Régis DELEPINE

SPOOFING AIS :
guerre économique
ou enjeux géostratégiques

Université BORDEAUX MONTAIGNE | Cyber criminalités

Promotion 2024-2025

RESUME

Le défi de l'usurpation de l'AIS ou spoofing dans l'industrie maritime persiste en tant que problème de longue date avec des conséquences importantes pour la sécurité mondiale, le commerce et la protection de l'environnement. Alors que la pratique consistant à tromper les autorités à travers de fausses identités ou des informations sur les navires obscurcies remonte à des siècles, l'usurpation a évolué avec les progrès technologiques, ce qui la rend de plus en plus complexe et difficile à combattre. Les récents conflits géopolitiques, tels que la guerre russe-ukrainienne et les sanctions ultérieures contre la Russie, ont déclenché une recrudescence des pratiques maritimes trompeuses. Ces événements ont servi de contexte géopolitique qui incite certaines entités à se livrer à des activités illicites pour évasion et contrebande de sanctions. Lorsque des navires se livrant à des activités illicites sont détectés, les conséquences sont graves. Il peut en résulter des sanctions, des saisies de marchandises, des actions en justice et des atteintes à la réputation des navires et de leurs propriétaires. Par conséquent, ces navires peuvent être rendus inutilisables pendant de longues périodes, entraînant des pertes financières substantielles pour leurs exploitants.

1. Introduction

Les pratiques trompeuses en matière de transport maritime ont des racines historiques profondes. Les marins ont utilisé des drapeaux naturels et des déguisements dès le XVIIe siècle. Ce précédent historique met en lumière l'ingéniosité persistante de ceux qui cherchent à tromper.
À l'ère actuelle de la technologie avancée, l'industrie maritime a développé des systèmes tels que l'AIS (système d'authentification automatique des navires) pour améliorer la transparence, la sécurité et la conformité réglementaire.
Cependant, les progrès technologiques ont également conduit à des tactiques trompeuses plus sophistiquées qui manipulent ou désactivent ces systèmes.
Le spoofing AIS représente une menace grandissante pour la sûreté maritime mondiale.

À la différence d'un simple brouillage, le spoofing consiste à injecter de fausses données dans le système AIS, ce qui peut induire en erreur les navires, les stations côtières et les systèmes de suivi maritime. Les impacts potentiels vont de la désorganisation du trafic à des risques de collision ou de piraterie.

Dans un contexte de forte densité de navigation, en particulier dans des zones stratégiques comme la mer Méditerranée, les conséquences peuvent être graves. Les flux maritimes, critiques pour le commerce mondial, dépendent d'un AIS fiable.

Plusieurs études récentes, notamment celles de l'Organisation Maritime Internationale (OMI) et de chercheurs indépendants, ont révélé des cas de spoofing volontaire :

- Création de navires fantômes,
- déplacements impossibles,
- disparition de vraies embarcations.

