Leurrage, usurpation d’identités, falsification de positions : Athanor Engineering arme les États contre les fraudeurs et les acteurs malveillants en mer

Présentée sur le salon EURONAVAL, la nouvelle version du WARSHIP AIS/X doit permettre à la PME française de s'imposer sur le marché international de la surveillance maritime.

Janvier 2025, au large de Taïwan. Un câble sous-marin reliant l'île aux États-Unis est endommagé. Le navire soupçonné embarquait deux transpondeurs AIS, deux numéros MMSI, et émettait tour à tour sous l'une ou l'autre identité. L'une d'elles empruntait même le numéro IMO d'un cargo vietnamien, selon Lloyd's List Intelligence.

L'épisode résume à lui seul le problème auquel s'attaque Athanor Engineering. L'AIS, ce système par lequel chaque navire annonce qui il est et où il se trouve, repose entièrement sur la bonne foi de l'émetteur. Pour démasquer ceux qui en abusent, la société a présenté officiellement, sur son stand d'EURONAVAL, la version compacte de sa station WARSHIP AIS/X.

Une PME au service exclusif des États

Athanor Engineering cultive une singularité : elle n'a jamais travaillé pour le marché civil. Tous ses équipements ont été développés pour répondre aux besoins d'administrations engagées dans l'action de l'État en mer.

Le WARSHIP AIS/X équipe aujourd'hui la Marine nationale, une partie de la flotte de la Douane française et la marine grecque. La société revendique dix ans d'expérience terrain, avec des déclinaisons navale et côtière.

La nouvelle version compacte reprend le cœur technologique du boîtier conçu sur mesure pour la marine française. Plus légère, elle peut équiper aussi bien un patrouilleur qu'un hélicoptère, un avion de surveillance ou un drone.

Quand les navires trichent

L'affaire taïwanaise est loin d'être isolée. En 2022 et 2023, des pétroliers ont annoncé croiser au large de Cabinda, en Angola, alors qu'ils chargeaient en réalité au Venezuela ; Spire Maritime évalue la capacité de ces navires à quelque 108 millions de barils. En Méditerranée, le pétrolier russe *Kapitan Schemilkin* prétendait tourner en rond au large de la Grèce en 2022, alors qu'il se trouvait à l'est de Malte : les images radar satellite ont trahi la supercherie, selon SkyTruth et Global Fishing Watch.

Autre méthode, plus radicale : couper l'AIS. Selon une étude publiée dans Science Advances en 2022, les navires de pêche ont cumulé 1,6 million d'heures d'extinction par an entre 2017 et 2019, soit environ 6 % de l'activité mondiale, le plus souvent en lisière des

eaux nationales. Le chalutier *Oyang 77* a ainsi disparu des écrans neuf fois en deux mois, début 2019, au bord de la ZEE argentine.

En Chine enfin, en 2019, au moins vingt sites côtiers, dont seize terminaux pétroliers, ont vu des navires (en réalité des fausses pistes) apparaîtrent dans un rayon de 200 mètres environ autour d'un dispositif de brouillage GPS installé à terre. Des milliers de navires, perdant leur position GPS réelle et voyant un grand nombre de fausses pistes ont probablement été concernés, rendant la situation maritime illisible, selon SkyTruth et C4ADS.

Démasquer l'émetteur

Face à ces manœuvres, un récepteur AIS classique ne voit rien : il décode les messages sans en vérifier la vraisemblance. Le WARSHIP AIS/X, lui, croise deux sources. D'un côté, le comportement des pistes et leur identité : trajectoire, historique, cohérence entre nom, MMSI, IMO et type de navire. De l'autre, la nature du signal radio lui-même : sa puissance à la réception et son temps de propagation.

Si un navire se dit à cinquante nautiques alors que son signal arrive avec la force d'un émetteur voisin, l'incohérence saute aux yeux. L'équipement signale alors la fausse piste, rattache plusieurs identités à un même émetteur et estime la position réelle de ce dernier. Athanor affirme être aujourd'hui la seule solution du marché à la fois capable de détecter et de localiser l'auteur de la tromperie. La société travaille désormais sur les couches basses du signal pour identifier le navire émetteur lui-même.

L'information ne reste pas à bord. Chaque station AIS/X diffuse ses alertes en chiffré à toutes les unités de la communauté dans sa portée VHF : navires, aéronefs, drones et stations côtières. Au-delà, le relais passe par le GSM près des côtes et par satellite plus au large. Le système est également connecté à CISE, le réseau européen de partage de l'information maritime, auquel il transmet immédiatement toute fausse piste détectée.

L'export en ligne de mire

Avec cette nouvelle version, Athanor Engineering change d'échelle. Câbles sous-marins menacés, contournement des sanctions pétrolières, pêche illicite : les zones grises se multiplient en mer, et avec elles la demande des marines, garde-côtes et douanes étrangères pour des moyens de vérifier ce que les navires déclarent.

La PME arrive sur ce marché avec deux atouts : des références opérationnelles dans deux marines européennes et un équipement libre de toute contrainte ITAR ou autre équivalent, donc sans dépendance à l’utilisation de composants critiques. Classé matériel de guerre, le WARSHIP AIS/X reste toutefois soumis à l'obtention d'une licence pour chaque vente à l'export.

Sources

1. Lloyd's List Intelligence, « Taiwan is hunting one cable cutting vessel disguised with three separate digital identities », 8 janvier 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 » (cas du Kapitan Schemilkin), 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, n° 44, novembre 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 » (cas de l'Oyang 77), The Conversation, repris par 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 novembre 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 décembre 2019. https://skytruth.org/insights/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations