marinetraffic

September 2025

AIS Spoofing and Sanctions Evasion

Implications for maritime insurance

By Dimitris Ampatzidis, Vasiliki Efstathiou, Sebastiano Ferraris, Atai Otorbaev, Kevin Kinnee and Jean-Charles Gordon

Contents

Executive summary

AIS spoofing, the deliberate falsification of a vessel's identity or location via its Automatic Identification System, undermines the system's intended purpose of enhancing maritime safety and transparency. This manipulation is increasingly used to conceal illegal operations within the shipping industry.

Deceptive practices in shipping have grown considerably in recent years. Conventional monitoring methods often struggle to promptly identify these activities due to their dependence on filtered AIS data, scattered information, and insufficient visual verification.

Effectively uncovering these risks necessitates the combination of continuous, unprocessed AIS data with high resolution satellite imagery and relevant risk indicators. Prompt detection hinges on the ability to link behavioral trends with vessel histories and external intelligence. Nevertheless, many current tools are often reactive, isolated, and lack the sophisticated analysis needed to recognize evolving deceptive tactics.

Key takeaways

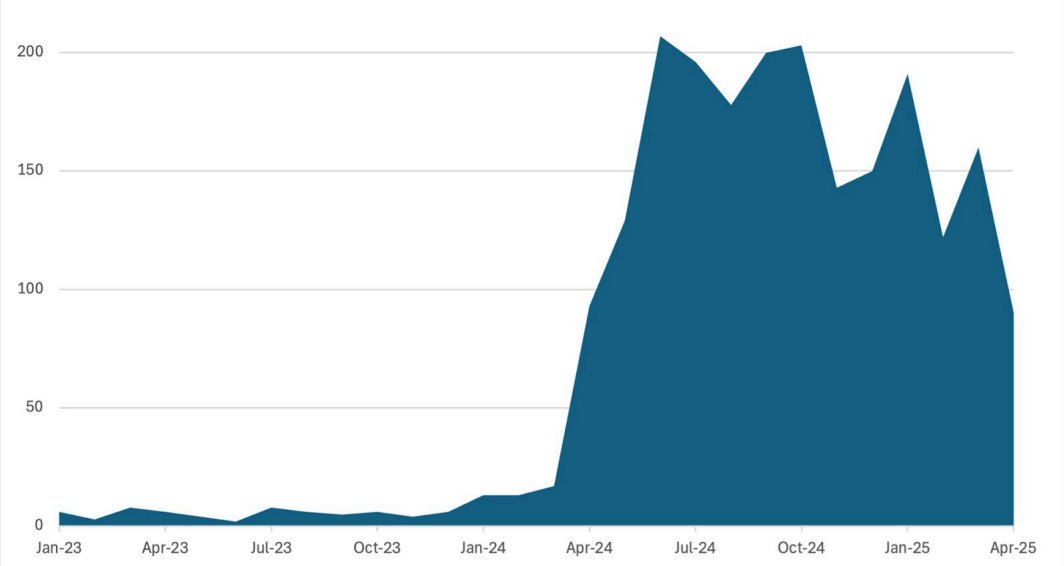
- AIS spoofing incidents dramatically increased by over 2,400% between 2023 and 2024, escalating from around 60 to more than 1,500 cases.
- Deceptive AIS activity exhibits consistent patterns like stationary grids, circular loops, and the reuse of past routes, allowing threat actors to imitate normal vessel behavior and avoid standard surveillance.
- A clear link exists between the increase in spoofing and significant regulatory changes, particularly the expanded sanctions enforcement by OFAC and the EU in 2024, highlighting the rapid adaptability of illicit actors.
- The majority (over 70%) of identified spoofing events feature dense grid formations or irregular loitering, frequently observed near sanctioned oil export centers, suggesting a calculated attempt to obscure trade movements via data manipulation.
- Integrating unprocessed AIS data with satellite imagery and land-based signal triangulation significantly improves detection precision (up to a fourfold increase), emphasizing the necessity of multi-layered, real-time intelligence to effectively counter the evolving methods of spoofing.
- The growing use of spoofing by sanctioned vessels concentrates insurance exposure and increases the likelihood of fraudulent or uninsured claims.

The rise of deceptive practices at sea

AIS was introduced to prevent collisions by broadcasting a vessel's position, speed, heading, and identity to its immediate surroundings. It has since become central to maritime monitoring, used by authorities and compliance teams alike. However, AIS is inherently insecure. The signal is unencrypted and easily manipulated.

Spoofing and other AIS tampering tactics, such as identity cloning and false location reporting, are now common. These methods are used to obscure illegal transshipments, sanctioned cargo movements, and operations by grey fleets. Some ships simulate being at anchor while conducting covert activity elsewhere. These manipulations often occur along routes linked to sanctioned oil and commodity flows.

Graph 1: Monthly volume of detected AIS manipulation incidents (from January 2023 till April 2025)



Source: Kpler

Spoofing activity remained minimal throughout 2023, with monthly incidents consistently below 25 cases. This changed rapidly in the first quarter of 2024, when detections began to rise sharply, exceeding 100 cases by March. The spike continued through the second quarter, peaking above 200 cases by mid-2024. For several consecutive months, spoofing incidents remained well above the 150 mark, marking a sustained period of elevated manipulation attempts. This trend persisted into early 2025, with fluctuations but no return to 2023 levels.

The timing of this escalation closely mirrors a wave of coordinated regulatory actions. In late 2023 and early 2024, the United States expanded its price cap enforcement under the Office of Foreign Assets Control (OFAC), including targeted advisories and vessel designations related to Russian-origin crude and refined products. The European Union followed with updates to its sanctions framework, mandating stricter due diligence requirements for EU-based shipping and insurance firms. The United Kingdom, through the Office of Financial Sanctions Implementation (OFSI) and the Foreign, Commonwealth & Development Office (FCDO), introduced additional compliance obligations and emphasized liability for those who fail to detect or prevent circumvention. These combined measures significantly raised the compliance burden on maritime actors and created stronger incentives for bad-faith operators to mask their movements.

Understanding AIS spoofing and signal manipulation

Global Navigation Satellite System (GNSS) signals are vulnerable to radio frequency interference, including deliberate disruptions. Depending on the attackers' goals and tools, interference may take the form of GNSS spoofing, jamming, or AIS spoofing.

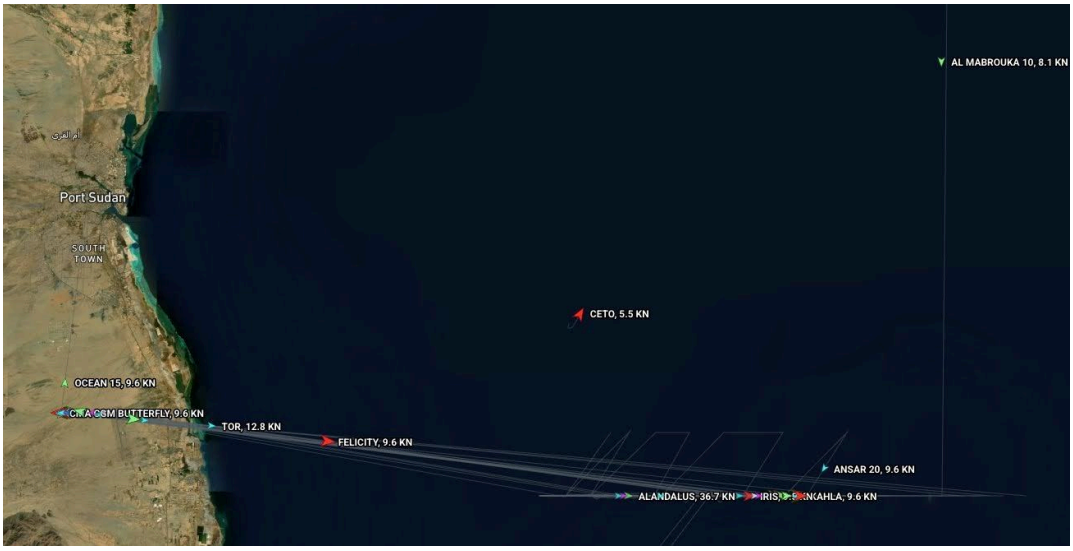
GNSS Spoofing is a form of electronic attack that manipulates GNSS receivers by broadcasting counterfeit satellite radio-frequency signals. These fake signals, transmitted with slightly higher power than authentic GNSS transmissions, trick the receiver into calculating an incorrect position, velocity, or time. Meaconing, a common spoofing method, captures genuine GNSS signals and rebroadcasts them with delay and increased power to mislead navigation systems. See image 1.

GNSS jamming, a more severe attack, uses much stronger signals to block real transmissions entirely, causing outages and complete signal loss. While more complex to execute, jamming is easier to detect due to its high signal power.

Both spoofing and jamming distort navigation. In maritime contexts, spoofed AIS messages produce implausible vessel paths—wrong locations, speeds, or routes—often clustering ships in unrealistic positions during interference.

AIS spoofing is a deceptive tactic where a vessel alters its AIS signals to hide its true identity or location. The goal is to obscure vessel activity temporarily by broadcasting false data. Unlike area-wide interference, AIS spoofing affects only the vessel performing it. The resulting track may appear plausible or clearly false. Here, the vessel itself is the bad actor, unlike GNSS spoofing or jamming, where attackers operate independently of any single ship's movements.

Image 1: Interference pattern of GNSS spoofing in the Red Sea Port Sudan area in May 2025



Source: Kpler

Patterns behind AIS spoofing

Identity falsification

This tactic involves altering static AIS data, such as MMSI, vessel name, IMO, call sign, or flag, to hide a vessel's true identity. Spoofers may use identities from active ships, retired vessels, or even entirely fictional ones. Duplicate use of an active identity can sometimes be spotted through simultaneous, conflicting tracks. More coordinated or fabricated identities, however, are harder to detect, especially when identity sharing is deliberate or the spoofed identity has no real-world counterpart.