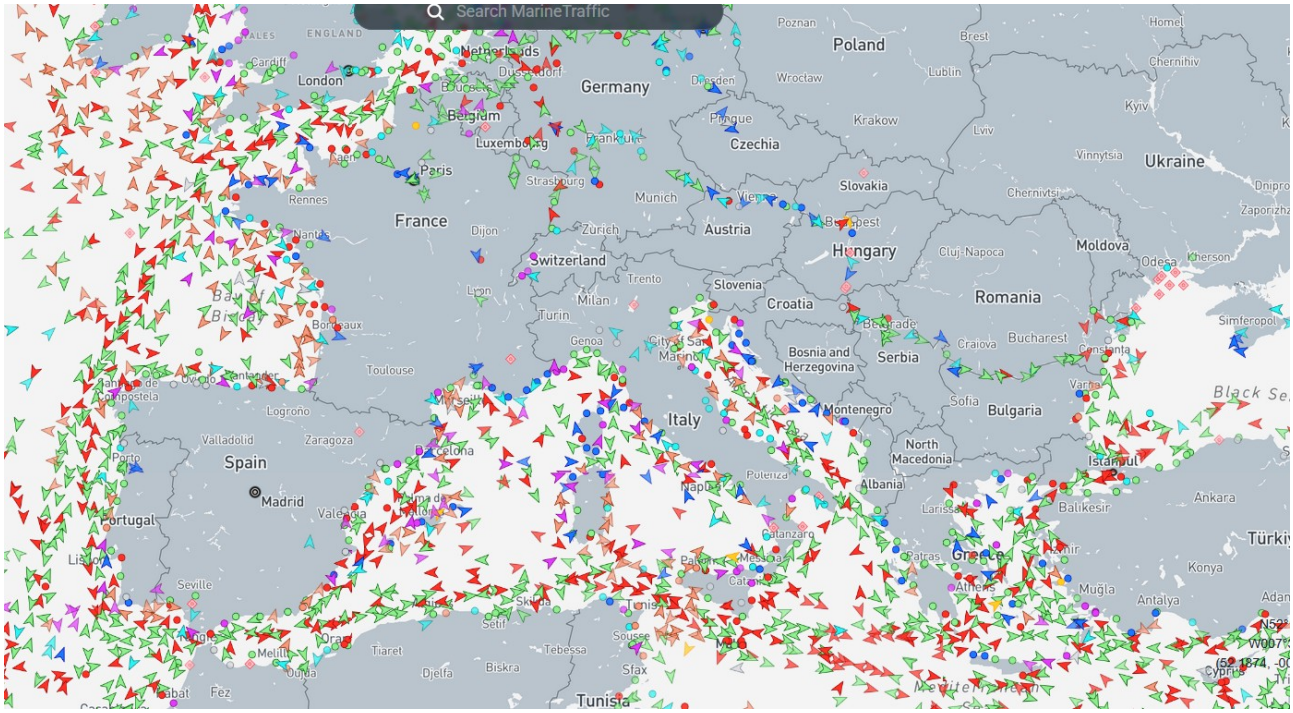


Figure 1 : *Trafic maritime capté par AIS en mer Méditerranée (source : MarineTraffic.com)*

Cette carte montre la densité exceptionnelle du trafic maritime dans la mer Méditerranée. Chaque triangle représente un navire transmettant sa position via l'AIS. On observe des concentrations notables près de Gibraltar, Marseille, Gênes, Athènes, Istanbul, et autour du canal de Suez. Cette densité rend la région particulièrement vulnérable à toute manipulation de données AIS, qu'elle soit accidentelle ou malveillante.

