



Information Provided by Trident Group America, Inc

THE DEAD RECKONING SOLUTION

GPS/GNSS Spoofing and the Cyber Threat That Can Sink Ships



THE THREAT IS REAL

GPS/GNSS spoofing is increasing—deceptive signals can quietly divert vessels off course.



THE RISKS ARE HIGH

Navigational deception can lead to groundings, collisions, port disruption, and catastrophic loss.



THE SOLUTION IS PROVEN

Dead reckoning—backed by disciplined navigation and resilient systems—keeps you on the true course.

When signals lie, dead reckoning tells the truth.
TRUST YOUR SKILLS. VERIFY. NAVIGATE. ARRIVE.





THE NEW MARITIME CYBER THREAT

GPS/GNSS Spoofing: From Theoretical Weakness to Operational Hazard



1. FEB 28, 2026 INCIDENT:

1,100+ vessels in UAE, Qatari, Omani, and Iranian waters lost reliable GPS, displaying false positions (e.g., over land, at airports).



2. GPS JAMMING & SPOOFING:

Signals overrode legitimate satellite transmissions, causing vessels to navigate on fabricated data, not just lost signals.



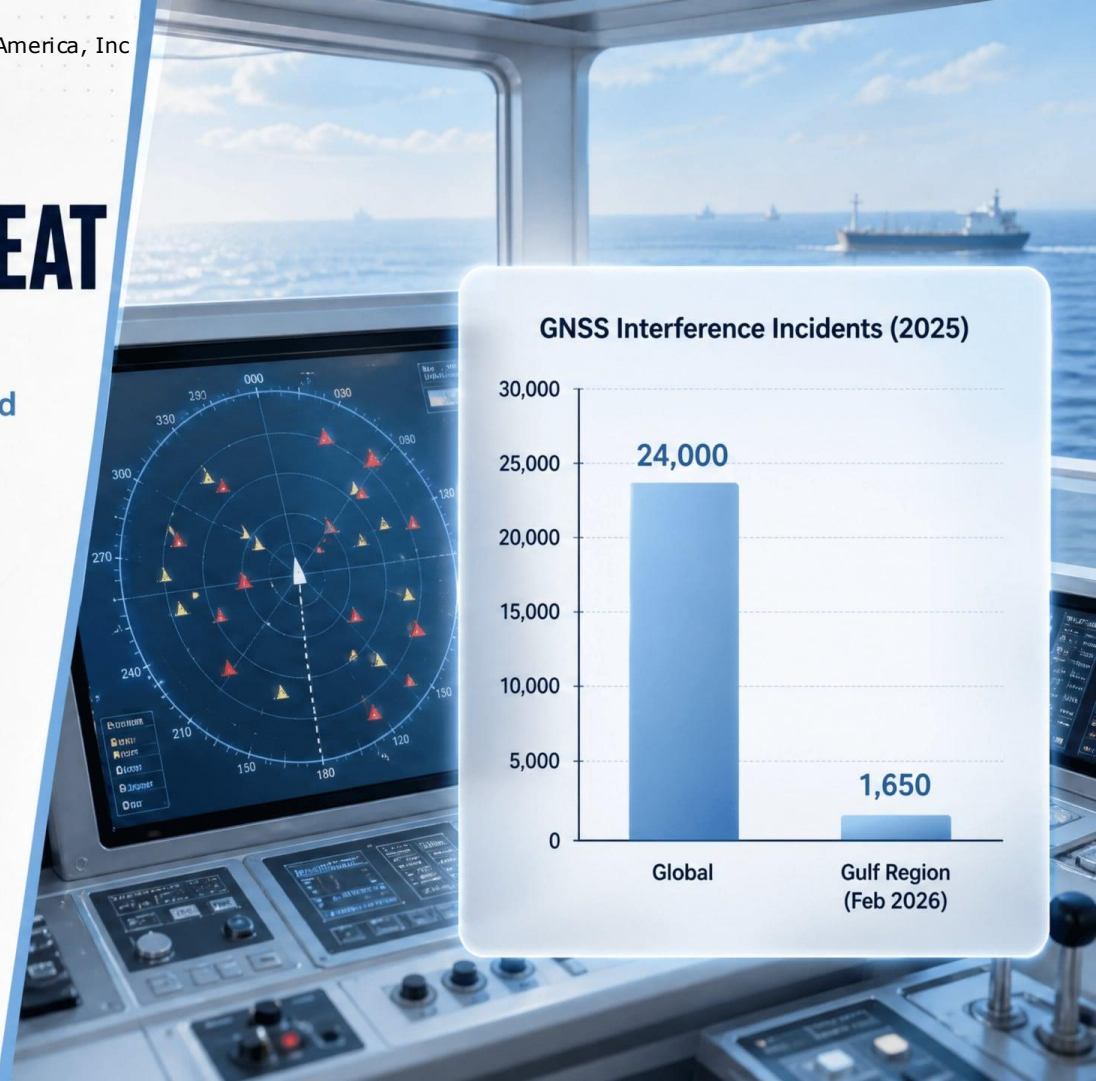
3. PHYSICAL CATASTROPHE RISK:

