IPRR IMPACT AND POLICY RESEARCH REVIEW
Managed & Published by
IMPRI IMPACT AND POLICY RESEARCH INSTITUTE

Impact and Policy Research Review (IPRR)
Vol. 4, Issue 2, July - December 2025, pp. 21-34

Policy Perspective

IMPRI IMPACT AND POLICY RESEARCH INSTITUTE
•ETHICAL •NON-PARTISAN •INDEPENDENT

Fusing AIS And OSINT: A Policy Blueprint For Smart Maritime Trade Compliance And Surveillance

Bhavya Bhav[1] & Ananta Proshad Chakraborty[2]

Abstract

The global maritime sector faces multiple challenges from organized criminal networks and their illegal activities, geopolitical tensions, sanctions evasion, and ship collisions, among others. These challenges require monitoring tools to reduce vulnerabilities by tracking the activities of those ships in real-time and responding accordingly. In this context, AIS helps track a vessel's location and activities of the vessel. Although it faces challenges in providing the identity of the vessel, its signals can sometimes be misleading. In contrast, OSINT can verify ship locations and analyze satellite imagery and detect suspicious actors, thereby revealing the identity of the vessel. Although without AIS signals, the ability to track a ship becomes extremely limited. Therefore, this paper proposes integrating Automatic Identification System (AIS) and Open-Source Intelligence (OSINT) to create a stronger ecosystem for maritime security and compliance, as the integration of both technologies complements each other. This analysis highlights the institutional, legal, and technical criteria required for the actual deployment, drawing on case studies of the sanctions frameworks of the European Union and the Indian Ocean. The results indicate that improving the security, equity, and resilience of international maritime trade requires integrating AIS and OSINT data.

Keywords: *AIS-OSINT integration, maritime surveillance, smart compliance, global trade governance, maritime intelligence.*

[1] IIT Tirupati, Andhra Pradesh - hs24m106@iittp.ac.in
[2] School Of International Relations And Peace Studies, Nalanda University, Bihar - anantapcb@gmail.com

1 Introduction

Maritime trade stands at the crossroads of global economic recovery, geopolitical instability, and rapid technological transformation. In 2023, global seaborne trade rebounded to 12.3 billion tons and is projected to grow steadily (Chirls, 2024). However, persistent disruptions, from the Black Sea and Red Sea conflicts to climate-related risks, continue to expose vulnerabilities in the world's shipping arteries. Freight rates have surged due to rerouting, port congestion, and increasing operational, with ripple effects on global inflation and food security (UNCTAD, 2024). The International Maritime Organisation (IMO) and regional authorities are facing mounting pressure to modernise surveillance and compliance mechanisms, as fraudulent ship registrations, "shadow fleet" operations, and AIS (Automatic Identification System) blackouts are undermining transparency, safety, and enforcement (European Parliament, 2024).

These dynamics underscore an urgent policy imperative: maritime governance must evolve from reactive monitoring to integrated, intelligence-driven oversight. Against this backdrop, the fusion of Automatic Identification System (AIS) and Open-Source Intelligence (OSINT) offers a robust framework for smart maritime trade compliance and surveillance. AIS provides near-real-time vessel identification and tracking; however, it cannot expose deceptive practices such as transponder spoofing, falsified registries, or illicit ship-to-ship transfers (Turgeon, 2024). OSINT, encompassing satellite imagery, social media, commercial databases, and trade records, add contextual intelligence that can verify, augment, or challenge AIS data. Together, these tools can detect dark fleet operations, monitor sanctions evasion, and uncover supply-chain manipulations that traditional enforcement misses (Meehling, n.d.). By integrating both, policymakers can transition toward predictive and adaptive governance, enhancing maritime domain awareness while promoting accountability and compliance.

However, the potential of AIS-OSINT fusion extends beyond enforcement. It provides a pathway for data-driven policymaking that aligns with international frameworks for sustainability and security. For example, the IMO's new regulatory scoping exercises on illegal operations, the push for greener and more resilient supply chains, and ongoing debates on seafarer welfare all highlight the need for transparent, interoperable information systems (IMO Takes Action on Seafarers'

Rights, Substandard Shipping, 2025). A unified AIS-OSINT approach can support these efforts by enhancing situational awareness, facilitating coordination among maritime authorities, and providing early warning of systemic risks, ranging from environmental disasters to illicit trade networks. This policy blueprint thus argues that fusing AIS and OSINT is not merely a technical upgrade but a strategic necessity. It offers an opportunity to reimagine maritime trade governance through more innovative, collaborative, and ethically grounded surveillance.

2 Understanding AIS and OSINT: Technical and Policy Foundations

The technical characteristics and policy foundations of AIS and OSINT differ significantly from one another. AIS tracks and identifies vessels using standardised technical protocols. However, to support intelligence activities, OSINT relies on open source data collection, analysis, and the intelligence tradecraft. The main policy factors for both technologies in their respective domains are transparency, accountability, governance, and ethical use (Chen et al., 2024).

2.1 Automatic Identification System

The 1974 International Convention of SOLAS has made AIS mandatory as a marine safety and monitoring system. This system is designed to avoid ship collisions. Ships with a gross tonnage of 300 tons or more are required to send AIS signals while undertaking international journeys, allowing them to be tracked by satellites and receivers along the coasts of other nations (IMO, 2022). It enhances maritime domain awareness, aids in search and rescue operations, and ensures navigation safety. The vast amount of data obtained by AIS enables global-scale monitoring, which can be integrated with security solutions (Da Silva Figueiredo et al., 2025). However, the respective system also has its limitations. For instance, it is very common for ships to disable or turn off their AIS transponders, which is generally termed as 'going dark.' Ships may also use false coordinates to spoof locations, duplicate Maritime Mobile Service Identity,[3] falsify destination and cargo information, and drift outside of satellite coverage. These manipulation techniques have become increasingly common among vessels in an effort to avoid sanctions or engage in illicit trading activities (Bergman, 2021). To ensure interoperable

[3] MMSI: For tracking and communication purposes, a vessel's radio and AIS signals are uniquely identified by a nine-digit identifier.

operation between devices and systems, AIS is governed by international standards, particularly those established by organisations such as the IEC[4] and IMO, as mentioned above. Ships use the AIS to track their movements and communicate with other vessels over radio frequencies, Time Division Multiple Access (TDMA),[5] enabling precise ship tracking and communication through Very High Frequency (VHF)[6] maritime channels. AIS transponders utilize High-Level Data Link Control (HDLC)[7] protocols and Gaussian Minimum Shift Keying (GMSK)[8] modulation, which automatically resolves channel contention even in high-traffic situations (Chen et al., 2024)

2.2 AIS: Policy Foundations

The principles of the NIST AI Risk Management Framework serve as the foundation for the responsible use of AI technologies.[9] Essential policy measures involve establishing governance teams within organisations tasked with developing and overseeing the AIS system, regularly assessing for bias and fairness, maintaining transparency in AI-generated decisions, particularly in insurance or claims contexts, and ensuring adherence through ongoing monitoring during the system's duration (Da Silva Figueiredo et al., 2025).

2.3 Open Source Intelligence (OSINT)

Open Source Intelligence is a method that gathers intelligence/information from publicly available data or sources. In the maritime domain, it collects data from satellite images, port records, ship registries, financial documents, and also social media. (Pohontu & Ermolai, 2024). Through data collection, it helps identify unusual patterns in vessel behavior. For example, covert ship-to-ship transfers or

[4] The International Electrotechnical Commission (IEC): Global technical standards for maritime communication systems, like AIS, are established by this international standards organization.
[5] A communication technique that allows multiple ships to send AIS data without interference by dividing radio frequencies into time slots.
[6] AIS uses this radio frequency band for dependable long-distance ship-to-ship and ship-to-shore communication.
[7] A data transmission protocol that provides secure and accurate delivery of AIS messages.
[8] AIS uses a digital modulation technique to improve the efficiency, stability, and noise resistance of signal transmission.
[9] The National Institute of Standards and Technology developed the voluntary and adaptable NIST AI Risk Management Framework (RMF) to manage risks associated with artificial intelligence. It divides AI risk management tasks into four main categories: Map, Measure, Manage, and Govern. The framework helps companies identify, assess, mitigate, and track the potential risks and benefits of AI systems throughout their entire lifecycle, promoting ethical and trustworthy AI development and application.