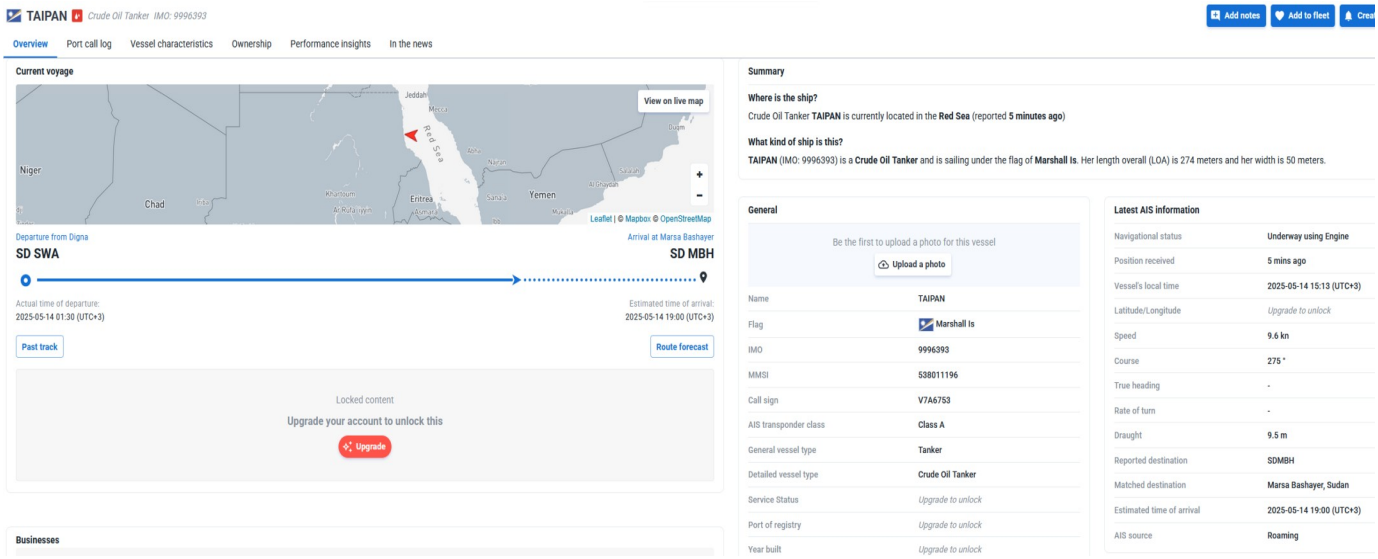
2. Fonctionnement de l'AIS

Le système AIS est un outil de sécurité et de surveillance maritime devenu incontournable dans la navigation moderne. Il repose sur un échange automatique de données entre navires, stations côtières et satellites pour améliorer la connaissance de la situation maritime en temps réel.

2.1 Principes de base

L'AIS permet à un navire d'émettre en continu un ensemble d'informations le concernant :

- Sa position GPS
- Son cap et sa vitesse
- l'Identité du navire (MMSI, nom)
- Le type de navire et dimensions
- La destination prévue et heure estimée d'arrivée



Navire TAIPAN de type Tanker en mer rouge, caractéristiques AIS, source « marine traffic »

Ces données sont transmises via des ondes radio VHF . Elles sont reçues par d'autres navires à proximité, par des stations côtières, ou par des satellites spécialisés, ce qui permet un suivi global en temps réel.

2.2 Types d'émetteurs

La convention internationale de 1974 pour la sauvegarde de la vie humaine en mer (Convention SOLAS) a imposé la mise en place d'un système international d'identification des navires, AIS :

- l’AIS de Classe A : Obligatoire pour les navires marchands et les navires de pêche de plus de 15 mètres. Ce système encapsule un nombre importants d’informations et Transmet celles ci toutes 10 secondes en navigation.
- l’AIS de Classe B : Utilisé par les navires de plaisance ou de petite taille (inférieur à 15 mètres) ou pour les filets posés par les pêcheurs. Moins puissant, envoie des messages toutes les 30 secondes avec un nombre moins important d’informations.
- Les satellites AIS (S-AIS) : permettent d’assurer une couverture mondiale en haute mer.

2.3 Objectifs et avantages

Le système AIS a plusieurs finalités :

- Prévention des collisions : Grâce à la visualisation des autres navires à proximité.
- Surveillance côtière : Les autorités maritimes peuvent suivre les mouvements en temps réel.
- Assistance à la navigation : Intégration des données AIS dans les systèmes ECDIS (système de visualisation de carte marine au format electronique).
- Analyse du trafic maritime : Données historiques exploitables pour des études logistiques ou environnementales.

2.4 Vulnérabilités du système

L’un des principaux problèmes de l’AIS est son manque de chiffrement et d’authentification des messages :

- Les signaux peuvent être interceptés et modifiés.
- Il est techniquement possible d’émettre de fausses données (spoofing) ou d’inonder le réseau de signaux erronés (attaque par saturation).
- Le système repose sur le GPS, qui lui-même peut être brouillé ou usurpé.

Ces failles sont aujourd’hui exploitées dans divers contextes, allant de la simple erreur technique à des manipulations stratégiques ou criminelles.

3. Qu’est-ce que le spoofing AIS ?

Le spoofing AIS consiste à émettre de fausses informations dans le système AIS, dans le but de dissimuler la position réelle d’un navire, simuler un trafic inexistant ou tromper les systèmes de surveillance maritime. Cette technique s’inscrit dans une logique de manipulation des données d’identification automatique à des fins illicites, politiques, stratégiques ou commerciales.

3.1 Définition technique

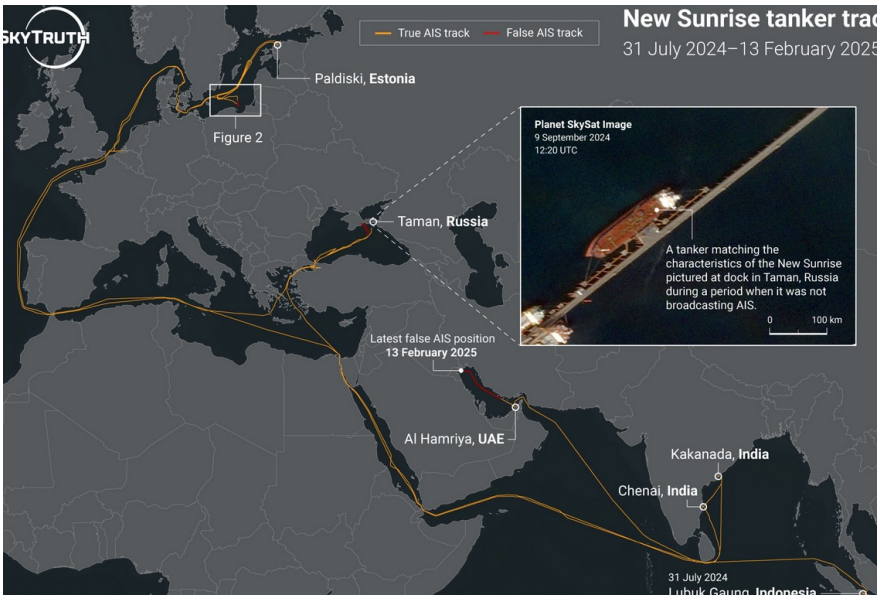
Le spoofing AIS repose sur la capacité d’injecter des messages AIS falsifiés dans le réseau. Cela peut se faire de différentes manières :

- En simulant un faux navire à une position déterminée (ghost ship).
- En modifiant les caractéristiques d’un navire réel (nom, MMSI, position).

- En dupliquant un navire en plusieurs endroits à la fois (mirroring).
- En créant de faux mouvements ou trajectoires (looping, hyper-speed).

3.2 Exemples concrets

- Navires de contrebande ou de pêche illégale qui masquent leur présence dans des zones interdites.
- Bateaux militaires ou de renseignement déguisés en navires civils.
- Manipulation de données économiques via de faux mouvements de pétroliers ou de cargos.



Le pétrolier NEW SUNRISE, battant pavillon libérien, diffuse un faux emplacement dans le golfe Persique après avoir laissé une traînée de déchets huileux et des questions restées sans réponse concernant ses activités dans les eaux européennes au cours des derniers mois.

- Sabotage d'analyses OSINT (Open Source Intelligence) basées sur les données AIS.

3.3 Technologies utilisées

Le spoofing AIS peut être effectué à l’aide :

- De simples émetteurs radio logiciels (SDR, Software Defined Radio) à faible coût.
- De stations AIS modifiées, terrestres ou embarquées.
- De logiciels open source capables de générer des messages AIS personnalisés.
- De relais satellite, capables de diffuser des signaux falsifiés à grande échelle.

3.4 Objectifs recherchés

Les motivations derrière le spoofing AIS sont diverses :

- Discrétion tactique : masquer les mouvements d’une flotte.
- Évasion de sanctions : simuler des routes commerciales conformes.

- Guerre informationnelle : déstabiliser les réseaux d’analyse maritime.
- Fausse alerte ou test de réaction de la part des autorités.

3.5 Limites de détection

Les systèmes de détection actuels rencontrent plusieurs obstacles :