This vulnerability, baked into civilian GPS design, leads to physical danger (e.g., near-collision prevented by human navigator).

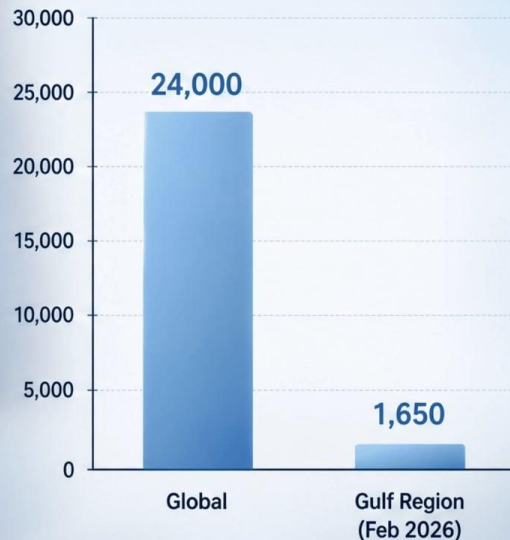


4. ESCALATING HAZARD:

Over 24,000 vessels affected by GNSS interference globally in 2025; 1,650+ disruptions in Gulf region since Feb 2026.



GNSS Interference Incidents (2025)





Information Provided by Trident Group America, Inc

WHY THE SIGNAL CANNOT BE TRUSTED

The Engineering Problem of Civilian GPS Vulnerability



1. CIVILIAN GPS DESIGN FLAW:

L1 C/A signal broadcasts position data in clear text, unencrypted, with no receiver verification mechanism.



2. WEAK SIGNAL STRENGTH:

Legitimate GPS signal is ~20 watts below noise floor at sea level, weaker than a car key fob at 10 meters.



3. EASY TO OVERPOWER:

Overriding requires a transmitter powerful enough to broadcast a fake signal above noise threshold (achievable with commercial hardware).



4. KNOWN WEAKNESS:

Navigation industry aware for decades; state actors and proxies now systematically exploiting this technical reality.



JAMMING VS. SPOOFING

Distinct Threats, Different Operational Signatures

- 1 JAMMING:** Broadcasting RF interference; receivers lose lock, display warnings. Detectable, effects obvious, source triangulatable (e.g., Kaliningrad-origin jamming).
- 2 SPOOFING:** Replaces legitimate signal with counterfeit; receiver accepts as genuine, displaying confident, plausible but fabricated position.
- 3 SPOOFING'S DANGER:** Fundamentally more dangerous because it is invisible; bridge equipment appears normal, vessel navigates on fiction.
- 4 CHARACTERISTIC SIGNATURE:** Multiple vessels in same area simultaneously converging on a single false position (often inland, fixed point).





GEOPOLITICAL ARCHITECTS OF THE THREAT

State-Backed Interference in Critical Maritime Corridors



1. BALTIC & NORTH SEA (RUSSIA):

Operating from Kaliningrad and St. Petersburg; persistent, deliberately operated spoofing infrastructure (e.g., 820+ incidents by mid-2025).



2. PERSIAN GULF (COMPLEX & DANGEROUS):

1,100 vessels disrupted within 24 hours (March 2026); 21 new AIS jamming clusters identified across UAE, Qatari, Omani, and Iranian waters.



