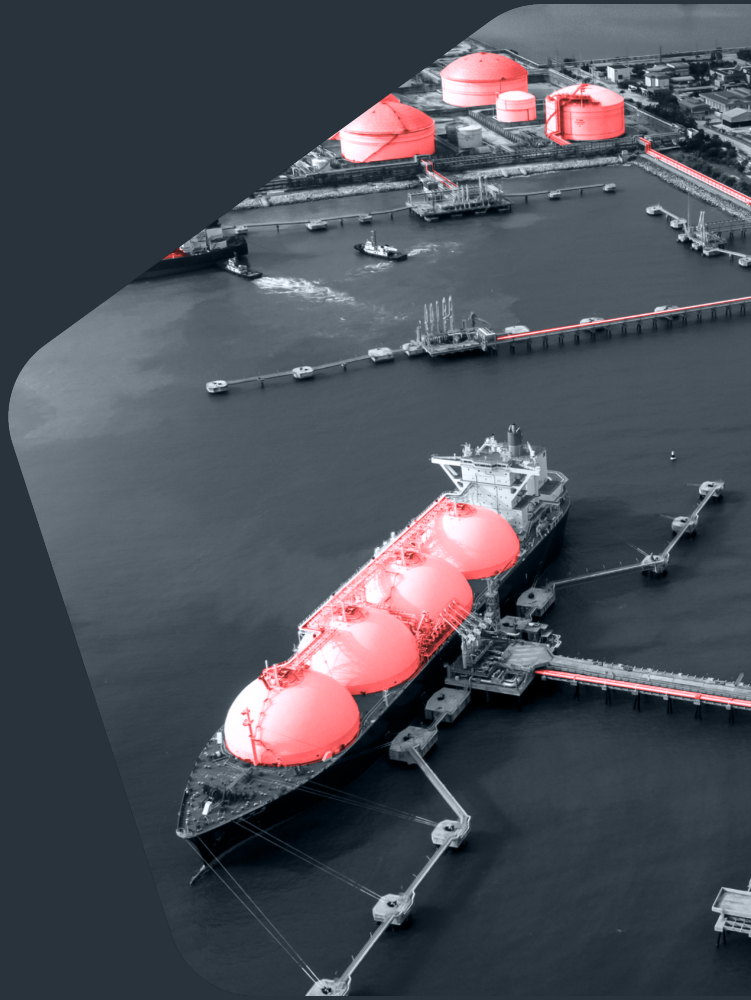
kpler

False positions at sea

distinguishing AIS spoofing from GNSS interference

Dimitris Ampatzidis (Maritime Risk & Compliance Manager)
Ana Subasic (Trade Risk Analyst)
Yuan Li (Junior Risk & Compliance Analyst)



The distinction
Why attribution matters

- **AIS spoofing is deliberate:** false identity or position data broadcast to conceal movement, activity or association
- **GNSS spoofing** feeds counterfeit satellite signals, so a working transponder transmits the wrong position
- **GNSS jamming** blocks reliable positioning altogether
- **Same symptom, different conclusion** – and a different response