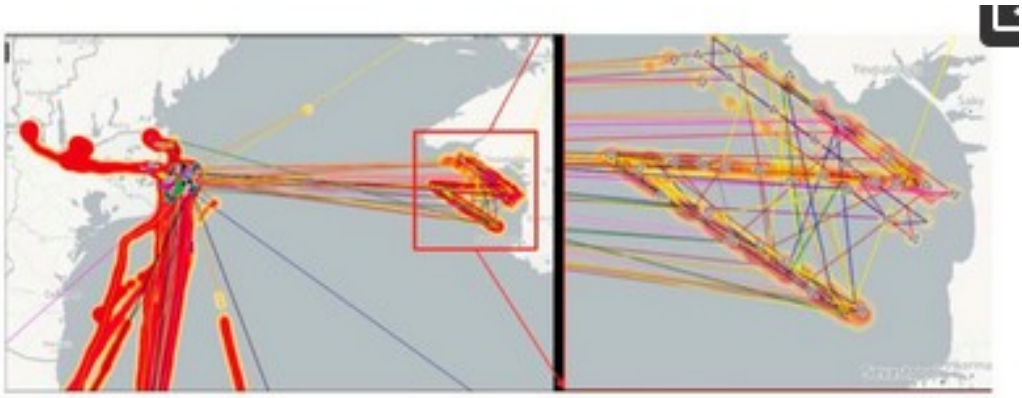
- L’AIS n’intègre pas de chiffrement ni de validation d’origine.
- Les fausses données se fondent dans les flux normaux.
- La vérification croisée (radar, imagerie satellite) nécessite des moyens coûteux et lents.

4. Études de cas de spoofing AIS

Le spoofing AIS n’est plus une hypothèse théorique : il est désormais bien documenté dans plusieurs contextes géopolitiques. Voici une sélection de cas réels, issus d’études ouvertes, de rapports spécialisés et d’observations OSINT.

4.1 Mer Noire et Russie (2014–2023)

Depuis l’annexion de la Crimée, la région de la mer Noire est un haut lieu du spoofing AIS. De nombreux navires civils apparaissent soudainement à terre ou dans des lieux improbables comme des aéroports ou des forêts. Ces anomalies visent à masquer des mouvements de navires militaires ou de contrebande.



Données Ais de navires usurpés pour dessiner un symbole Russe pro-guerre en mer noire

https://www.tradewindsnews.com/technology/ship-ais-data-spoofed-to-draw-pro-war-russian-z-symbol-in-black-sea/2-1-1456329

4.2 états unis

Des traces AIS de navires fantômes repérées en Californie, Une ONG américaine d’imagerie a relevé d’étranges traces AIS de navires qui se trouvaient pourtant à des milliers de kilomètres au

Même moment, défaillance du système GPS, hackers ?

Alors que l'AIS présentait des navigations en cercles totalement farfelues, les vrais navires se trouvaient en réalité à l'autre bout de la planète. | DR

4.3 Iran et contournement des sanctions

Des pétroliers iraniens simulent des escales fictives dans des ports légaux (Oman, Sri Lanka) alors qu'ils livrent du pétrole vers la Syrie ou la Chine. Le spoofing est utilisé pour dissimuler l'origine réelle de la cargaison, via des itinéraires virtuels.

- Tactique : changement de numéro MMSI (identité d'un navire) , fausses positions, dissimulation intermittente.
- *https://www.unitedagainstnucleariran.com/blog/december-2022-iran-tanker-tracking-and-year-review*

4.4 Venezuela et cargaisons illicites

Dans les eaux vénézuéliennes, le spoofing est largement utilisé pour masquer le trafic de pétrole brut malgré les sanctions américaines. Des navires disparaissent des écrans AIS pendant plusieurs jours, ou bien apparaissent dans des zones où ils ne sont pas physiquement présents.

- Un exemple fréquent est l'échange de cargaison en haute mer (ship-to-ship transfer) sans position AIS valide.

4.5 Port de Shanghai (Chine) – Brouillage et spoofing hybrides

En 2019, plusieurs centaines de navires autour de Shanghai ont vu leur position se déplacer soudainement de plusieurs kilomètres, parfois vers l'intérieur des terres. Le phénomène combinait spoofing AIS et spoofing GNSS, probablement à des fins de dissuasion ou d'expérimentation technologique.

- L'incident est apparu en parallèle de tensions commerciales et de mesures de contrôle portuaire.

5. Conséquences sur la sécurité maritime

Le spoofing AIS ne constitue pas seulement une anomalie technique : il représente une menace croissante pour la sécurité maritime globale. Ses effets peuvent être regroupés en trois grandes catégories :

- La sécurité des opérations en mer,
- la sûreté des transports internationaux
- et la gouvernance maritime mondiale.