3. ACCELERATING TREND:

Gulf interference not a one-off; pace of escalation tracks directly with regional military conflict tempo (e.g., 3,000+ vessels disrupted in June 2025).



4. SAFETY RISKS:

Joint open letter from 14 coastal states declared GNSS interference and AIS manipulation were 'increasing safety risks,' demanding action.



THE INSURANCE AND LIABILITY LABYRINTH

Navigating Coverage in a World of Falsified Data



1. **ACTIVE AIS MANIPULATION:** If a vessel actively manipulates AIS for sanctions evasion or identity concealment, the insurer can void coverage entirely under willful misconduct clauses.



2. **PASSIVE GNSS INTERFERENCE:** Navigating in good faith on GPS data corrupted by external jamming or spoofing presents a complex legal picture for claims handlers.



3. **CYBER EXCLUSION CLAUSES:** Ambiguity remains: is a grounding caused by spoofing a traditional maritime peril or excluded under modern cyber exclusion clauses?



4. **FAILURE OF SEAMANSHIP:** A navigator's failure to cross-check spoofed positions against alternative sources may be argued as a failure to take reasonable precautions.

MARINE INSURANCE POLICY TERMS AND CONDITIONS

4. WARRANTIES AND REPRESENTATIONS

The Assured warrants that all information provided is true, accurate and complete.

8. EXCLUSIONS

8.1 Cyber Exclusion Clause

This insurance does not cover loss, damage, liability, or expense caused by or resulting from any cyber act, including but not limited to the use of malicious code, failure or breach of computer systems, or manipulation, interference, or corruption of electronic data.

8.2 War and Sanctions Exclusion

This insurance excludes loss, damage, liability or expense arising from war, civil war, terrorism, rebellion, revolution, insurrection, mutation, or sanctions.

10. CONDITIONS PRECEDENT

10.1 Seaworthiness and Due Diligence

The Assured shall exercise due diligence to ensure the seaworthiness of the vessel and the accuracy of all navigational data, employing all reasonable means available under the circumstances.

12. GENERAL PROVISIONS

12.3 Notice of Circumstances

The Assured shall give notice of any circumstance which may give rise to a claim under this policy as soon as practicable.

Ambiguity:
Cyber or Peril?

Sanctions &
War Exclusion
Interpretation

Reasonable
Precautions?

Duty of Care
Under Scrutiny



THE DEAD RECKONING SOLUTION: TECHNOLOGY

Reducing Vulnerability with Multi-Constellation GNSS



1. **MULTI-CONSTELLATION GNSS:** Receivers track signals from multiple systems (GPS, Galileo, GLONASS, BeiDou) simultaneously to ensure redundancy.