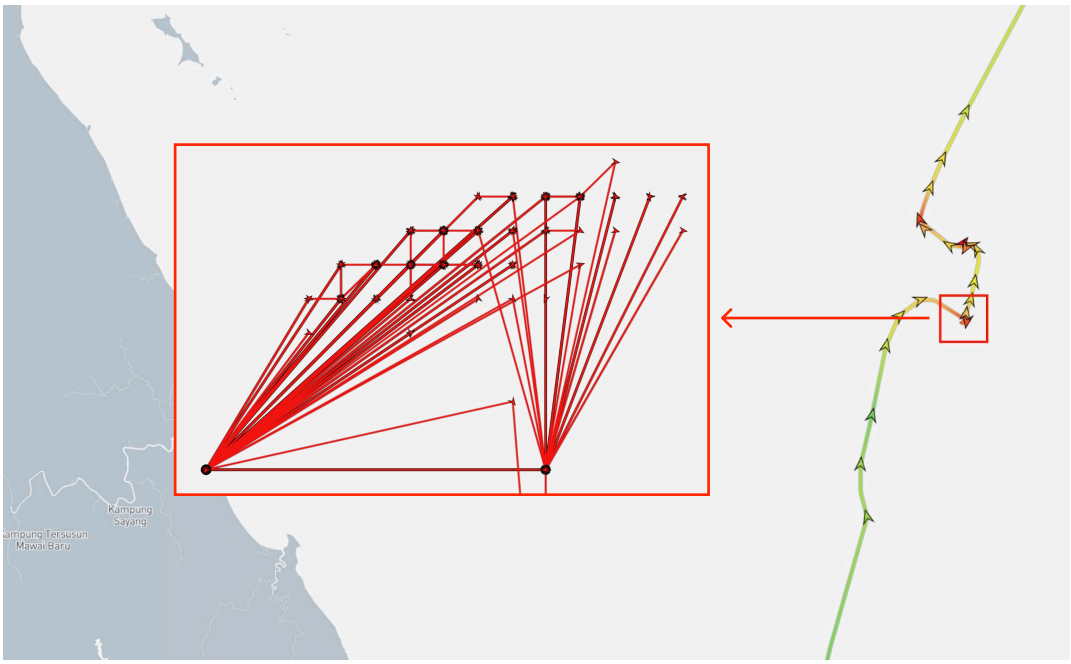
Location falsification

Location falsification involves manipulation of the mobility-specific information of dynamic AIS messages. The motive behind the action is for the vessel to conceal its true location by reporting misleading tracking data. This practice is ubiquitous across the globe and is encountered in the form of fabricated voyages in open seas as well as in port areas. This practice is more common than identity falsification and can be manifested via a vessel's mobility behaviour. In what follows we present prevalent location falsification patterns and means of detecting these.

Location falsification patterns

Stationary dense grid: This spoofing pattern involves repeated transmission of identical coordinates in a tightly packed, grid-like formation. At first glance, it may appear as a single point on a vessel's track. However, closer analysis reveals clusters of overlapping positions reported over several days. Each grid node reflects hundreds of repeated lat/lon pairs, typically with speeds recorded at 0 knots.

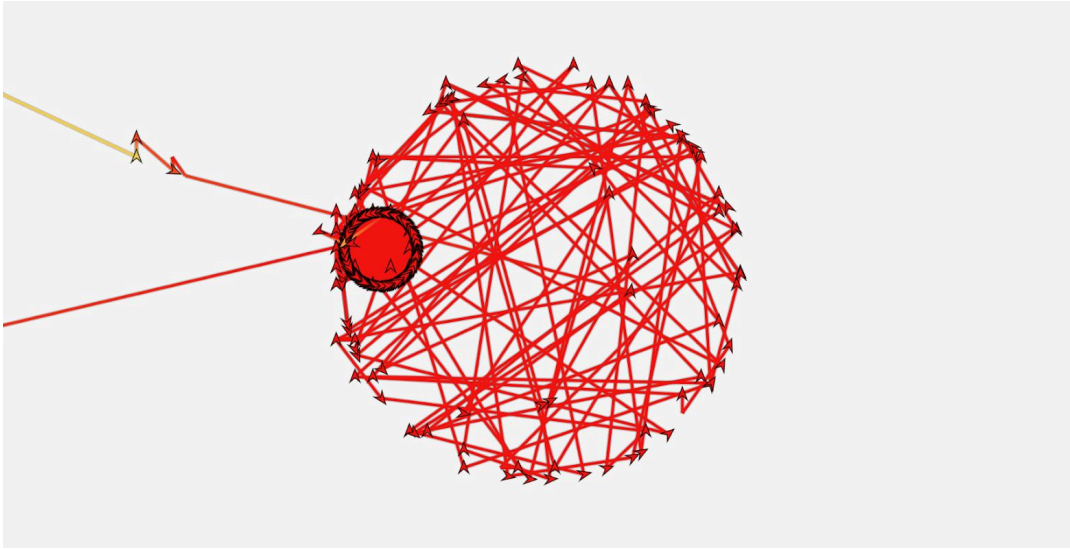
Image 2: Stationary dense grid example



Source: Kpler

Stationary circular pattern: another common pattern in the positions reported by spoofing vessels is reflected in the form of symmetric circular arrangements. The majority of reported speed values are equal to 0 and even though the positions are located in very close proximity, the reported kinematic values do not account for the expected positional transitions reflected in the trajectory.

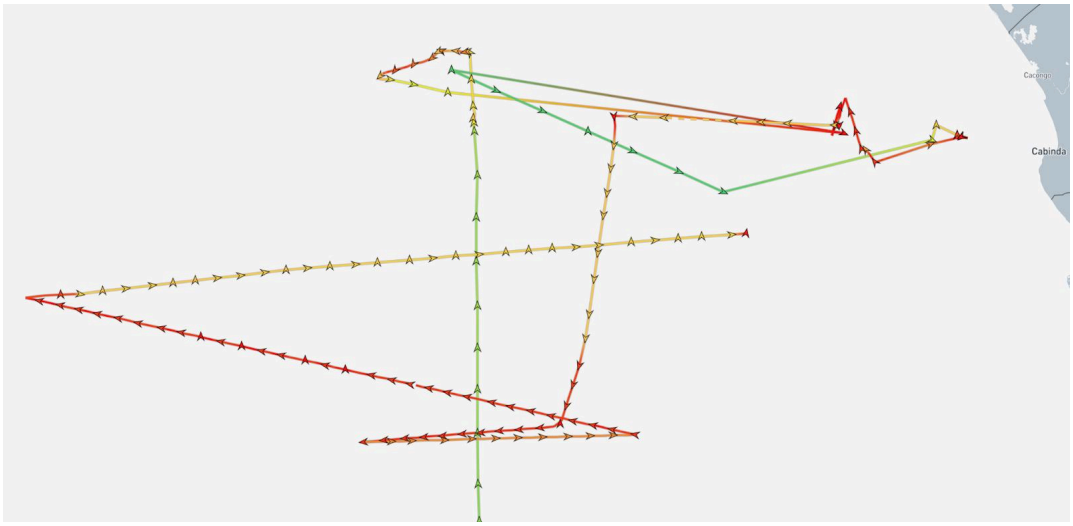
Image 3: Stationary circular pattern example



Source: Kpler

Erratic loitering: these patterns are characterised by abrupt changes in course and speed which subsequently lead to trajectories with unconventional shapes, and kinematic behaviour that is inconsistent with the expected fluctuations in the respective parameters.

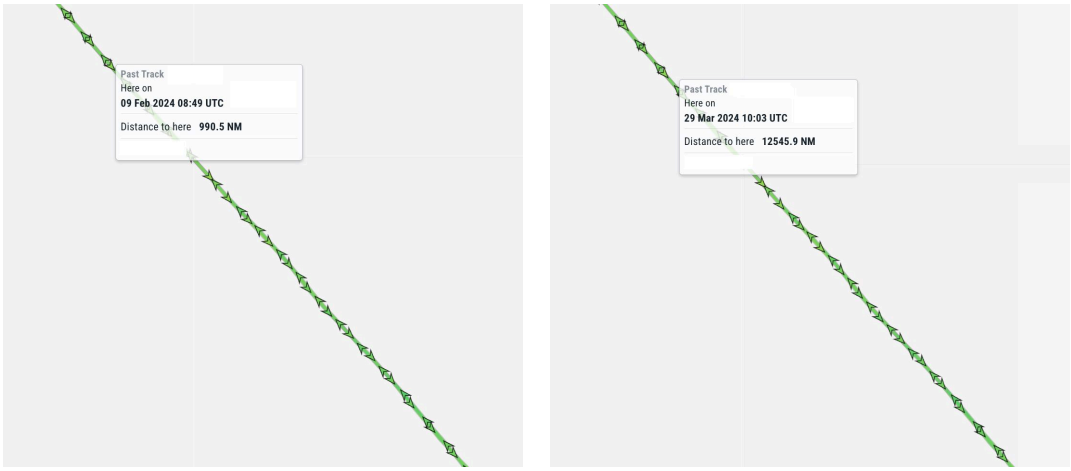
Image 4: Erratic loitering example



Source: Kpler

Retransmission of a historical voyage: In this spoofing method, a vessel replays a past voyage, making the track appear legitimate but offset in time. Since the trajectory is real, these cases are difficult to detect, as the anomaly lies in the timing rather than the path itself.