5.1 Risques pour la navigation et la sécurité des navires

5.1.1 Collisions et incidents de navigation

Les faux signaux peuvent créer une situation où plusieurs navires pensent se trouver dans une même zone, ou à l'inverse, masquent la présence réelle d'un navire.

Cela augmente significativement le risque de collision, surtout dans les zones à fort trafic (détroits, ports, zones de transbordement).

5.1.2 Perte de conscience situationnelle

Lorsque le spoofing est combiné à des manipulations GPS, les capitaines peuvent être induits en erreur sur leur position réelle. Cela nuit à leur capacité de prise de décision, particulièrement en cas de mauvaise visibilité ou de trafic dense.

5.1.3 Incapacité à respecter les règles COLREG

La convention COLREG (Convention internationnale de régulation pour la prévention des collisions à la mer) repose sur la position et la route des navires pour établir des priorités de manœuvre. Des données erronées compromettent l'application de ces règles et rendent le comportement des navires imprévisible.

5.2 Menaces pour la sûreté maritime

5.2.1 Disparition de navires à des fins illégales

Le spoofing permet à des navires de se rendre invisibles ou de simuler des trajets légitimes. Il est largement utilisé dans :

- Le trafic de drogues ou d'armes.

- Le transport clandestin de pétrole (notamment dans le contournement des sanctions).
- La pêche illégale.

5.2.2 Infiltration de navires non identifiés

Dans certains cas, des navires non enregistrés peuvent usurper l'identité d'un autre pour accéder à des zones sensibles (ports commerciaux, installations pétrolières offshore, eaux territoriales). Cela représente un risque majeur de sûreté portuaire.

5.3 Impact sur la régulation et la surveillance maritime

5.3.1 Déstabilisation des dispositifs de surveillance

Les autorités maritimes, les organismes de contrôle des pêches, et les compagnies d'assurance maritime s'appuient de plus en plus sur les données AIS. La prolifération du spoofing remet en question la fiabilité de ces systèmes de contrôle.

5.3.2 Risques géopolitiques

L'usage stratégique du spoofing par certains États ou acteurs militaires pourrait provoquer des tensions régionales :

- Navigation simulée dans des zones contestées.
- Brouillage de navires adverses dans le cadre d'opérations hybrides.
- Usage de navires civils comme vecteurs de désinformation.

6. Moyens de détection et de lutte contre le spoofing AIS

Face à la montée du spoofing AIS, diverses stratégies ont été développées pour identifier, prévenir et atténuer ses effets.

Ces contre-mesures combinent des approches technologiques, opérationnelles et coopératives, à différents niveaux (armateurs, autorités, organismes internationaux).

6.1 Détection par analyse des données AIS

La méthode la plus courante repose sur l'analyse d'anomalies dans les flux de données AIS :

- Sauts de position soudains
- Vitesses irréalistes (ex. : 400 nœuds)
- Positions incohérentes avec le cap
- Trajectoires impossibles (ex. : à terre)

Exemple de saut de position AIS simulé (source : https://globalfishingwatch.org/data/example-of-ais-data-for-one-vessel-nov-1-2016/).

6.2 Corrélation avec des sources indépendantes

Pour confirmer un spoofing, on recoupe les données AIS avec d'autres systèmes :

- Imagerie satellite (visible, radar SAR)
- Systèmes radar portuaires
- Trajectoires historiques (vitesse moyenne, comportement habituel)

6.3 Surveillance collaborative et communautaire

Des plateformes ouvertes permettent de signaler et analyser les cas suspects :

- Global Fishing Watch
- MarineTraffic
- SkyTruth Alerts
- Windward (IA privée)

6.4 Contre-mesures embarquées ou portuaires

Certaines compagnies développent ou testent :

- Filtres anti-spoofing dans les logiciels de navigation
- Fusions AIS / Radar / EO (caméras optiques)
- Analyse comportementale par IA.

  Ces technologies sont encore coûteuses et peu standardisées, surtout pour la flotte marchande traditionnelle.