suspicious voyages to ports that may have been sanctioned (Larsen et al., 2023). OSINT aids in addressing a few important questions for the authorities, such as the identity of the owner, who owns the vessel, and who earns the profit? Previous suspicious behaviour or not? Whether the AIS reports conflict with the satellite imagery found through OSINT or not? Whether sanctioned entities have political ties or not, etc. Technical tracking alone is incapable of uncovering hidden relationships, and that is where OSINT helps expose them. Linking shipping practices to international legal frameworks, such as sanctions programs or counter-piracy initiatives, promotes accountability (Pohontu & Ermolai, 2024). Moreover, this method is now an essential component of maritime intelligence due to the global expansion of commercial satellites and digital data. Transparency is now a shared governance responsibility due to the growing contributions of civil society, journalists, and private organizations to maritime monitoring (Larsen et al., 2023).

3 The Synergy: Why AIS and OSINT Must Work Together?

AIS shows a ship's location and its activities. On the other hand, OSINT reveals the ship's identity and the significance of its actions. Together, if integrated, they create an ecosystem of security and compliance intelligence. AIS by itself is unable to provide context. It is legal for a ship to turn off tracking in proximity to crowded ports. In that context, OSINT can detect suspicious actors, but it is nearly impossible to track a ship's movements in the absence of AIS. Hence, both are complementary to each other (Chen et al., 2024). Specifically, if both are integrated, the benefits would include verifying satellite images against false or misleading AIS signals, identifying owners and connections to illegal networks, and authorities can use behavioral patterns to predict future violations. Through their combination, maritime awareness becomes proactive rather than reactive. Global trade governance initiatives, counter-piracy missions, and the enforcement of international sanctions have already been impacted by this collaboration (Da Silva Figueiredo et al., 2025; Chen et al., 2024).

4 Challenges in Fusing AIS and OSINT

Although combining AIS and OSINT provides more robust maritime surveillance, integration is challenging due to several significant issues. The issues include the ethical, political, legal, and technical aspects. For example, AIS-OSINT systems collect a substantial amount of behavioural information about crew members, businesses or companies, and the ships themselves. There are concerns about privacy rights and limits in surveillance, as excessive monitoring may lead to violations of companies' privacy or discrimination against nationals. Shipping companies, which are often innocent, may be vulnerable to data misrepresentation, especially small-scale companies that lack sufficient legal protections.

Therefore, it is necessary to stop discrimination, wrongful detention of the ships, and data abuse. Without verified sources, OSINT also carries the risk of disseminating false information (Larsen et al., 2023). Moreover, maritime intelligence must balance the political challenges, as international relations are significantly impacted by maritime intelligence. Governments frequently disagree about what constitutes illegal actions. For instance, the imposition of sanctions by one country may be interpreted as economic aggression by another country. Although many developing countries criticise such sanctions as hurting the world's energy supply (OFAC, 2024). Furthermore, there are challenges in the legal arena because digital intelligence is not yet entirely reflected in maritime laws. Additionally, concerns remain regarding jurisdiction, as many AIS-OSINT enforcement operations occur outside territorial waters. Foreign ships are allowed to navigate freely in international waters under the United Nations Convention on the Law of the Sea (UNCLOS), 1982. There are restrictions on the extent to which governments can use intelligence to support or justify inspections and sanctions. In fact, some doubts remain related to data ownership. Private companies own the majority of the satellite surveillance and AIS tools.

