitoring, robust hardware, alternative navigation methods, proactive reporting and insurance coverage that addresses spoofing and jamming. This is how the maritime sector can charter a safer course through waters increasingly clouded by signal threats.

Discover Beazley’s **Cyber Defence for Marine**.

Beazley delivers protection designed for marine operators facing cyber risk. Our solution provides affirmative Hull & Machinery coverage, loss of hire indemnity for cyber risks including the impacts of GNSS incidents. Combined with Beazley’s traditional cyber and proactive security services it covers the full range of risks, reducing exposure and maintain operational continuity. It’s a clear, structured approach to safeguard assets and revenue when systems are compromised.

Home

©Beazley Group | LLOYD's Underwriters