AIS spoofing vs GNSS spoofing

Manipulated layer, typical source, scale, intent attribution and main risk

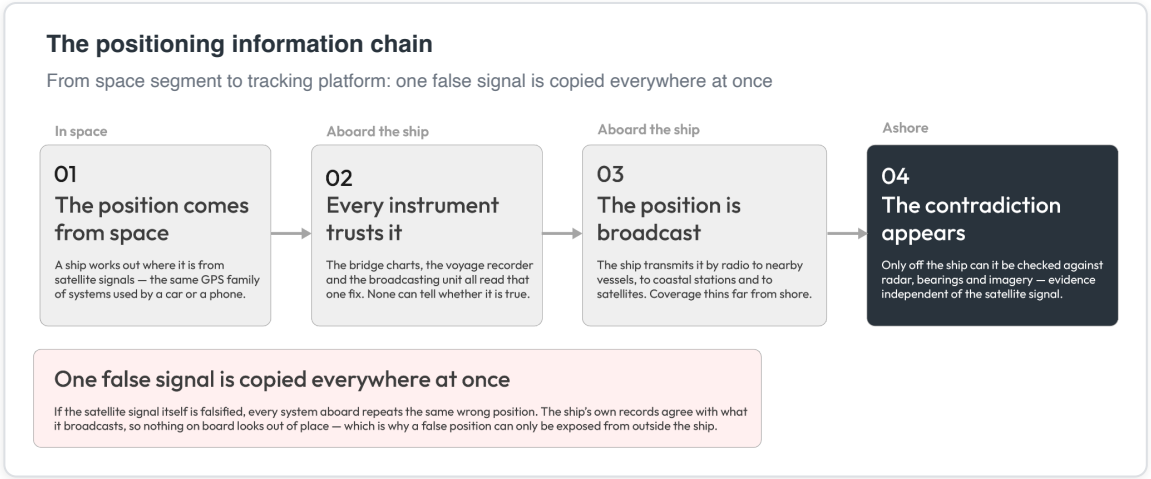
Comparison	AIS Spoofing	GNSS Spoofing
Manipulated layer	The AIS message itself, identity, position, or status broadcast to other stations	The vessel´s receiver computes a false position/time from a terrestrial transmitter. Satellite signal in space is not altered
Typical source	Onboard transponder configuration or software manipulated by the vessel / operator	External RF transmitter mimicking genuine satellite signals, orignating off the vessel
Typical scale	Usually vessel-specfic, one ship at a time, along its own voyage	Often regional, multiple, unrelated vessels affected simultaneously in one area
Intent attribution	Deliberate act by the vessel or operator, clear intent to deceive	Intent, if any, lies with a third-party source, the vessel is typically a victim, not an actor
Main risk	Sanctions evasion, compliance exposure, deceptive trade	Navigation and collision safety, insurance disputes, and wrongful misattribution of intent

Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

kpler

The chain
How GNSS faults spread

- **AIS broadcasts what GNSS gives it** – it does not independently verify geolocation
- **One bad input, many consistent outputs:** AIS, ECDIS and VDR agree because they share the same source
- **Internal consistency is weak evidence** of position integrity
- **Corroborate outside the GNSS path:** radar, visual bearings, inertial, SAR/optical imagery, reception patterns



Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

kpler

GNSS interference is a regional condition, not a vessel story.

- **Spoofing** gives the wrong answer: a credible but false position
- **Jamming** gives no answer: no reliable fix at all
- **Not every anomaly is deliberate:** equipment faults, antenna obstruction and atmospheric effects can look similar
- **Scale is the clearest indicator:** unrelated vessels shifting together, then normalising after leaving the area