7. Enjeux géopolitiques et perspectives

Le spoofing AIS s'inscrit désormais dans un contexte plus large de cyber-conflits maritimes, d'enjeux économiques stratégiques et de luttes d'influence entre puissances. Ce phénomène révèle les failles d'un système mondial interconnecté, mais aussi les dynamiques d'adaptation des acteurs étatiques et privés.

7.1 Une technique d'influence et de dissimulation

Le spoofing AIS est fréquemment utilisé à des fins géopolitiques et militaires, notamment pour :

- Masquer des activités illicites ou sensibles : présence de navires de guerre, ravitaillement en mer, commerce sous sanctions.
- Détourner l'attention : simuler des trajets ou des présences fictives dans des zones sensibles.
- Exercer une pression diplomatique : par des incursions virtuelles dans des ZEE contestées.

Exemple : Des pétroliers affiliés à l'Iran et au Venezuela ont utilisé des identités AIS falsifiées pour contourner les sanctions américaines [1].

7.2 Vulnérabilité du commerce maritime mondial

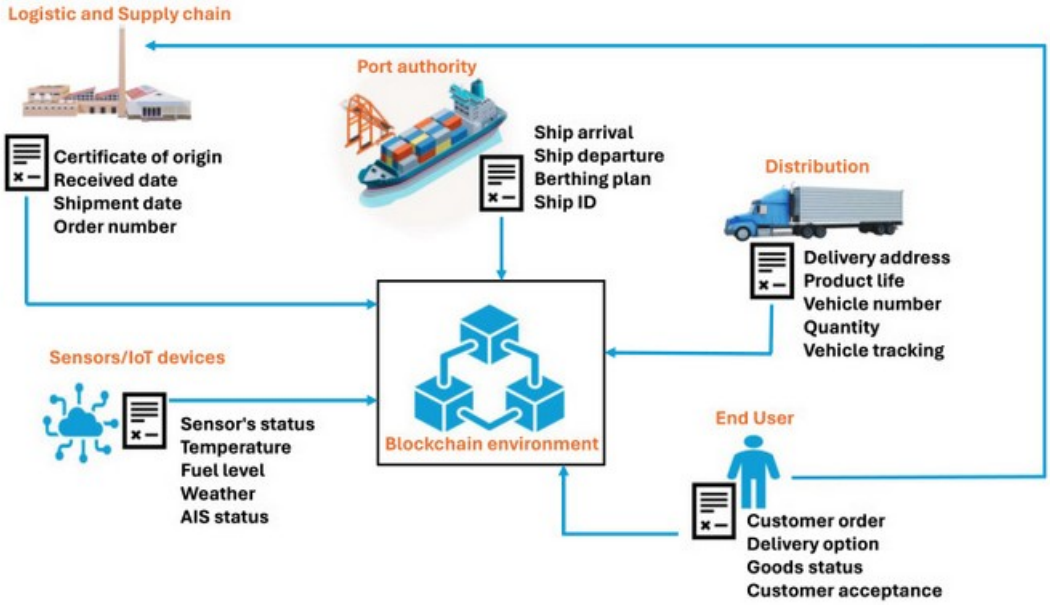
Plus de 90 % du commerce mondial dépend du transport maritime. Le spoofing AIS représente donc un risque systémique, capable de :

- Désarmer les mécanismes de surveillance portuaire
- Perturber les chaînes logistiques (retards, collisions, confusion)
- Fausser les données environnementales (suivi des émissions, pêche illégale)

7.3 Vers une nouvelle génération de systèmes AIS ?

Des pistes émergent pour rendre le système AIS plus résilient :

- Cryptographie : authentification des messages AIS via des clés publiques/privées [4].
- Corrélation multisources : comparaison avec des images satellites, radar passif, VHF et capteurs de bord.
- Blockchain maritime : traçabilité numérique inviolable des mouvements de navires [5].



https://www.sciencedirect.com/science/article/pii/S0167739X24001213

L’avenir du positionnement maritime repose sur la fusion des données et l’authenticité vérifiable des transmissions.