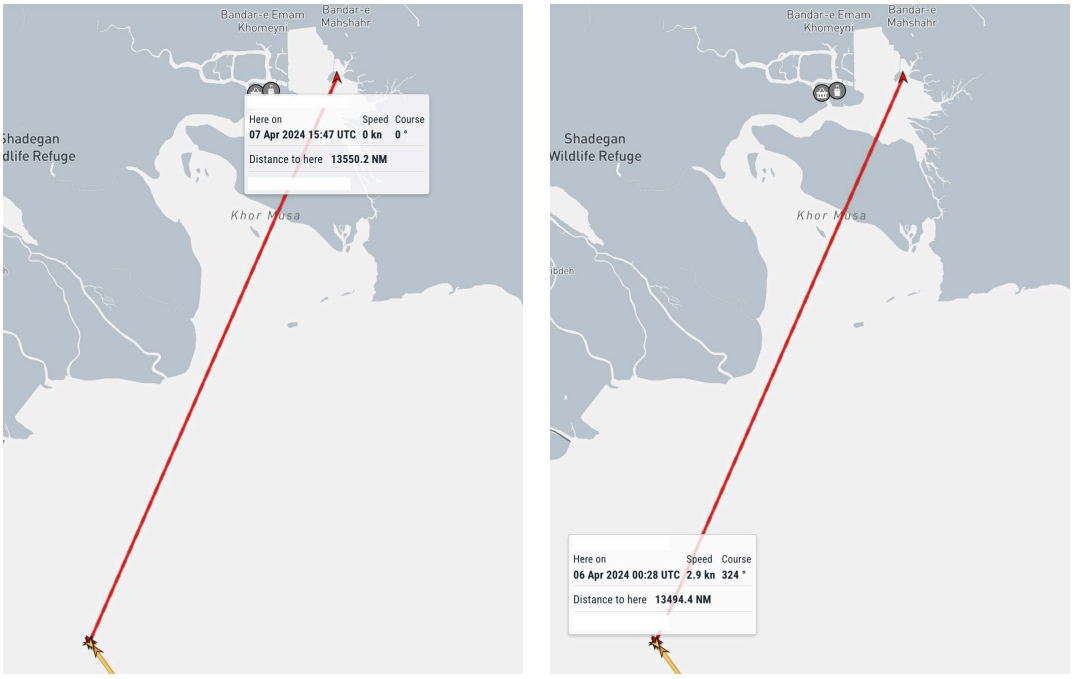
Image 5: Retransmission of a historical voyage - trajectory segments during February 2024 and March 2024 where the same vessel appears to be retracing the identical route



Source: Kpler

Leaps to true location: Despite typically broadcasting fabricated locations through either concentrated, localized fake signals or by mimicking believable long-distance voyages, vessels engaged in spoofing sometimes inadvertently disclose their real position via occasional AIS messages. For instance, one vessel exhibited a tight, grid-like spoofing pattern, yet after a 17-hour absence in transmissions, a solitary AIS signal surfaced at Iran's Mahshahr Export Port before the false signals reappeared in Iraq. These infrequent inconsistencies can unveil a vessel's actual travel history.

Image 6: The vessel is transmitting several positions consistently located within the Khor Al Zubair anchorage area



Source: Kpler

AIS spoofing detection methods

The wide range of spoofing patterns makes detection difficult for both AI and human analysts. To address this, several complementary methods are used:

- Kinematic analysis to flag implausible vessel movements
- Ground station localization to spot mismatches between AIS data and reception zones
- Satellite imagery to locate vessels in places inconsistent with their AIS reports
- Human expertise for contextual assessment and verification

Kinematic analysis algorithms

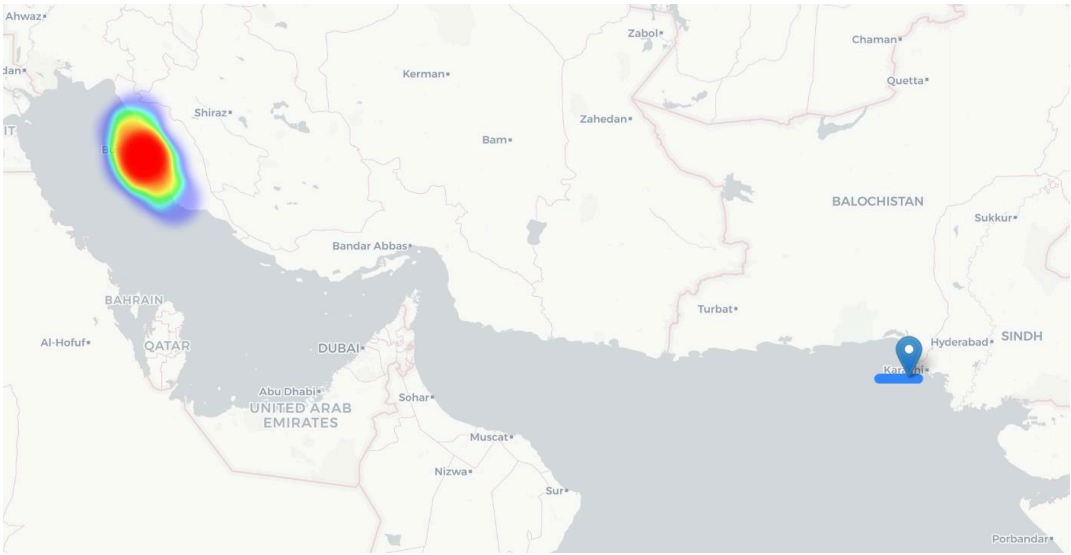
These models analyze vessel speed, heading, and course to predict future positions. By comparing predictions with AIS-reported locations, the system flags discrepancies. Persistent or significant mismatches suggest potential spoofing, especially when patterns of deviation are dense or prolonged.

Ground station localisation algorithm

By checking whether a vessel's reported location aligns with the range of receiving ground AIS stations, algorithms can detect false positioning. When transmitted data conflicts with expected reception zones, the system distinguishes between spoofing and minor transmission noise.