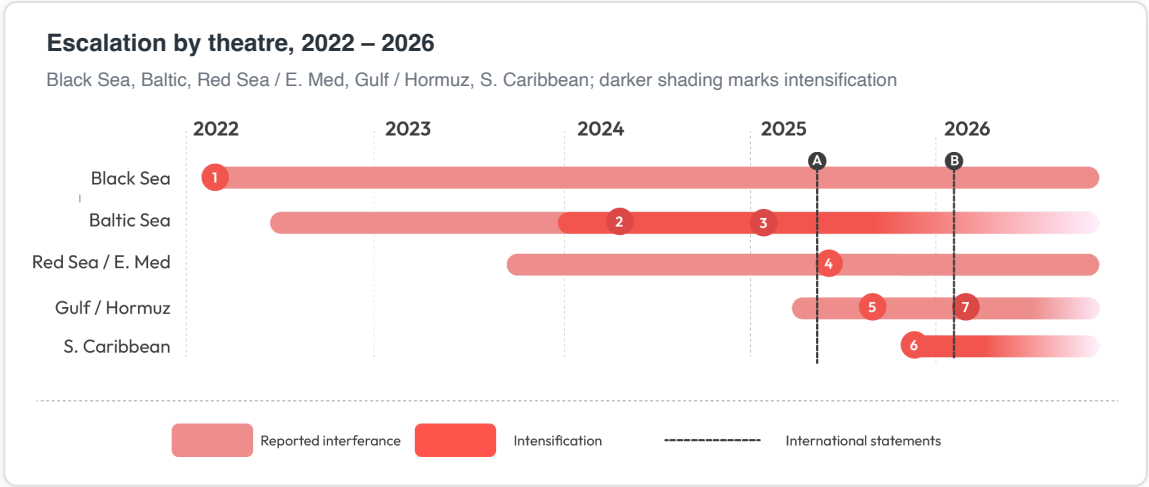


Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

kpler

The escalation
From nuisance to norm

- **Before 2022:** GNSS interference at sea treated as a localised nuisance
- **By 2026: a standing condition** in several of the busiest corridors, from the Baltic to the Gulf
- **March 2025: ITU, ICAO and IMO** expressed grave concern over rising jamming and spoofing
- **A change in character, not just volume:** an area effect tied to conflict and infrastructure protection



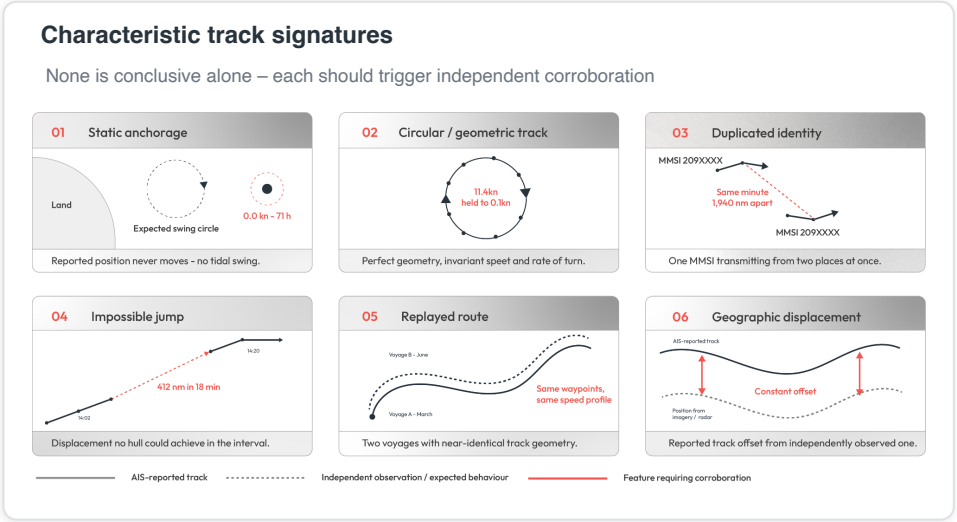
Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

kpler

Five AIS spoofing techniques, each leaving a different signature in the data

AIS carries no authentication – any field can be falsified:

- **Identity manipulation:** cloned MMSI, IMO or name, or a decommissioned vessel's identity
- **Position manipulation:** a fabricated location or a consistent offset from the true one
- **Pre-programmed or replayed tracks:** stored voyages that repeat too closely between transits
- **Ghost or synthetic targets:** messages for a vessel that is not physically there
- **Combined behaviour:** e.g. spoofed position + AIS gap, or identity changes around a dark STS





Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

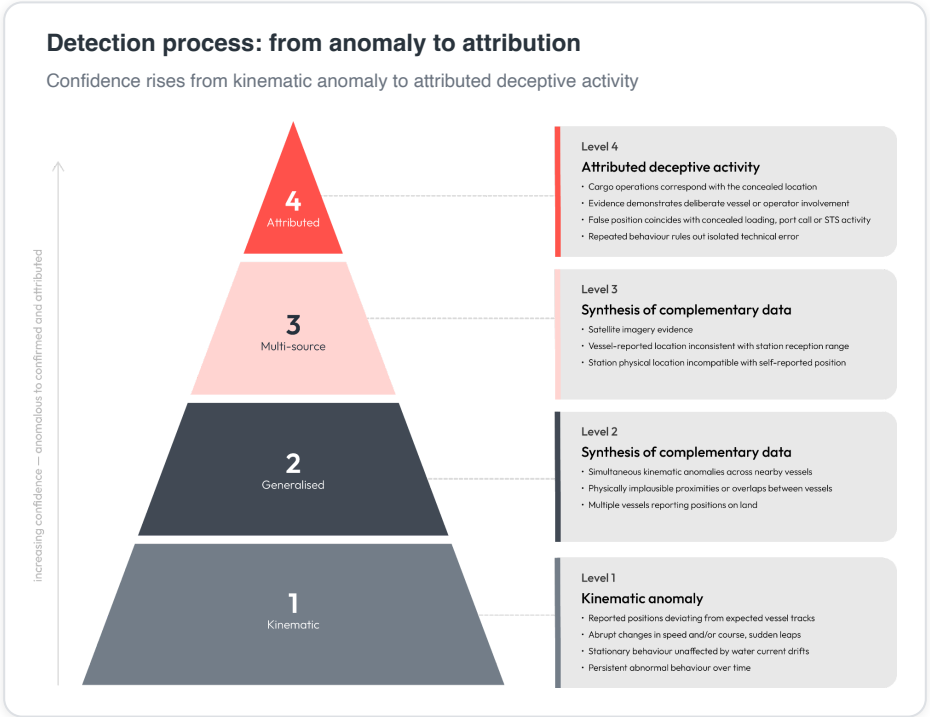
kpler

How Kpler moves from anomaly to attribution

Four levels of confidence:

- **Level 1 – Kinematic:** a track, speed or course the vessel could not physically achieve; persistence matters
- **Level 2 – Generalised:** unrelated vessels show the same anomaly, pointing to regional interference
- **Level 3 – Multi-source:** imagery or reception data contradict the reported position – false, but not yet why
- **Level 4 – Attributed:** the false position lines up with cargo work, a port call or STS the vessel had reason to conceal

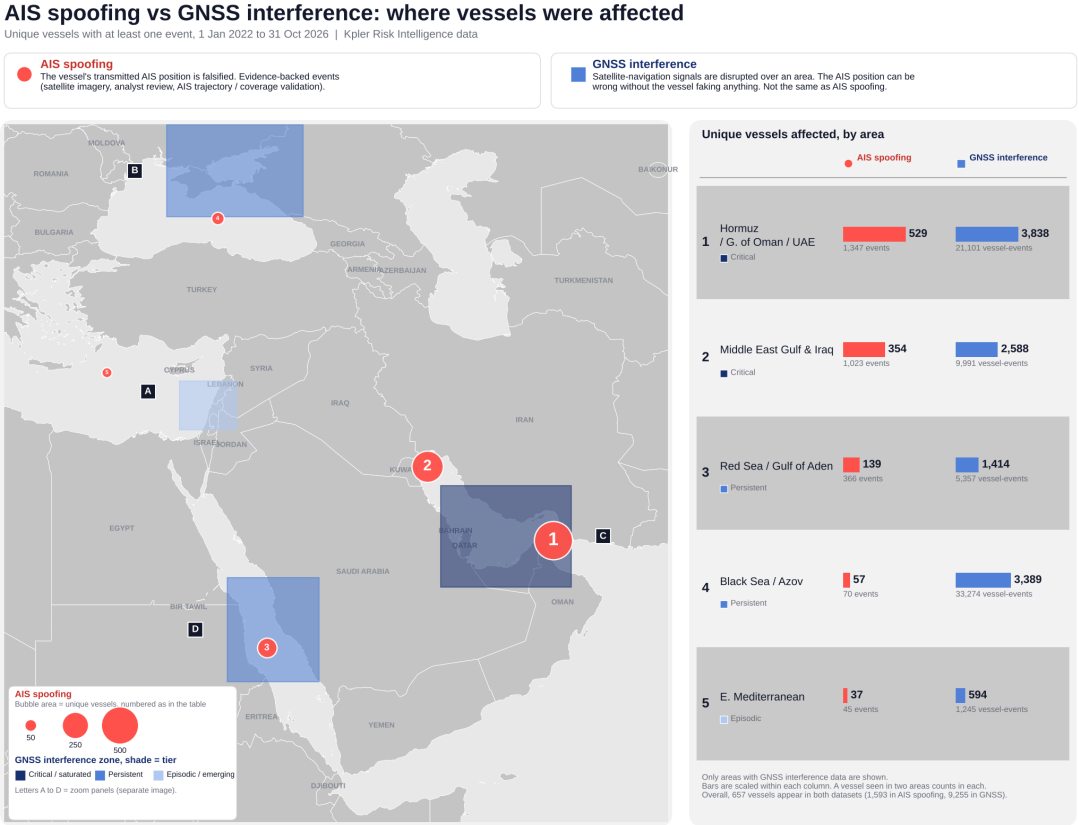
Not every case climbs all four levels: a regional finding at Level 2 can stop vessel-level attribution.



Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

kpler

Vessel-level spoofing and area-wide interference overlap only partly



August 2025 – Oct 2026

- **Red Sea ranks 3rd** for vessel-level spoofing (139 events)
- **The Gulf is the only theatre where both are severe,** which makes attribution hardest there
- **Interference tracks military events;** spoofing tracks trade and sanctions pressure

Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

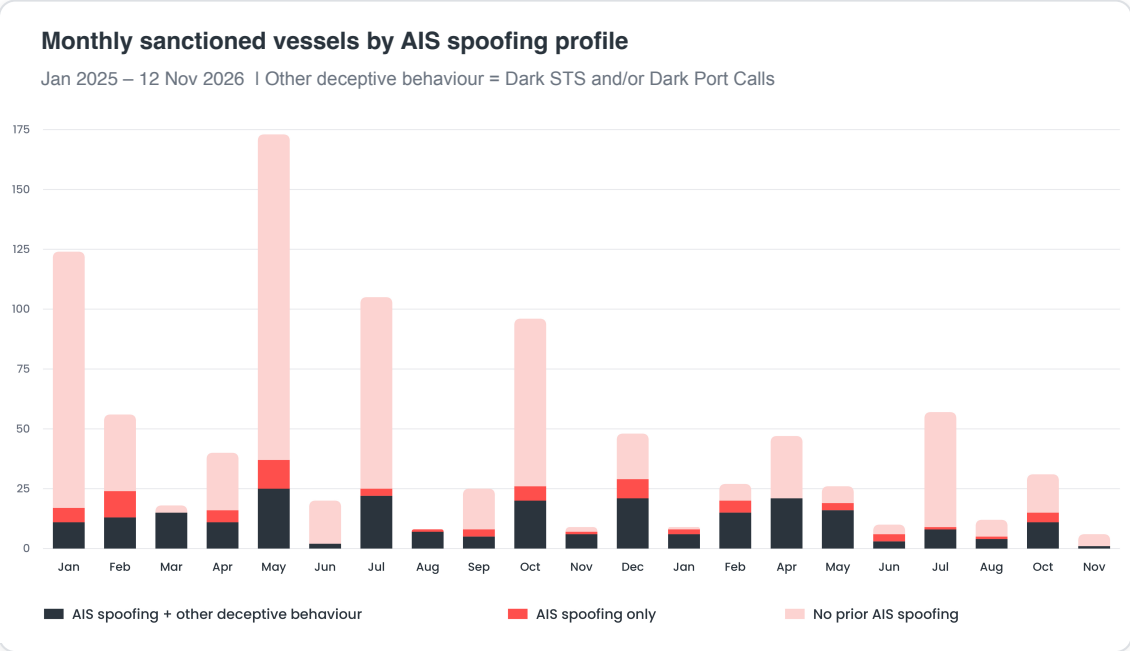
kpler

AIS spoofing rarely appears in isolation.

