Volume XXIX 2026
MBNA Publishing House Constanta 2026



Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

An OpenLayers-Based Web GIS Platform for Spatial Security Management of Critical Maritime Infrastructure

To cite this article: Mihailescu Marius Iulian, Marascu Valentina, Nita Stefania Loredana, Asalomia Laurentiu Bogdan, Gheorghe Samoilescu, Scientific Bulletin of Naval Academy, Vol. XXIX 2026, pg. 309-329.

Submitted: 26.04.2026
Revised: 25.10.2026
Accepted: 03.11.2026

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-26-I1-029
SBNA© 2026. This work is licensed under the CC BY-NC-SA 4.0 License

An OpenLayers-Based Web GIS Platform for Spatial Security Management of Critical Maritime Infrastructure

Mihailescu Marius Iulian[1], Marascu Valentina[1,2,*], Nita Stefania Loredana[3], Asalomia Laurentiu Bogdan[4], Gheorghe Samoilescu[5]
[1]SPIRU HARET University, Engineering and Computer Science Faculty, Romania, email: m.mihailescu.mi@spiruharet.ro
[2]National Institute for Laser, Plasma and Radiation Physics, Low Temperature Plasma Department, Romania, valentina.marascu@gmail.com
[3],,Ferdinand I" Military Technical Academy, Faculty of Information Systems and Cybersecurity, Romania, stefania.nita@mta.ro
[4]Northern Marine Management Limited, Scotland, asalomiabogdan@yahoo.com
[5]"Mircea cel Batran" Naval Academy, Romania, samoilescugheorghe@yahoo.com
*** valentina.marascu@gmail.com**

Abstract. Recent attacks have highlighted the need for real-time security monitoring of ocean infrastructure, from underwater internet cables and offshore energy installations, to LNG terminals and cargo ports. Look at the Nord Stream pipeline attack or those cable cuts in the Baltic Sea. Recent attacks have highlighted the need for real-time security monitoring of ocean infrastructure, underwater internet cables, offshore energy installations and LNG terminals, and cargo ports. Think of the attack on the Nord Stream pipeline or the severing of cables in the Baltic Sea. The four main elements of the system are: detection of AIS data anomalies, the real-time tracking of ships, determination of "ghost ships" (by cross-referencing AIS and satellite radar data), anomaly events identification, cyber threat statistics that track GPS jamming attempts, SCADA systems hacks, false AIS signals as well as undersea cable hacking attacks (the system also uses NATO standard sea security zones that issue STANAG 5516 alerts with a specific threat level). When we tested the platform with five simulated attack scenarios, it detected an oncoming threat in under 12 seconds, never missed a single alert when ships traversed too close to infrastructure, and successfully associated suspicious boat movements with cable signal disturbances. These results highlight the ability of the platform to identify complex, cross-domain maritime security threats.

Keywords: WebGIS; OpenLayers; AIS; SCADA; Maritime Security; Cybersecurity; Dark Vessel.

1. Introduction

The maritime domain is one such sector in which substantial changes have taken place over the past few years, as it has developed into a deeply-integrated cyber-physical environment with digital technologies and geospatial intelligence converging onto critical infrastructure. Operational control, surveillance and navigational functions of modern ports are largely undertaken using networked systems. Also, as well is more generally in offshore energy facilities, submerged communication cables both in one off projects such as those evaluating supply chains to ocean going vessels. This type of digital integration serves, in

many respects, exceedingly well in terms of operations performance and worldwide connectivity. Also, is left open another realm of vulnerability which lays maritime facilities at the mercy of a new tier technopreneurial organized cyber-physical attacks. Recent attacks targeting critical maritime infrastructure (CMIS), including those attributed to nation-state actors and hybrid threat groups in the wake of recent events, highlight vulnerabilities. The assets are both physically exposed and reveal weaknesses in existing monitoring and response systems, as evidenced by the sabotage of underwater pipelines and the attacks on subsea communication cables. Existing maritime surveillance frameworks are largely AIS dependent and separable intelligence sources, fragmentary systems not well positioned to identify complex domain-spanning threat phenomena like cyberattacks, electronic warfare and active physical disruption.

The lack of an integrated geographic platform that combines different data sources to offer a single view of operational performance is the most serious challenge. By integrating cyber threat indicators, proximity to infrastructure and vessel behaviour, tools are required that can connect the three in real-time, so maritime security organisations including naval forces, port authorities and infrastructure operators can react immediately. Without these capabilities, the ability to identify low-signature anomalies in the form of AIS manipulation, GPS spoofing or coordinated operations between black vessels operating near key assets is elusive; leading to delayed reactions and higher risk exposure. The study addresses this gap and presents the MARITIME SENTINEL, the prototype Web GIS platform developed to aid spatial security governance in the maritime environment. It uses open-source technologies to provide a real-time framework for visualising threats on a geographic basis. Its built on OpenLayers v8 and a Python Flask backend it combines multiple data layers like real-time AIS feeds, satellite-based vessel identification, cyber threat intelligence and military operational areas into a single maritime cybersecurity application. It illustrates the potential for modern web-centric geospatial technologies to support cross-domain threat detection via a spatial risk framework that combines concepts of cyber situational awareness with traditional maritime surveillance. Second, it demonstrates with attack scenario simulations that this type of integrated log processing might reduce discovery. Also, it improves comprehension on the relationship between real world events, other physical world events and cyber event correlation. This research further presents a paradigm shift on moving beyond isolated monitoring systems, that only provide alerts towards smart-based, integrated infrastructures that seeks to integrate ambient performance measures, with spatial visualisation in the environmental context of maritime cyber security. Also, it permits appropriate response mechanisms tailored to applicable dynamic risk circumstances specific for the maritime cyber-physical domain.

2. Background and related work

The maritime domain is defined as a cyber-physical environment, where an integrated ecosystem of physical assets and infrastructure. Together, they create a wider attack surface and more serious operational and security implications from breaches. Broadly speaking, there is a uniform agreement today that maritime cybersecurity has taken on unprecedented significance from. not just defending the IT systems onboard the vessels. but to extending towards ports and offshore installations, subsea communication cablestowards autonomous ships as well the entire logistics chain (Dimakopoulou & Rantos 2024;Progoulakis et al. 2024; Clavijo Mesa et al. 2024;Son & Huh 2025). In parallel, new studies have shown an increased focus on monitoring and detection capabilities rather than risk assessments driven just by compliance. This indicates a transformation into real-time operational resilience into the maritime environments (Dimakopoulou & Rantos, 2024; Clavijo Mesa et al., 2024; Liu & Amri, 2025; Vaarandi et al., 2025).

2.1. Maritime cyber-physical threat landscape

An extensive volume of recent research produces approximations, suggesting that maritime positioning, monitoring and control systems are highly vulnerable to hostile interference. While AIS is still an important basis for understanding maritime activities, vessel traffic coordination and safe navigation it is well known among experts to be vulnerable to many forms of attacks such as intentional signal denial,

message replay attacks, and information manipulation (identity re-assertion/falsifying identity, fake message injection). Studies with publication dates from 2024 onward are focused on advanced techniques to detect anomalies and identify deception attempts. Such methods may include machine learning to study the behaviour of vessels and detect deviations from expected radio frequency signal patterns or vessel activities (Agrebi et al, 2025; Maganaris et al, 2024). Despite the operational implications of this study, it essentially acts as a cautionary tale with respect to AIS-based monitors not being viewed as veritable sources of truth in combative areas. At the same time, the continuous threat of jamming and spoofing GPS and other satellite navigation systems are causing a headache for sea-going operations as vessels depend on these signals for navigation, timing and route programming. Threats on operational activities from navigation signal deception are routinely considered one of the most serious by present day security risk assessments for both conventionally crewed and autonomous maritime vessels, especially when automated system control layers or fully autonomously controlled bouys are under operation (Son & Huh, 2025; Agrebi et al., 2025). For integrated cyber-physical systems, this threat is aggravated by incompatible navigation information, leading to potential false alarms on coastal monitoring centres, unsupported boundary violations or potentially dangerous vessel manoeuvres (Progoulakis et al., 2024; Son & Huh, 2025; Agrebi et al., 2025).

Additionally, MITRE is working in the area of assessing vulnerabilities associated with maritime operational technology environments, which encompasses SCADA systems, dynamic positioning equipment, apparatus controls and port industrial infrastructure. Since 2024, research has emphasized the need for maritime cybersecurity assessments that assess both information technology and operational technology elements. This is because breaches of operational technology can result in an actual propulsion failure, positioning it with a critical error (Dimakopoulou & Rantos 2024; Progoulakis et al., 2015) cargo handling failures or damage to offshore production facilities itself (Clavijo Mesa et al., 2019). An integrated perspective of cyber-physical risk analysis such as the aforementioned for dynamic positioning systems of drillships (Progoulakis et al., 2024) necessitates that we move beyond understanding maritime security incidents simply as information integrity breaches and distant malfunctions at the level of a sensor, control system or physical operation..

