Spoofing, identity theft, position falsification: Athanor Engineering equips States against fraudsters and malicious actors at sea

Unveiled at the EURONAVAL exhibition, the new version of the WARSHIP AIS/X is set to establish the French SME on the international maritime surveillance market.

January 2025, off Taiwan. An undersea cable linking the island to the United States is damaged. The suspected vessel carried two AIS transponders and two MMSI numbers, and transmitted alternately under one identity or the other. One of them was even using the IMO number of a Vietnamese cargo ship, according to Lloyd's List Intelligence.

This episode sums up the problem Athanor Engineering is tackling. AIS, the system through which every ship announces who it is and where it is, relies entirely on the good faith of the transmitter. To unmask those who abuse it, the company officially presented the compact version of its WARSHIP AIS/X station on its EURONAVAL stand.

An SME exclusively serving States

Athanor Engineering has a distinctive feature: it has never worked for the civilian market. All its equipment has been developed to meet the needs of administrations engaged in State action at sea.

The WARSHIP AIS/X is currently fitted on French Navy vessels, part of the French Customs fleet and the Hellenic Navy. The company draws on ten years of field experience, with naval and coastal versions.

The new compact version retains the technological core of the unit custom-designed for the French Navy. Lighter, it can equip a patrol vessel as well as a helicopter, a maritime surveillance aircraft or a drone.

When ships cheat

The Taiwan case is far from isolated. In 2022 and 2023, oil tankers reported cruising off Cabinda, Angola, while they were actually loading in Venezuela; Spire Maritime estimates the capacity of these vessels at some 108 million barrels. In the Mediterranean, the Russian tanker *Kapitan Schemilkin* claimed to be sailing in circles off Greece in 2022, while it was actually east of Malta: satellite radar imagery exposed the deception, according to SkyTruth and Global Fishing Watch.

Another, more radical method: switching off the AIS. According to a study published in Science Advances in 2022, fishing vessels accumulated 1.6 million hours of AIS dark time per year between 2017 and 2019, roughly 6% of global activity, most often on the edges of national waters. The trawler *Oyang 77* vanished from screens nine times in two months in early 2019, on the edge of Argentina's EEZ.

Finally, in China in 2019, at least twenty coastal sites, including sixteen oil terminals, saw vessels (actually false tracks) appear within a radius of about 200 metres around a shore-based GPS jamming device. Thousands of ships, losing their true GPS position and seeing large numbers of false tracks, were probably affected, rendering the maritime picture unreadable, according to SkyTruth and C4ADS.

Unmasking the transmitter

Faced with these manoeuvres, a conventional AIS receiver sees nothing: it decodes messages without checking whether they are plausible. The WARSHIP AIS/X, by contrast, cross-checks two sources. On the one hand, the behaviour and identity of the tracks: trajectory, history, consistency between name, MMSI, IMO and ship type. On the other, the nature of the radio signal itself: its received power and its propagation time.

If a ship claims to be fifty nautical miles away while its signal arrives with the strength of a nearby transmitter, the inconsistency is obvious. The equipment then flags the false track, links several identities to a single transmitter and estimates its actual position. Athanor claims to be the only solution on the market today capable of both detecting and locating the source of the deception. The company is now working on the lower layers of the signal to identify the transmitting vessel itself.

The information does not stay on board. Each AIS/X station broadcasts its alerts, encrypted, to all units of the community within its VHF range: ships, aircraft, drones and coastal stations. Beyond that, relay is provided via GSM near the coast and via satellite further offshore. The system is also connected to CISE, the European maritime information sharing network, to which it immediately transmits any false track detected.

Setting sights on export

With this new version, Athanor Engineering is moving up a gear. Threatened undersea cables, evasion of oil sanctions, illegal fishing: grey zones are multiplying at sea, and with them the demand from foreign navies, coast guards and customs services for means of verifying what ships declare.

The SME enters this market with two strengths: operational references in two European navies and equipment free of any ITAR or equivalent restrictions, and therefore no dependence on the use of critical components. As it is classified as war materiel, however, the WARSHIP AIS/X remains subject to an export licence for each sale abroad.

Sources

1. Lloyd’s List Intelligence, “Taiwan is hunting one cable cutting vessel disguised with three separate digital identities”, 8 January 2025. https://www.lloydslistintelligence.com/resources/blog/taiwan-is-hunting-one-cable-cutting-vessel-disguised-with-three-separate-digital-identities
2. Spire Maritime, “Uncovering sanctioned oil exports using AIS Position Validation”, 2023. https://insights.spire.com/maritime/uncovering-sanctioned-oil-exports-using-ais-position-validation
3. SeafoodSource, “Global Fishing Watch, SkyTruth warn of vessels falsifying coordinates” (Kapitan Schemilkin case), 2022. https://seafoodsource.com/news/environment-sustainability/global-fishing-watch-skytruth-warn-of-vessels-falsifying-coordinates

4. H. Welch et al., “Hot spots of unseen fishing vessels”, Science Advances, vol. 8, no. 44, November 2022, DOI 10.1126/sciadv.abq2109. https://doi.org/10.1126/sciadv.abq2109
5. H. Welch, “When fishing boats go dark at sea, they’re often committing crimes” (Oyang 77 case), The Conversation, republished by gCaptain. https://gcaptain.com/when-fishing-boats-go-dark-at-sea-theyre-often-committing-crimes
6. M. Harris, “Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai”, MIT Technology Review, 15 November 2019. https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/
7. SkyTruth, “Systematic GPS Manipulation Occurring at Chinese Oil Terminals and Government Installations”, 12 December 2019. https://skytruth.org/insights/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations