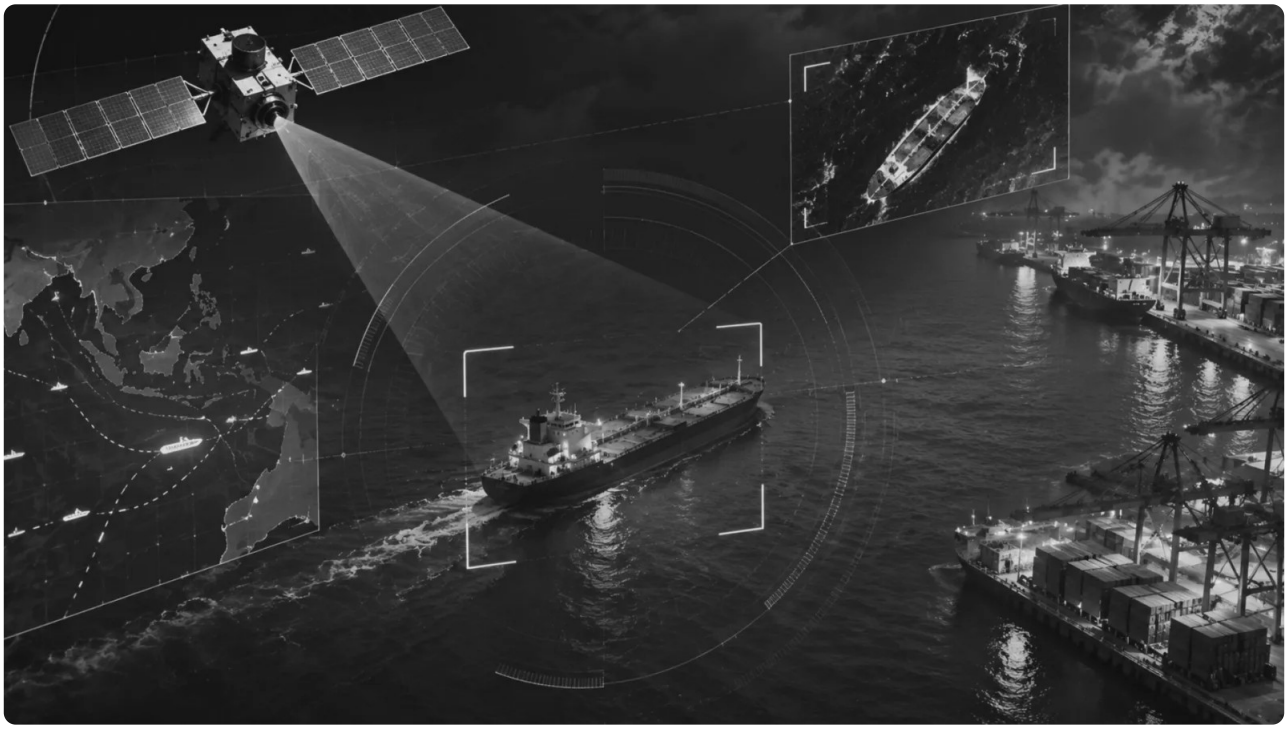
ARTICLES

Maritime OSINT Explained: How AIS, Satellite Imagery and Port Data Help Track Suspicious Shipping

Author: Muskan Mehta • **Published:** November 12, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Maritime Open Source Intelligence (OSINT) is increasingly important in identifying suspicious shipping activity, sanctions evasion, illegal fishing and other illicit maritime operations. This article examines how Automatic Identification System (AIS) data, satellite imagery, port records and commercial information can be integrated to verify vessel identities, movements and activities.It proposes a three-layer verification framework centred on identity, movement and commercial activity, demonstrating how the cross-referencing of these sources can help distinguish routine anomalies from potentially suspicious behaviour. Focusing on India and the wider Indian Ocean Region, the article identifies practical priorities for strengthening maritime domain awareness through institutional coordination, historical vessel records, targeted satellite surveillance, information sharing and specialised analytical capacity.

1. Introduction

A ship can vanish from a tracking screen without vanishing from the ocean. It can change its name, flag or ownership while still sailing familiar routes. It can report a routine commercial voyage while its actual movements tell another story. For maritime authorities the real difficulty is not simply locating vessels. It is determining whether the information about them is reliable.

International shipping moves across spaces that often lie beyond the immediate reach of any single national authority. The same networks that enable trade can also hide illegal fishing, sanctions evasion, unreported transfers and trafficking.[4] Traditional surveillance remains necessary, but it cannot alone confirm the identity, movements and commercial purpose of every vessel. Maritime open source intelligence offers a practical response. It draws on AIS transmissions, satellite imagery, port records, registries and corporate data to construct a fuller picture of activity at sea.

The central argument is straightforward. Maritime OSINT must move beyond tracking positions toward verifying behaviour. AIS shows where a ship claims to be. Satellite imagery can test whether it was physically present. Port and commercial records reveal whether the reported journey aligns with actual activity. The greatest value appears when these sources are compared rather than treated in isolation. For India, and for the Indian Ocean more broadly, the task is to turn scattered maritime information into something more coherent and usable.

2. AIS Remains a Starting Point, Not the Full Picture

The Automatic Identification System was designed for navigational safety. It allows vessels and shore authorities to exchange identity, position, speed, course and status.[1] [2] Over time it has become a primary source for tracking commercial shipping. Analysts can check whether a vessel follows an expected route, how long a voyage takes, whether it makes unexplained stops, and whether its movements match its declared intentions.

Yet AIS records only what a vessel transmits. It does not independently confirm that the information is true.[3] A ship may stop transmitting, commonly described as going dark. It may also send inaccurate positions or manipulate identifying details.[4] Not every interruption is suspicious. Equipment failure, poor reception or operational necessity can explain gaps. The concern arises when an unexplained interruption coincides with other irregularities.

Consider a tanker on an established route whose AIS signal disappears for several hours and then reappears closer to its destination. The gap alone proves nothing. But if satellite imagery places a vessel of similar dimensions near another tanker during that window, and subsequent port records raise questions about cargo or voyage details, the interruption takes on greater weight. The analytical task is not to treat every AIS gap as evidence of wrongdoing. It is to ask what the vessel may have been doing while its reported position was unavailable.

3. Satellite Imagery as an Independent Check

Satellite imagery supplies an independent view of maritime activity, especially useful when AIS is absent or doubted. Optical imagery captures visual detail under clear conditions but is limited by cloud, darkness and atmosphere. Synthetic Aperture Radar works day and night and through cloud, making it particularly valuable in regions where optical coverage is unreliable.[5]

Organisations such as the European Maritime Safety Agency treat AIS, satellite AIS, SAR, optical imagery and port notifications as complementary sources.[6][7] Global Fishing Watch’s work on dark vessels has shown how radar and optical imagery, combined with machine learning, can reveal activity that public tracking systems miss, especially among fishing vessels that do not broadcast AIS.[8] A system that relies solely on AIS will always contain gaps.

Detection, however, is not identification. A radar return indicates presence. Establishing which vessel it is requires comparison with dimensions, location, timing and available tracking records.[7] Satellite imagery functions best as a verification tool rather than a substitute for AIS. Its contribution is to test whether a reported position is consistent with physical presence.

4. Port and Commercial Data Complete the Context

A vessel's story cannot be read from its movements at sea alone. Every commercial voyage is embedded in a network of ports, terminals, companies, cargo interests, insurers and managers. Arrival and departure times, previous calls, inspection records and, where available, cargo declarations help establish whether a journey is commercially plausible.[9] Registration and corporate records add ownership and management context.

A tanker may appear to follow a normal route while its administrative history raises questions. Recent changes in registered owner or management, an inconsistent subsequent port call, or relationships with other vessels can all matter. None of these details by itself proves illicit activity. A route change may be legitimate. Proximity to another ship does not automatically confirm a transfer.[4] Yet the combination of unexplained movements, satellite observations and inconsistent commercial records creates a stronger basis for further examination than any single indicator. Ownership opacity deserves particular attention. Frequent changes of name, flag, owner or manager are not inherently unlawful, but they warrant closer scrutiny when they coincide with other anomalies.[4] Maritime intelligence must follow the vessel beyond its location and into the commercial relationships that make its journey possible.

5. A Three Layer Verification Approach

AIS, satellite imagery and port records are often discussed separately. The practical challenge is connecting them so that inconsistencies become visible and prioritised. One workable frame is a three layer verification model organised around three questions.

- **First**, is the vessel who it claims to be? This identity layer compares name, IMO number, MMSI, flag, dimensions, registered owner and technical manager, with particular attention to historical records. The IMO number is intended to remain constant across a vessel's life and therefore helps link records even when names or flags change.[10] Identity information still requires checking against reliable sources rather than automatic acceptance.

- **Second**, is the vessel where it claims to be? This movement layer compares AIS tracks with satellite detections, reported voyage details and expected speed and route. Unexplained interruptions, physically implausible movements or mismatches between reported position and satellite observation should prompt further review. Timing is essential. A satellite image captures a moment, not continuous movement. Analysts must account for the time of capture, possible vessel speed and data accuracy.

- **Third**, does the commercial activity make sense? This activity layer examines port calls, cargo information where available, terminal visits, inspection histories, ownership changes and relationships with other vessels or companies. An ordinary looking route may look different once port history or commercial links are considered. An unusual call may have a legitimate explanation in context.