2.2. Existing maritime surveillance systems

Traditional systems of maritime surveillance still rely heavily on AIS data streams, radar technology, Vessel Traffic Services (VTS), and regionally focused monitoring networks. These technologies are particularly useful for vessel traffic management and navigation support (particularly in coastal areas, key waterways and ports), with a concomitant effect of retaining some level of awareness about ship movements. However, they have inherent limitations. Recent studies reveal that the initial invention of AIS technology was geared towards enhancing radar systems, preventing (de)collision at sea and ensuring support to VTS functions. Moreover, most of existing surveillance systems still conduct within the context of this cooperative tracking method (Liu & Amri, 2025; Maganaris et al., 2024; Xie et al., 2025). This means that while these systems are great at providing ships with accurate, continuous streams of data; but they break down completely when faced with the introduction of intentional misinformation, stealth operations or cross-domain interference.

From 2024 onwards, research efforts have advanced in the practical use of data-driven surveillance strategies on AIS information streams. On the basis of recurrent neural networks, transformer architectures and semi-supervised anomaly detection systems deep-learning models have been developed which are more efficient for identifying operational anomalies, irregular movement behaviours and unusual paths (Maganaris et al., 2024; Xie et al., 2025) Nevertheless, most current approaches are centered on improving detection from a single data source (usually AIS tracking data) without amalgamation of information from infrastructure monitoring systems, satellite intelligence, and cyber-security to generate more contextual awareness. While this specialisation has improved pattern recognition, it lacks the breadth of situational awareness necessary to protect critical maritime infrastructure effectively.

2.3. Geospatial intelligence in maritime security

In the spatial context you are likely to know how important is a vessel event based on port proximity, offshore platforms, subsea cables, military zones and logistics corridors. Thus, geospatial intelligence has been very important with respect to maritime security. Advanced GIS studies nowadays have found that geospatial platforms are used in the maritime-port sector for navigation support, infrastructure management, logistics optimisation and spatial planning. However, they are used less commonly as integrated cyber-physical threat intelligence systems (Isbaex et al., 2025). Of note, remote-sensing research shows the benefits of using satellite observation in combination with cooperative vessel reporting to accurately identify mis-reporters, non-reporting vessels and possibly suspicious activity near sensitive areas (Xie et al., 2025; Li et al., 2025).

For our relevance check, we could take the recently published transition to AIS-plus-imagery fusion used for dark-vessel detection as an example. The integration of AIS with detects from optical or SAR is shown to significantly improve vessel association and identify time periods where ships are missing from cooperative reporting channels (Li et al., 2025). This is especially important for maritime security applications, since dark behaviour rarely matters on its own. The threat-context significance sheds light on the potential danger when geospatial correlations are drawn to strategic infrastructure, signal degradation activities, no-go zones, or suspicious patterns of loitering. Indeed, the remaining literature in the fusion phase of health system development continues to be underdeveloped.

2.4. Limitations of current solutions

Progress has been substantial, but current research still exhibits four persistent limitations. However, the research of maritime cyber security starts from using descriptive patterns for threats and focusing on policy studies and high-level surveys of the industry instead of functional geospatial systems (Dimakopoulou & Rantos 2024; Clavijo Mesa et al., 2024; Son & Huh, 2025; Liu & Amri, 2025). Second, surveillance studies often focus on the assessment of vessel movements from AIS data excluding cyber threat signatures like spoofing attacks (Karimi & Lamas, 2022), unauthorised access attempts (Llevo et al., 2021) or communication irregularities where no AIS signals are sent (Vaarandi et al., 2025; Maganaris et al., 2024; Xie et al, 2025). Third, satellite-based techniques for detection of hidden vessels usually end with identification and do not connect the results with warning/cyber-physical infrastructure alerts or defence operational data (Xie et al., 2025; Li et al., 2025) Fourth, maritime and port geographic information system studies prioritiz planning and administration applications ahead of live threat presents and response practices (Isbaex et al., 2025).

Response time is another major challenge. According to the 2025 maritime cybersecurity monitoring analysis, automated monitoring research is still developing, with disaggregated system designs, computational methods, and implementation strategies across diverse information technology, operational technology, vessel, and port contexts (Vaarandi et al., 2025). This has led to modern methods that can detect without necessarily having operational knowledge or comprehension, but not quickly enough! Breaching such parlance unveils an important operational hiatus, in relation to for example, maritime sites from under-sea cables through LNG installations right down to offshore facilities and defence exclusion zones.