Hence, countries that monitor data may not be able to obtain the necessary information. Lastly, advanced analytics, fast data processing, and safe digital systems are necessary for the fusion of AIS-OSINT. Developing countries lack many of these capabilities. Another significant issue is the quality of the data (Soner et al., 2023). Although OSINT sources may be limited, AIS data can be tampered with

or contain errors. False Alerts can arise from the mismatched/tempered datasets. For instance, bad weather can cause a ship to lose AIS contact, and the authorities may mistakenly presume that the ship is evading sanctions. Another, more specific technical challenge is about cybersecurity. To deceive naval forces, AIS can be compromised, allowing fake signals to be generated and transmitted (Sage, 2023).

5 Case Study: Indian Ocean Piracy and Smuggling Networks

The Indian Ocean remains one of the world's most vital maritime corridors, facilitating a large share of global oil shipments and containerized trade. However, its vastness and porous governance architecture have made it fertile ground for piracy, arms trafficking, narcotics smuggling, and illicit trade in wildlife and minerals. According to the International Maritime Bureau (IMB) 2025 Annual Report, in 2024, a total of 126 crew members were taken hostage, compared to 73 in 2023 and 41 in 2022. Twelve crew were reported kidnapped, compared to 14 in 2023 and two in 2022, while a further 12 crew were threatened and one was injured in 2024 (ICC International Maritime Bureau, 2025). Although the number of successful high-profile hijackings has declined, smaller-scale piracy and smuggling networks continue to adapt and operate with impunity (Ibrahim, 2024). The threat is particularly acute in areas such as the Horn of Africa, the Arabian Sea, and the western coast of India, where non-state maritime threats converge, and trade compliance becomes increasingly challenged.

According to one strategic assessment, maritime piracy and the security of maritime traffic remain key strategic issues for the region (Cordesman, 2016). Many smugglers exploit weakened regulatory enforcement, trans-shipment loopholes, and the use of "dark" vessels that either deactivate their AIS transponders or spoof their signals. This blending of legitimate trade flows with illicit networks hampers both maritime trade compliance and surveillance. Traditional maritime domain-awareness frameworks struggle to monitor these dynamic networks because of fragmented data sharing among littoral states, jurisdictional issues between military/naval authorities, customs and port administration, and the technical challenge of verifying vessel identity and cargo. For example, IUU (illegal, unreported, and unregulated) fishing in the Indian Ocean is strongly linked to trafficking and smuggling networks, further complicating

enforcement efforts (Camurri, 2022). From a policy perspective, fusing AIS data with OSINT offers a viable and innovative response. By combining real-time vessel tracking with social-media monitoring, port-call records, commercial satellite imagery, and AIS anomaly detection, policymakers can uncover behavioral patterns that indicate illicit activity, such as repeated transponder gaps, unreported at-sea rendezvous, or anomalous route deviations. Machine-learning algorithms can flag high-risk vessels for inspection and risk profiling, thereby enhancing compliance audits and interdiction. Thus, the piracy and smuggling ecosystem in the Indian Ocean underscores the urgency of integrating technological innovation with cooperative governance. AIS-OSINT fusion represents not merely surveillance enhancement, but a strategic policy tool for securing maritime trade lanes, strengthening compliance, and countering transnational maritime crime.

6 Case Study: EU and U.S. Maritime Sanctions Monitoring

Both the European Union (EU) and the United States (U.S.) have developed advanced systems for maritime sanctions monitoring to counter illicit trade, sanctions evasion, and the rise of "dark fleets." These efforts increasingly rely on integrating AIS data with OSINT, such as satellite imagery, port records, and corporate registries. The U.S. model, led by the Office of Foreign Assets Control (OFAC), combines regulatory enforcement with public guidance to industry. OFAC's *Sanctions Guidance for the Maritime Shipping Industry* (U.S. Treasury, 2024) and the *2025 Advisory on Iranian Oil Sanctions Evasion* detail deceptive practices like AIS manipulation, flag hopping, and ship-to-ship transfers (OFAC, 2025). The U.S. encourages financial institutions and insurers to use AIS-OSINT fusion, comparing vessel tracks with satellite imagery and registry data, to detect high-risk behavior (K&L Gates, n.d.).