The strength of the model lies in the relationships between layers. An AIS interruption is an anomaly. A satellite detection may supply independent evidence of presence. A port record may clarify what happened before or after. Together they can support a more reliable assessment. The model also requires a clear distinction between an unusual event and a confirmed violation. Analysts should be able to identify an anomaly, judge whether multiple indicators justify elevated concern, and decide whether the evidence warrants referral to the appropriate authority. This prevents treating every unusual vessel as a threat.

In practice, a hypothetical oil tanker in the western Indian Ocean might report a voyage toward a commercial port, lose its AIS signal for roughly a day, and then resume transmission as if it had continued on course. Historical records may show recent ownership and management changes. Satellite imagery may place a vessel of comparable size near another tanker during the gap. Subsequent port history may not fully match the original voyage information. None of these facts proves an illegal transfer or sanctions breach. Legitimate explanations may exist. The combination, however, supplies a reason to investigate further: checking registration history, examining the timing and location of the satellite observation, seeking relevant documentation and comparing movements with other records. Maritime OSINT does not replace enforcement agencies. It helps them decide where limited resources should be directed.

6. Relevance for India and the Indian Ocean

The Indian Ocean is central to trade, energy transport and regional connectivity. It also hosts persistent challenges of illegal fishing, trafficking, piracy and other illicit activity.[11] For India the task is not limited to monitoring approaches to its own coastline. It is understanding activity across a wider maritime environment in which ships, cargo and commercial networks cross multiple jurisdictions.

India already possesses important institutional foundations. The Information Fusion Centre Indian Ocean Region facilitates information sharing with regional and international partners.[12][13] The Directorate General of Maritime Administration maintains relevant monitoring and reporting structures.[14] The next step is ensuring that information held by different institutions can be compared and used more effectively. Three priorities stand out. First, stronger historical vessel identity records would allow assessment beyond a ship’s current name or flag. Previous names, ownership changes, management arrangements and registration history provide essential context. Second, satellite based detection should systematically complement conventional tracking, particularly in areas of uneven coverage. Third, maritime intelligence needs closer connection to commercial port activity so that inconsistencies surface earlier rather than through fragmented investigations after the fact.

7. Practical Policy Recommendations

Turning the three layer verification approach into routine practice requires a small number of concrete institutional steps rather than another isolated technology project.

- **First**, establish a common vessel risk assessment framework that all relevant agencies can use. The framework should define how identity inconsistencies, unexplained AIS gaps, satellite detections, unusual port behaviour and ownership changes are scored and combined. A single anomaly should not automatically produce a high risk classification. The purpose is to create a shared language for prioritising cases so that limited investigative capacity is directed where multiple indicators converge.

- **Second**, create and maintain a historical vessel identity record that links present identity to previous names, flags, owners and managers. Each entry should carry its source and date so that outdated or conflicting information can be identified. This record need not be a new public database. It can begin as an internal resource shared among the Navy, Coast Guard, maritime administration and customs, with controlled access for partner agencies through the IFC IOR.

- **Third**, treat satellite imagery as a targeted verification tool rather than continuous blanket coverage. Authorities should prioritise areas and time windows where AIS behaviour, commercial intelligence or partner alerts already suggest elevated risk. SAR imagery is especially useful where cloud or darkness limits optical observation.[5]

Partnerships with research institutions and commercial providers can expand access without requiring every agency to develop full in house satellite capacity.

- **Fourth**, formalise information sharing procedures between the Navy, Coast Guard, Directorate General of Maritime Administration, customs authorities and major port operators. Clear protocols for the exchange of vessel alerts, registration discrepancies and cargo related concerns would reduce the current tendency for each agency to hold pieces of the same puzzle. The IFC IOR is well placed to host a standing mechanism for circulating verified assessments rather than raw data alone.

- **Fifth**, develop structured public private cooperation. Shipping companies, insurers, classification societies and maritime data providers routinely hold commercial and operational information that government agencies may not independently possess.[4] A framework that allows selective sharing of risk indicators while protecting commercially sensitive details would improve the quality of assessments without placing unnecessary burdens on legitimate operators.

- **Sixth**, invest in sustained analyst training. Maritime OSINT requires familiarity with shipping operations, vessel registration practices, satellite interpretation, basic maritime law and regional security dynamics. Technology can surface patterns. Trained analysts are needed to judge which patterns are meaningful and which are artefacts of weather, technical failure or ordinary commercial practice. Universities and policy research institutions can support this capacity through short specialised programmes and secondments.

- **Seventh**, set clear standards for evidence and escalation. An anomalous vessel should not be publicly labelled suspicious or illicit on the basis of incomplete information. Authorities should distinguish between an initial alert, an assessment supported by multiple indicators, and evidence that meets the threshold for formal investigation or enforcement action. This distinction protects legitimate shipping, maintains confidence in information sharing arrangements, and reduces the risk of false attribution.