Images 7-9 illustrate three legs of a vessel's voyage which according to the AIS-reported messages commenced on December 26, 2024 in Karachi, Pakistan. As the vessel is heading eastbound on December 26 and 27, the respective AIS signal reception is localised in the northeast coast of the Persian Gulf depicted in the heatmap in Image 7.

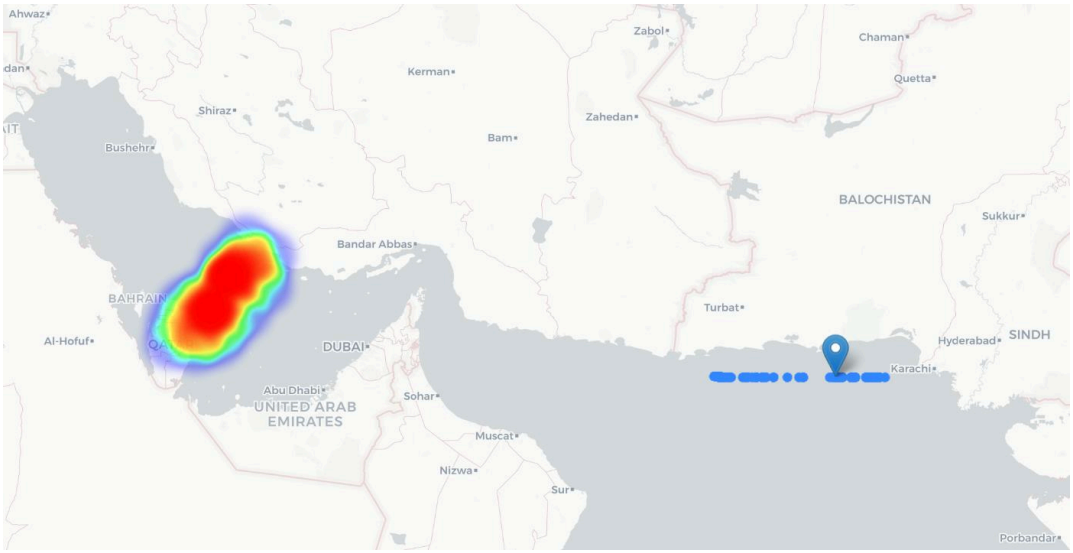
Image 7: Snapshot of a vessel's voyage which according to the AIS-reported messages commenced on December 26, 2024 in Karachi, Pakistan



Source: Kpler

As the vessel continues sailing eastbound during December 28 and 29 the respective signal reception activity illustrated as a heatmap, indicates southbound mobility within the Persian Gulf Image 8.

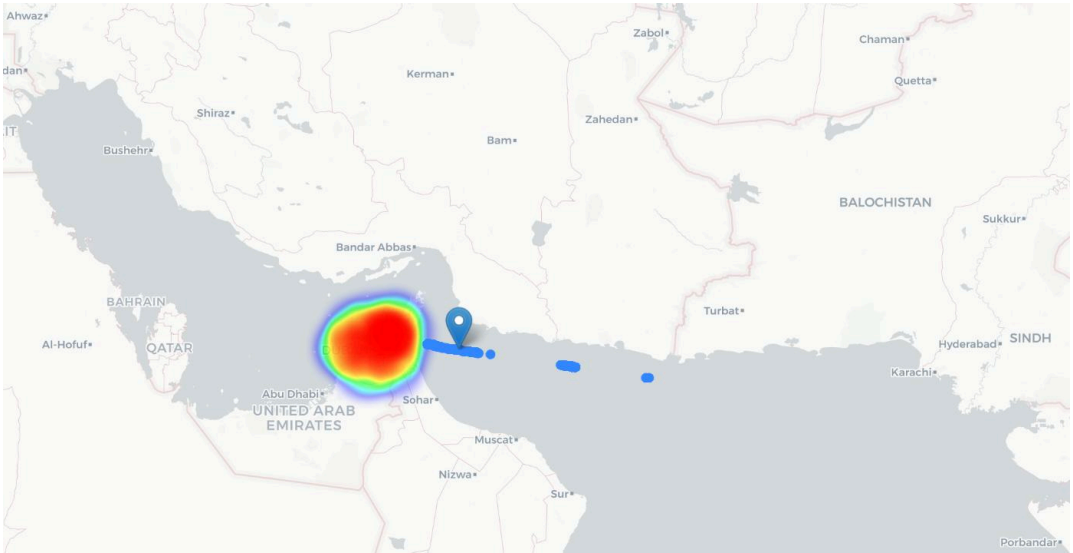
Image 8: Snapshot of a vessel's voyage which according to the AIS-reported messages commenced on December 26, 2024 in Karachi, Pakistan



Source: Kpler

The vessel is finally seen in the north part of the Gulf of Oman on December 31st, its reported positions converging with the location of signal reception activity, suggesting the vessel resumed normal transmission, visualized on Image 9.