This model leverages financial pressure and transparency to enforce sanctions worldwide. The EU emphasizes collective surveillance and data sharing across member states. The European Maritime Safety Agency (EMSA) operates *SafeSeaNet*, integrating terrestrial and satellite-AIS data with Earth-observation imagery to monitor vessel movements (SafeSeaANET - EMSA - European Maritime Safety Agency, n.d.). A European Parliament analysis highlights how EMSA tools have been adapted for sanctions enforcement, especially in tracking oil shipments

linked to Russia (EPRS, 2024). EU analysts use multi-source fusion: AIS gap detection followed by OSINT verification through imagery, port logs, and ownership searches. This creates actionable intelligence for national enforcement agencies while maintaining a shared situational awareness framework. Comparatively, the U.S. model excels in *deterrence and enforcement*, while the EU system provides *broad situational visibility and coordination*. Both face challenges, spoofed AIS data, fragmented jurisdiction, and limited satellite access, but their complementary approaches demonstrate the value of AIS-OSINT fusion. Together, the EU and U.S. experiences form a global benchmark for "smart compliance," showing that integrating AIS and OSINT not only strengthens sanctions enforcement but also builds transparency across maritime trade.

Policy Blueprint: Smart Maritime Trade Compliance and Surveillance

To counter the maritime challenges, a new paradigm, *Smart Maritime Trade Compliance and Surveillance* (SMTCS), is needed. The integration of AIS and OSINT provides an advanced intelligence architecture that enables transforming maritime oversight from reactive monitoring to predictive governance. This blueprint outlines a governance and implementation framework for SMTCS based on *four pillars: principles for innovative surveillance governance, institutional reforms, legal and regulatory enablers*, and *capacity-building mechanisms*.

7 Principles for Smart Surveillance Governance

7.1 Transparency and Accountability by Design

Intelligent maritime surveillance must embed transparency as a structural feature. AIS-OSINT fusion generates sensitive behavioural data about vessels, companies, and crew; thus, data collection must follow verifiable audit trails. Governance protocols should adopt "accountability by design" standards, modelled on the NIST AI Risk Management Framework, ensuring all algorithmic decisions are explainable, documented, and reviewable by independent authorities.

7.2 Ethical and Proportionate Use of Intelligence

Governments must ensure that surveillance remains proportionate to the risks it aims to address. Overcollection or misuse of OSINT may violate privacy or

commercial rights. Surveillance ethics committees, comprising representatives from the public, private, and civil society sectors, should evaluate data access requests and prevent the discriminatory targeting or wrongful detention of vessels.

7.3 Interoperability and Data Integrity

The SMTCS must align with IMO, IEC, and UNCLOS frameworks to ensure data interoperability and integrity. AIS and OSINT systems should follow standardized metadata schemes, cryptographic authentication, and open APIs that allow real-time data exchange without compromising confidentiality.

8 Institutional Reforms

8.1 Establish a Global Maritime Intelligence Fusion Centre (GMIFC)

It could be established under the leadership of the International Maritime Organization (IMO), in collaboration with major maritime powers and regional security organisations such as the Indian Ocean Rim Association (IORA), ASEAN, and the Gulf of Guinea Commission. It would serve as a multi-source intelligence hub connecting AIS, OSINT, and satellite feeds.

8.2 Public-Private Partnerships (PPP) for Data Access

PPPs are essential because the majority of AIS and satellite data is privately held. Governments and commercial providers should work out safe data-sharing agreements that benefit both parties, such as providing discounted access in return for capacity support, co-branding, or recognition within the SMTCS network.

9 Legal and Regulatory Instruments

9.1 Recognition of Digital Intelligence in Maritime Law

In line with UNCLOS frameworks, AIS manipulation alerts and OSINT-verified anomalies should be clearly identified as valid triggers for compliance checks, boarding decisions, and sanctions investigations. This reduces ambiguity in international waters and strengthens the legal basis for digital enforcement actions. IMO member states may include AIS-OSINT under UNCLOS-based national frameworks to legally validate them.