Taken together, these measures shift maritime OSINT from an activity centred on collecting more data toward a disciplined process of verification and prioritisation. They build on institutions India already has rather than requiring an entirely new architecture.

Looking ahead, artificial intelligence and automated satellite analysis will make monitoring more efficient. Machine learning can help identify unusual movements, compare detections with AIS and surface connections between ships, companies and ports. The same advances may also encourage more sophisticated manipulation, not only concealing location but constructing digital histories that appear consistent across records. What can be described as a synthetic maritime identity remains a forward looking risk rather than a widespread present reality, yet existing concerns about AIS manipulation, fraudulent registration and opaque ownership structures indicate why preparation is warranted.[4] The response should not be total reliance on automated systems. Algorithms generate false alerts as readily as genuine ones. Weather, technical failures, legitimate ship to ship operations and commercial schedule changes all produce unusual data patterns. Human assessment and independent verification will continue to matter.

The oceans cannot be monitored effectively through any single tracking system. AIS supplies a record of reported movements, satellite imagery reveals physical activity that may otherwise remain invisible, and port data supplies commercial context. The real value emerges when these sources are brought together. The three layer verification approach outlined here offers one way to connect identity, movement and commercial activity so that inconsistencies

can be identified early, assessed carefully and referred when warranted. For India this is an opportunity to strengthen maritime domain awareness in the Indian Ocean without treating technology as a substitute for institutional coordination. Better records, targeted satellite use, shared information and trained analysts can make existing surveillance more effective.

Ultimately, maritime OSINT should not be measured by how many vessels appear on a screen. Its value lies in whether authorities can establish which vessels are operating, whether their reported movements are credible, and whether their activities warrant further attention. The next challenge in maritime security is not simply to see more ships. It is to recognise when the information surrounding a ship does not add up.

References:

[1] International Maritime Organization (IMO), “AIS transponders.”

https://www.imo.org/en/ourwork/safety/pages/ais.aspx

[2] IMO Assembly Resolution A.917(22), *Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)*, 2001. https://law.resource.org/pub/us/cfr/ibr/inc/imo/imo.a.0917.2001.pdf

[3] National Academies Press, chapter on AIS limitations (static data is manually enteredand its integrity is not assured). https://www.nationalacademies.org/read/10708/chapter/3

[4] U.S. Department of State, U.S. Department of the Treasury (OFAC) and U.S. CoastGuard, *Global Maritime Advisory: Guidance to Address Illicit Shipping and Sanctions Evasion Practices*, 14 May 2020. https://ofac.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf

[5] European Maritime Safety Agency (EMSA), *CleanSeaNet: Maritime surveillance service for pollution prevention*. https://emsa.europa.eu/tags/download/6453/4322/23.html

[6] EMSA, “Data sources” (combined maritime data). https://www.emsa.europa.eu/combined-maritime-data-menu/data-sources.html

[7] EU Coast Guard Functions, “Copernicus Maritime Surveillance Service products”

(vessel detections correlated with AIS). https://archive.coastguard.europa.eu/node/757

[8] F. S. Paolo et al., “Satellite mapping reveals extensive industrial activity at sea,” *Nature* 625 (4 January 2024): 85–. https://doi.org/10.1038/s41586-023-06825-8

[9] “Keeping European Shipping on the Straight & Narrow,” MarineLink, 11 March 2013 (summarising an EMSA brochure on SafeSeaNet port arrival and departure data). https://www.marinelink.com/amp/news/european-shipping352365

[10] IMO, “IMO Identification Number Schemes.”https://www.imo.org/en/OurWork/IIIS/Pages/IMO-Identification-Number-Schemes.aspx

[11] V. Adm. Pradeep Chauhan (Retd), presentation on maritime domain awareness,National Maritime Foundation, 15 September 2021. https://globalnetplatform.org/system/files/session_04_pres_by_vadm_p_chauhan_mda_more_than_a_buzzword_15_sep_21.pdf

[12] Gayathri Iyer, “Sense for sensibility: Maritime domain awareness through theInformation Fusion Centre – Indian Ocean Region,” Observer Research Foundation. https://www.orfonline.org/expert-speak/sense-for-sensibility-maritime-domainawareness-through-the-information-fusion-centre-indian-ocean-region-ifc-ior-60811

[13] “Indian Navy launches Information Fusion Centre to boost maritime security,” *The Week*, 22 December 2018. https://www.theweek.in/news/india/2018/12/22/Indian-Navylaunches-Information-Fusion-Centre-to-boost-maritime-security.html

Directorate General of Shipping / Directorate General of Maritime Administration(transition under the Merchant Shipping Act, 2025), Government

The views expressed are those of the authors and do not represent the views of CNAWS.

?ImageSource: ChatGPT