947 vessels sanctioned, Jan 2025 – 12 Nov 2026

318 vessels (33.6%) spoofed before designation:

- **Spoofing + other deceptive behaviour:** 243 vessels (76.4%)
- **Spoofing only:** 75 vessels (23.6%)



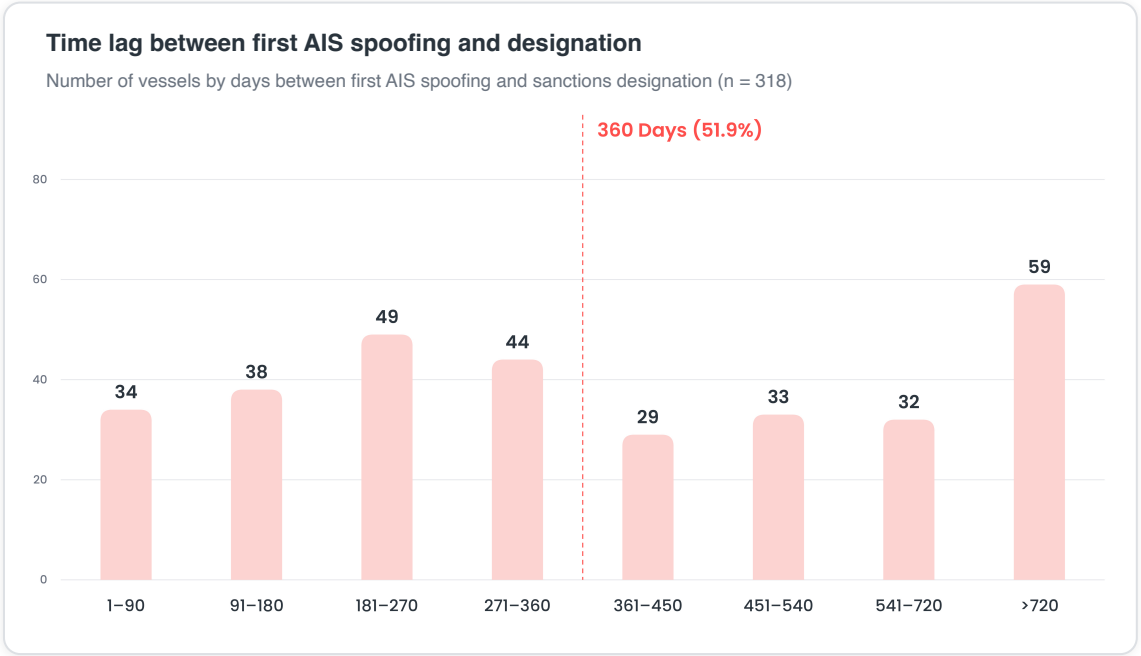
Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

kpler

AIS spoofing is an early signal: 51.9% of vessels were sanctioned within 360 days

Of the 318 vessels with AIS spoofing before designation:

- **121 vessels designated within nine months** of first spoofing: 34 within 90 days, 38 within 91–180, 49 within 181–270
- **59 vessels sanctioned more than two years later,** so the link is not always immediate
- **Best used as an early behavioural risk signal** within a wider vessel risk profile



Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

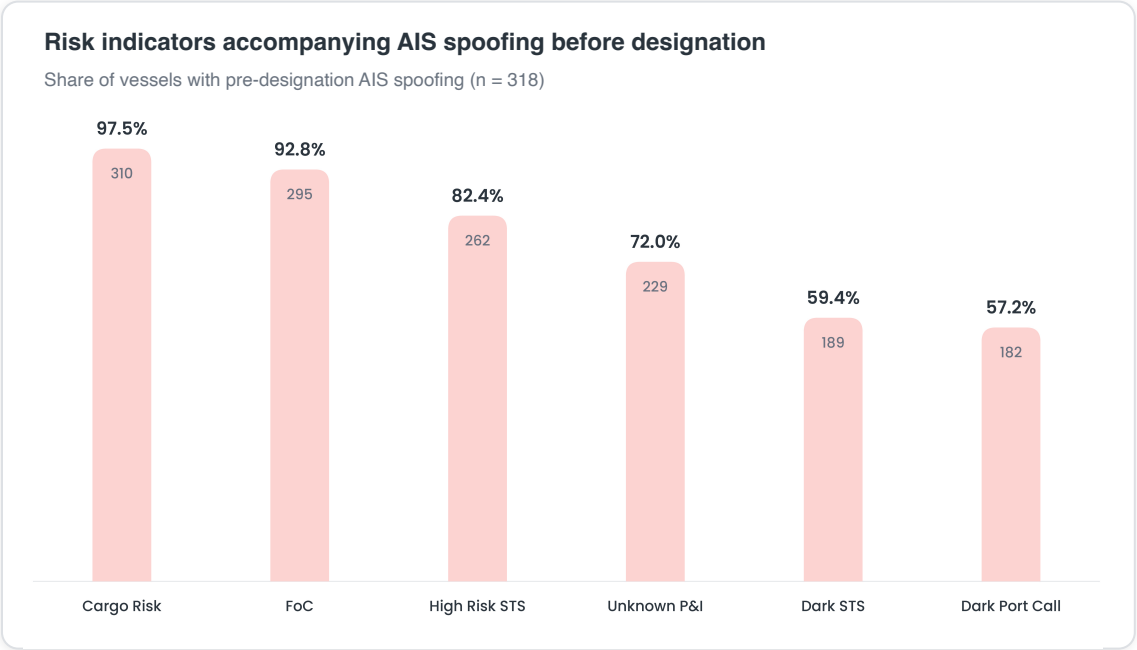
kpler

Vessels that spoof carry a broader high-risk profile before designation

Of the 318 vessels with AIS spoofing before designation:

- **Restricted cargo:** 310 (97.5%)
- **Flag of convenience: 295** (92.8%)
- **High-risk STS transfers:** 262 (82.4%)
- **Unknown P&I coverage:** 239 (72.0%)
- **Dark STS transfers:** 189 (59.4%)
- **Dark port calls:** 182 (57.2%)

Spoofing matters most as part of a wider risk profile, not as evidence of sanctions evasion on its own.



Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

False AIS positions do not all call for the same response

VESSEL-SPECIFIC SPOOFING

Enhanced due diligence, not an automatic finding

Check ownership, management, flag and identity history, and trace cargo origin and destination **before** drawing any conclusion on misconduct.

CORROBORATE THE TRACK

Test against independent location evidence

Review nearby AIS gaps, dark port calls and STS activity, and test the reported track against **satellite imagery** or other independent sources.

WHERE RISK REMAINS MATERIAL

Watchlisting or contractual controls

After due diligence, watchlisting or contractual controls may be appropriate – reported at the **confidence level the evidence supports**.

AREA-WIDE GNSS INTERFERENCE

Operational safety comes first

Alert crews and cross-check GNSS against **radar, visual navigation, inertial systems and coastal references**.

PRESERVE THE RECORD

Keep receiver and bridge logs

Preserve logs and assess any impact on **port calls, pilotage, STS activity or route deviations**.

DON'T OVER-ESCALATE

Affected does not mean higher risk

Assess vessel-level and area-wide anomalies **separately**, using multiple sensors rather than AIS alone.

Copyright © 2014 – 2025 Kpler. Confidential. All rights reserved. Contents included in this presentation must not be shared in any way possible with external parties without the consent of Kpler.

kpler

kpler

Thank you! Q&A

Dimitris Ampatzidis
Maritime Risk & Compliance Manager
dampatzidis@kpler.com

Ana Subasic
Trade Risk Analyst
asubasic@kpler.com

Yuan Li
Junior Risk & Compliance Analyst
yli@kpler.com