9.2 Data Governance, Privacy, and Accountability

International regulations must specify which data is open for security and which information needs higher security. Establishing oversight organizations by governments to regulate the use of analytics is necessary to prevent discrimination, detentions, or harm to one's reputation resulting from the misuse of faulty intelligence. Documented verification procedures must serve as the foundation for all enforcement decisions.

9.3 Obligation of the Maritime Industry

To ensure consistent evidentiary standards and risk indicators, sanctions and enforcement practices should be harmonised through regional coordination, particularly between central sanctioning authorities such as the United States and the European Union, to prevent shadow fleets from exploiting flag shopping and regulatory arbitrage.

10 Capacity Building and Inclusion

10.1 Equitable Access to Technology and Funding

For developing nations near important trade routes, international donors and development banks should prioritize maritime digitization projects that provide safe AIS upgrades, reasonably priced satellite services, and AI-enabled monitoring. This enhances global surveillance coverage.

10.2 Human Skills Development and Institutional Strengthening

Specialized training programs should emphasize analytics, OSINT verification, cybersecurity, and maritime law enforcement. Joint academies and simulation exercises promote cooperation among navies, coast guards, and customs agencies, resulting in more coordinated responses.

10.3 *Inclusive Participation of Local Stakeholders*

It is essential to involve port employees, small-scale shipping operators, and fishing communities in grievance procedures and awareness campaigns. By shielding crews from erroneous notifications or misidentification, digital monitoring systems will gain credibility and lessen suspicion.

10.4 Regional Information Sharing Networks

Regarding piracy, smuggling, and sanctions evasion, neighbouring states ought to establish official regional intelligence exchanges, shared watchlists, and early warning platforms. Additionally, regional centres ensure that information does not remain isolated in national headquarters, but instead reaches frontline authorities swiftly.

11 Conclusion

Maritime trade remains the backbone of the global economy. However, it is under threat from geopolitical tensions, cyber vulnerabilities, and illegal networks that exploit weaknesses in current governance frameworks. AIS is an important tool for ensuring safety and navigation. However, when it comes to complex threats like piracy, sanctions evasion, or "shadow fleet" operations, AIS becomes inadequate. As a result, AIS and OSINT integration provides a more proactive, smart, and contextual approach to maritime surveillance. Although this fusion improves maritime security and trade compliance, there are challenges regarding privacy, jurisdiction, and shared accountability etc. Strengthening legal frameworks, encouraging institutional collaboration, ensuring equitable access to technology, and incorporating ethical safeguards helps increase the system's legitimacy and trustworthiness. A responsible and predictive maritime intelligence system based on collaborative governance would be required to safeguard maritime supply chains and promote economic resilience in the future. Thus, AIS-OSINT fusion is a strategic investment in the long-term stability of global maritime trade rather than being just a technical development.

References

AIS transponders. (2022). https://www.imo.org/en/ourwork/safety/pages/ais.aspx

Bergman (2021). Systematic data analysis reveals false vessel tracks. Global Fishing Watch. https://globalfishingwatch.org/data/analysis-reveals-false-vessel-tracks/

Camurri, M. (2022, February 10). *Maritime security in the Indian Ocean: The practice of illegal, unreported and unregulated (IUU) fishing*. Mondo Internazionale.

https://mondointernazionale.org/en/focus-allegati/maritime-security-in-the-indian-ocean-the-practice-of-illegal-unreported-and-unregulated-iuu-fishing

Chen, Y., Qi, X., Huang, C., & Zheng, J. (2024). A data fusion method for maritime traffic surveillance: The fusion of AIS data and VHF speech information. Ocean Engineering, 311, 118953. https://doi.org/10.1016/j.oceaneng.2024.118953

Chirls, S. (2024, October 23). Containers lagged ocean shipping gains in 2023, UN report finds. FreightWaves. https://www.freightwaves.com/news/containers-lagged-ocean-shipping-gains-in-2023-un-report-finds

Cordesman, A. H. (2024). *Indian Ocean Region Strategic Net Assessment: The Red Sea and Horn Subregion*. https://www.csis.org/analysis/indian-ocean-region-strategic-net-assessment-red-sea-and-horn-subregion