Image 9: Snapshot of a vessel's voyage which according to the AIS-reported messages commenced on December 26, 2024 in Karachi, Pakistan

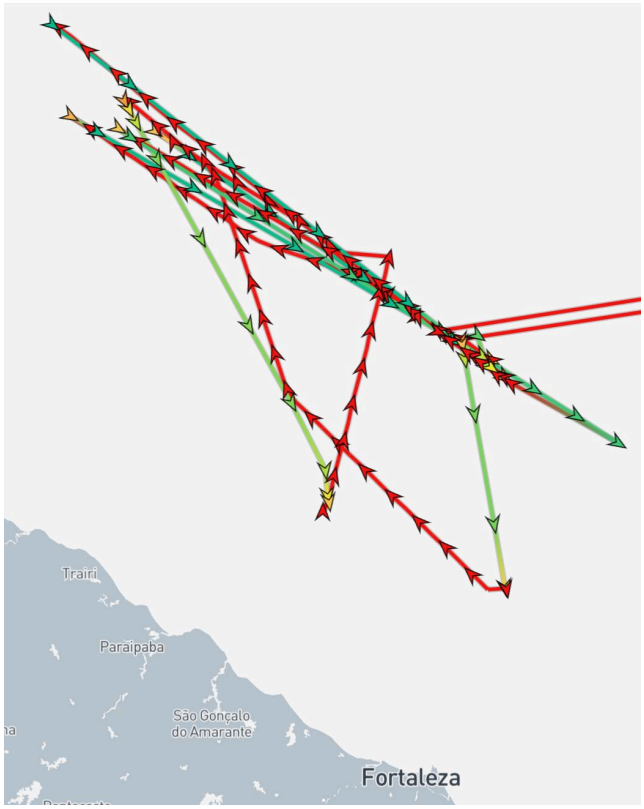


Source: Kpler

Combined sources for unprecedented accuracy

The wide range of spoofing patterns necessitates identifying the distinct facets manifested in a vessel's behavior via a range of data sources and methods, The trajectory in Image 10 manifests erratic loitering with sharp changes of direction. These features led the algorithm that performs kinematic analysis on vessel tracks to flag this trajectory as abnormal.

Image 10: A fabricated vessel trajectory that lasted for a period of 5 months



Source: Kpler

Additionally, the ground station localisation algorithm flagged a non-viable signal reception pattern where the fabricated AIS messages reporting positions near Fortalezza were being received by stations located in the Caribbean sea, nearly 2000nm away. While algorithms can flag anomalies via complementary evidence, human validation is essential. Analysts verify such cases using satellite imagery, as in this example where the vessel was visually confirmed near Barcelona, Venezuela during the reported period.

Image 11: Vessel found in the wider port area of Barcelona, Venezuela

Source: Sentinel Hub's EO Browser

The consequences of ignoring spoofing

Spoofed vessel data poses serious risks for port authorities, insurers, and flag registries. Concealing a ship's true identity or location makes it harder to evaluate cargo, past activity, or compliance, increasing the chance that ports may admit high-risk or sanctioned vessels based on false data.

Legally, undetected spoofing can quickly result in sanctions breaches. Entities that overlook AIS anomalies or suspicious routing may face fines or operational restrictions, with regulators rejecting ignorance as a defense.

Financially, spoofing undermines trade transparency. It causes cargo to vanish from tracking systems, distorting commodity flows, disrupting pricing, and enabling insurance fraud, including duplicate claims for the same cargo.

The national security risks of AIS spoofing

AIS spoofing poses a growing threat to maritime situational awareness, particularly for government stakeholders tasked with national security, sanctions enforcement, and maritime safety. Unlike AIS jamming, which causes a denial of positional data by disabling GNSS signals, spoofing actively deceives receivers by faking GNSS signals, causing the AIS transponder to broadcast a false location. This form of deception compromises real-time vessel tracking, allowing illicit actors to obscure STS transfers, mask sanctioned oil movements, and circumvent port authority scrutiny. For government agencies such as the Department of Homeland Security, U.S. Coast Guard, and OFAC, AIS spoofing complicates efforts to attribute suspicious activity, enforce embargoes, and maintain a clear maritime operating picture in contested or high-risk waters.

International maritime authorities such as the **UK Maritime Trade Operations (UKMTO)** and in the U.S., **The Office of Naval Intelligence (ONI)** also monitors spoofing and jamming events, often issuing incident alerts and intelligence assessments to ensure regional maritime security coordination and threat awareness.

In May, 2025, according to the UKMTO, ships transiting the Strait of Hormuz and the southern Red Sea experienced repeated GPS signal interference in May, with disruptions lasting several hours and forcing crews to rely on backup navigation methods **(UKMTO, 24–30 May 2025)**. During the same period, vessels anchored off Ras Isa, Yemen, were reportedly denied departure even with UN clearance, with some boarded by armed personnel under threat of force **(UKMTO, 26 April–2 May 2025)**. Meanwhile, the ONI recorded several violent boarding attempts in Southeast Asia and the Gulf of Guinea, including knife-point robberies and armed crew kidnappings **(ONI WTS Report, 30 April–28 May 2025)**. These developments identify the growing operational and physical risks for vessels, and the need for real time location accuracy.

While national security agencies track these risks, the same vessel tactics also undermine insurance market stability by distorting cargo tracking and liability assessment.