8. Conclusion et recommandations

Le spoofing AIS n’est plus un phénomène marginal : il est devenu un outil stratégique de manipulation de l’espace maritime, avec des conséquences concrètes sur la sécurité, le commerce et la stabilité géopolitique mondiale.

L’étude de cas et l’analyse de terrain confirment que la falsification des signaux AIS permet aujourd’hui de masquer des trafics illégaux, contourner des sanctions, mener des opérations militaires sous couverture, ou semer le doute dans des zones sensibles. Face à cette cybermenace hybride, les États comme les organismes maritimes doivent adapter rapidement leurs outils et leurs pratiques.

8.1 Bilan des vulnérabilités

Les failles les plus critiques identifiées sont :

- L’absence de chiffrement ou d’authentification dans le protocole AIS standard (VHF, classe A/B)
- La dépendance excessive à une seule source de positionnement (GNSS)
- Le manque de coordination internationale dans la détection des anomalies AIS
- La difficulté à attribuer une attaque ou falsification à un acteur identifiable

8.2 Recommandations techniques

Renforcer l’authentification des messages AIS

Implémenter des solutions de cryptographie légère, adaptées à la bande VHF.
Définir une norme OMI obligatoire de signature numérique des messages

Croiser les sources de données en temps réel

AIS + imagerie satellite + radar + Automatic Radar Plotting Aid (ARPA)
Systèmes de “vérification distribuée” (blockchain, consensus communautaire)

Mettre en place des systèmes de détection automatique des anomalies

Utilisation de l’intelligence artificielle (modèles de comportement navire/route)
Plateformes open-data de signalement participatif

8.3 Recommandations organisationnelles et politiques

Créer un cadre réglementaire international

Élaboration par l’OMI d’un protocole AIS v3 sécurisé
Sanctions pour usage frauduleux avéré de l’AIS

Former les acteurs du maritime à la détection du spoofing

Intégration dans les formations STCW, (Convention internationale sur les normes de formation des gens de mer).
Guides opérationnels pour les capitaines et opérateurs du suivi des trafics navires (VTS).

Développer une résilience numérique des chaînes logistiques

Audit de cybersécurité maritime pour les grands ports et armateurs
Simulation de crise et plans de réponse aux manipulations AIS

8.4 Perspectives de recherche

Des domaines à approfondir pour la recherche et l’innovation :

- Protocoles AIS cryptés résistants aux interférences
- Capteurs passifs ou biologiques pour la détection d’anomalies acoustiques
- Effets du spoofing sur les systèmes autonomes (navires sans équipage, drones)

Références bibliographiques :

- [1] Humphreys, T.E. (2022). *Shadows on the Sea: GNSS Spoofing and Maritime Misinformation*. Texas University GNSS Lab.
  [2] Parks, R., & Fishel, J.T. (2020). *Maritime Cybersecurity and the Threat of AIS Spoofing*. Naval War College Review, Vol. 73.
  [3] SkyTruth. (2023). *Tracking Deceptive Shipping Practices with AIS*. https://skytruth.org
  [4] IALA. (2021). *AIS Authentication and Encryption Feasibility Study*. IALA Guideline G1158.
  [5] UNCTAD. (2022). *Digitalization and Blockchain in Global Maritime Supply Chains*. United Nations Conference on Trade and Development.
- UNODC. (2022). *Maritime Crime and the Digital Threat*. United Nations Office on Drugs and Crime.
- OMI , organisation maritime internationnale, *https://www.imo.org/* . IMO. (2023). *Guidelines on Maritime Cyber Risk Management*. MSC-FAL.1/Circ.3.
- Tsioufis, T., & Lagkas, T. (2021). *AIS Data Spoofing and Maritime Cybersecurity: A Review*. *Journal of Marine Science and Engineering*, 9(11), 1219.
- Shao, H. et al. (2020). *Detecting AIS Spoofing using Multi-Source Fusion and AI*. *IEEE Transactions on Intelligent Transportation Systems*.
- IALA. (2021). *Feasibility Study on Securing AIS Transmissions*. IALA Guideline G1158.
- *https://www.polestarglobal.com/resources/ais-spoofing/*