Da Silva Figueiredo, R., Simões, J., De Farias, C. M., & Caprace, J. (2025). A comprehensive data fusion model for AIS-Based maritime research. 2022 25th International Conference on Information Fusion (FUSION), 1–6. https://doi.org/10.23919/fusion65864.2025.11123948

European Parliament. (November, 2024). *Russia's 'shadow fleet': Bringing the threat to light*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI%282024%29766242_EN.pdf

Gullentops, M. (2024, April). *Revised rules on the European Maritime Safety Agency (EMSA)* (EPRS BRI(2023) 751 433). European Parliamentary Research Service.

https://moderndiplomacy.eu/2024/12/23/piracy-as-non-traditional-security-threat-in-indian-ocean-countermeasures-by-pakistan/

https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751433/EPRS_BRI%282023%29751433_EN.pdf

https://www.imo.org/en/mediacentre/pressbriefings/pages/imo-takes-action-on-seafarers-rights-substandard-shipping.aspx

https://www.klgates.com/us-raises-bar-for-sanctions-compliance-in-maritime-energy-and-metals-sectors-05-20-2020

https://www.maritimeinformed.com/insights/open-source-intelligence-maritime-surveillance-safeguarding-co-1752213079-ga.1752213381.html

https://www.ukpandi.com/fileadmin/uploads/ukpandi/Documents/uk-p-i-club/articles/2025/2024-Jan-Dec-IMB-Piracy-and-Armed-Robbery-Report-2.pdf

ICC INTERNATIONAL MARITIME BUREAU. (2025). *ICC- IMB Piracy and Armed Robbery against Ships Report - January - December 2024*.

IMO takes action on seafarers' rights, substandard shipping. (April, 2025). International Maritime Organization (IMO).

International Convention for the Safety of Life at Sea (SOLAS), 1974. (n.d.). https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx

K&L Gates. (n.d.). *U.S. Raises Bar for Sanctions Compliance in Maritime, Energy, and Metals Sectors*.

Larsen, O. H., Ngo, H. Q., & Le-Khac, N. (2023). A quantitative study of the law enforcement in using open source intelligence techniques through undergraduate practical training. Forensic Science International Digital Investigation, 47, 301622. https://doi.org/10.1016/j.fsidi.2023.301622

Meehling, M. (n.d.). *Open source intelligence for maritime surveillance: Safeguarding the global shipping industry*.

Modern Diplomacy. (2024, December 23). *Piracy as non-traditional security threat in Indian Ocean: Counter-measures by Pakistan*.

Office of Foreign Assets Control (2024) | U.S. Department of the Treasury. https://ofac.treasury.gov/

Office of Foreign Assets Control. (2025, April 16). *Sanctions Advisory: Guidance for shipping and maritime stakeholders on detecting and mitigating Iranian oil sanctions evasion*. U.S. Department of the Treasury. https://ofac.treasury.gov/media/934236/download?inline

Pohontu, A., & Ermolai, V. (2024). Artificial Intelligence in Maritime Domain Awareness Applications: Trends and Prospects. In the Intelligent systems reference library (pp. 193–204). https://doi.org/10.1007/978-3-031-63337-9_10

SafeSeANET - EMSA - European Maritime Safety Agency. (n.d.). https://www.emsa.europa.eu/ssn-main.html

Sage, E. C. (2023). Shining a light on AIS Blackouts with maritime OSINT. Frontiers in Computer Science, 5. https://doi.org/10.3389/fcomp.2023.1185760

Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2023). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. Applied Ocean

Research, 142, 103855. https://doi.org/10.1016/j.apor.2023.103855

Turgeon, T. (2024). https://www.darkshipping.com/post/advantages-and-limitations-of-ais

UNCTAD. (October, 2024). *UNCTAD: Review of Maritime Transport 2024 - SAFETY4SEA*. Safety4Sea. https://safety4sea.com/unctad-review-of-maritime-transport-2024/