The value of real-time, raw AIS & satellite fusion

For effective maritime compliance, real-time detection is crucial because enforcement depends on capturing a vessel's movements as they happen. Delay can lead to the loss of crucial evidence and reduced accountability. Raw AIS data is vital for identifying spoofing as it retains anomalies such as course alterations, identity duplications, or absent timestamps, which are often removed in filtered data that prioritizes clarity over the preservation of manipulation indicators. Satellite imagery provides a visual verification that can either support or contradict AIS data, potentially revealing discrepancies like a vessel claiming to be in one location but actually anchored in a prohibited zone, indicating possible fraud or undisclosed port visits. Combining AIS, satellite, and port information allows for thorough cross-verification. Consistency among these sources strengthens reliability, whereas discrepancies signal the need for more detailed investigation.

For insurers, such integrated intelligence can form the backbone of proactive compliance monitoring, underwriting decisions, and claims verification.

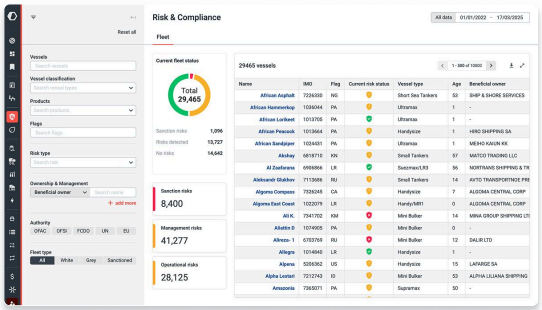
Restoring integrity at sea

AIS spoofing severely jeopardizes maritime transparency, safety, and oversight. The intentional falsification of identities and concealment of vessel movements put both operators and the environment at significant risk. Combating this threat demands a concerted effort from all parties involved. Regulatory bodies must place a strong emphasis on data integrity, while insurance providers need to rigorously verify voyage information. Similarly, port authorities should implement robust screening processes to identify potential manipulation. Shipowners bear the responsibility of safeguarding their fleets against compromise through inadequate controls. Access to dependable and unfiltered data is paramount; its absence only delays detection and perpetuates misuse. The maritime sector needs to transition from a system of reactive compliance measures to one of proactive, intelligence-driven monitoring. Securing the integrity of maritime operations necessitates not only enhanced technological tools but also a collective dedication to accountability and unambiguous visibility.

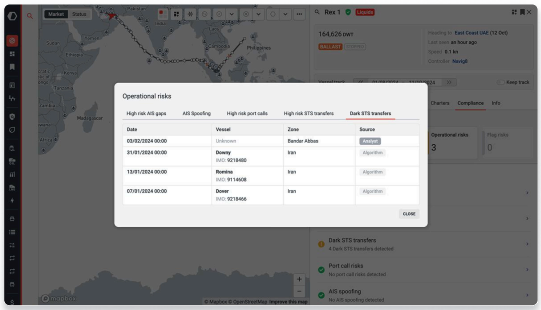
Kpler Risk & Compliance

Designed to help businesses mitigate risks with ease.

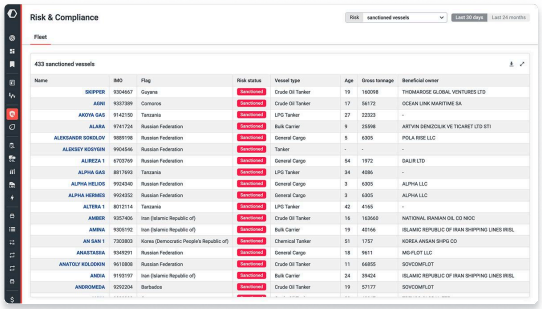
Real-time compliance monitoring



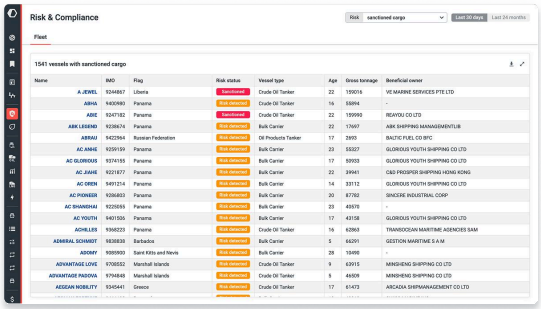
Dark STS transfers



Sanctioned vessels



Sanctioned cargo



Built on the best data in a unified platform

Kpler Risk & Compliance is the ideal solution for those aiming to accurately identify risks.

It delivers unmatched cargo data insights paired with precise, real-time positional information from the world's largest AIS network. This allows Kpler to pinpoint at-risk cargo movements, ship-to-ship transfers, AIS gaps, spoofing activities, and effectively decode potential illicit activities.

Coupled with daily updates on sanctioned vessels, flags, and cargo, as well as insights into ownership structures and vessel affiliations, it helps safeguard customer reputations.

This information is integrated into a unified and user-friendly platform, enabling proactive risk management and ensuring your operations remain compliant and protected from potential penalties.

Explore the in-depth data and intelligence behind this report and much more.

Request demo →

marinetraffic