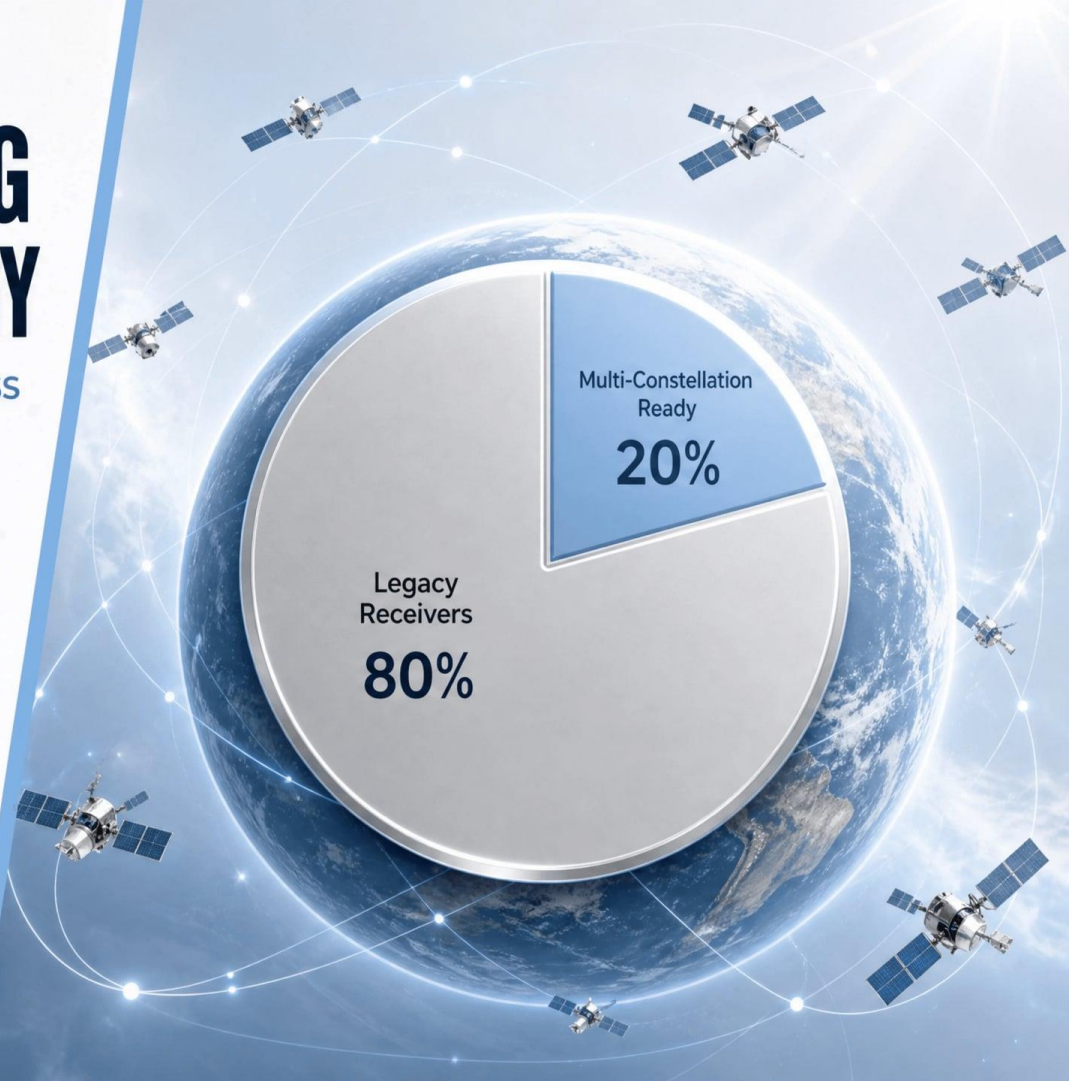
2. **DISCREPANCY DETECTION:** Spoofing one constellation doesn't spoof all; advanced receivers compare data across inputs to detect and reject interference.



3. **GALILEO OSNMA:** EU Galileo introduced Open Service Navigation Message Authentication (July 2025), a cryptographic mechanism for signal verification.



4. **HARDWARE LAG:** Adoption is limited by the need for updated hardware; the vast majority of vessels use legacy receivers without OSNMA support.





THE DEAD RECKONING SOLUTION: HUMAN ELEMENT

The Irreplaceable Skill of Independent Navigation



1. **FOUNDATIONAL SKILLS:** Admiralty charts, radar bearings, depth sounders, and celestial observations are not archaic backups but essential cross-checking tools.



2. **CROSS-CHECKING INFRASTRUCTURE:** These traditional methods provide the necessary infrastructure for a trained navigator to detect when digital instruments lie.



3. **DEAD RECKONING DEFINED:** Calculating current position from a known last position using heading, speed, and elapsed time; entirely independent of satellite signals.



4. **OPERATIONAL REQUIREMENT:** UKMTO advisory: maintain a continuous independent plot, treat unconfirmed GPS as suspect, and report discrepancies immediately.





CONCLUSION

Adapting to the New Reality of GNSS Vulnerability



1. **STRUCTURAL VULNERABILITY:** Civilian GPS signals are inherently vulnerable to jamming and spoofing, a persistent geopolitical reality that requires constant vigilance.



2. **DUAL APPROACH:** Effective resilience requires both technological countermeasures (multi-constellation, authentication) and human procedural safeguards (dead reckoning).



3. **REGULATORY LAG:** The timeline from regulatory mandate to fleet-wide implementation of new tech spans years, leaving a persistent gap in maritime security.



4. **IRREPLACEABLE HUMAN SKILL:** The trained human navigator, equipped with traditional skills and critical judgment, remains the ultimate defense against falsified digital data.