2.5. The position of the current work

The underlying research is positioned at the confluence of maritime cybersecurity, maritime monitoring and web based geospatial intelligence. MARTIME SENTINEL platform The proposed MARITIME SENTINEL platform is meant to provide an integrated operational layer for the surveillance of critical maritime infrastructure, in contrast to earlier work on AIS anomaly detection (Maganaris et al., 2024), spoofing-specific defense (Agrebi et al., 2025), cyber-risk assessment for vessels (Progoulakis et al., 2024) or high-level maritime cyber-security surveys (Dimakopoulou & Rantos, 2024; Clavijo Mesa et al.). The innovation is not in the introduction of a stand-alone detection algorithm, but in fusing multiple streams of evidence (real-time AIS, SAR-assisted dark-vessel signals, cyber-physical threat intelligence and NATO aligned-alert zoning) into one synchronized geospatial interface.

Hence, the current study expands on earlier literature in three unique ways. First we extend from monolithic maritime analytics to multi-domain fusion, specifically integration of cyber event data, non-cooperative and cooperative vessel reporting. Secondly, it spatially contextualises maritime threat detection based upon anomalies that is localised to the specific vessel level as opposed to simply abstract events, prioritising proximity relative to infrastructure. Third, it implements these capabilities in an open-source Web GIS architecture built with OpenLayers and Flask that closes the gap between academic detection research and ready-to-use maritime cyber situational-awareness platforms. In that sense, MARITIME SENTINEL is a systems-integration contribution to maritime cyber physical defence based on but separate from the recently surveyed bodies of work.

3. High-level architecture overview

MARITIME SENTINEL is a browser-based and modular geospatial intelligence tool that integrates maritime, cyber, and infrastructure datasets to present a holistic operational view in near real-time. It is based on a distributed client-server model consisting of scalable backend infrastructure for handling data gathering, computing and malicious analysis of threats coupled with a lightweight and fast client-side UI. The platform enables faster detection of threats and easy onboarding of new data sources and analytical tools.

The overall architecture consists of three components (Figure 1). Which we can see a presentation layer with OpenLayers v8 to perform Web GIS user interface, an application layer with Python Flask server that hosts RESTful APIs and the data integration layer collecting normalizing and adding value over heterogeneous streams of maritime and cyber threat information.

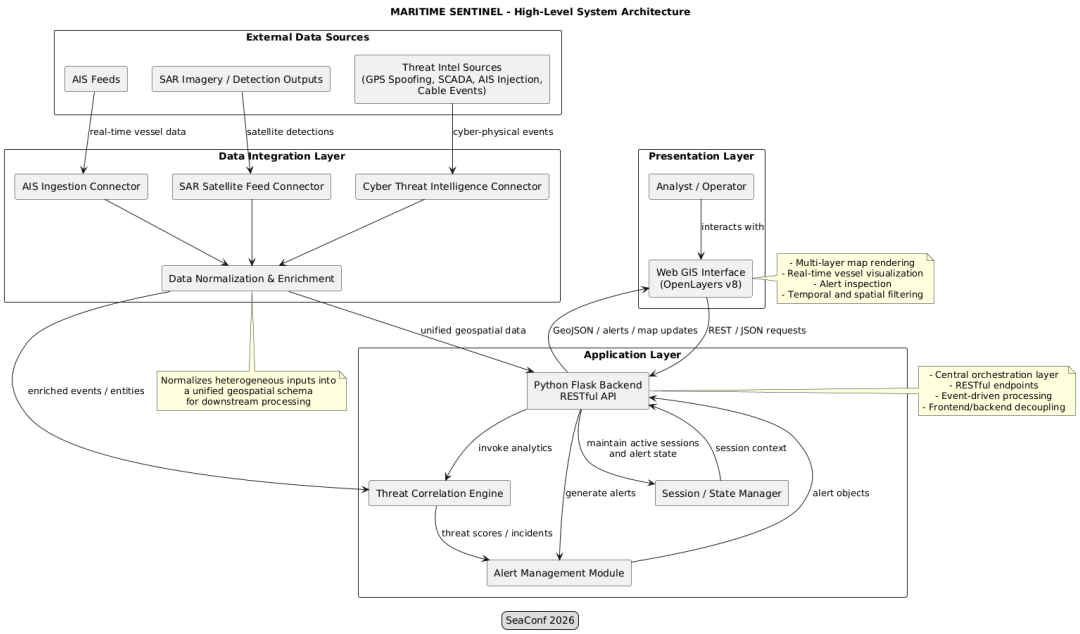


Figure 1. MARITIME SENTINEL – High-Level System Architecture

3.1. High-level architecture overview

The frontend uses OpenLayers v8 to produce an interactive geospatial visualisation system that works on the web browser. It can handle different layers on the map, and deal with vector / raster data, as well as update maps in real time via async calls to an embedded API. The system handles continuous data updates while providing near real-time visualisation of ship movements, alert conditions and spatial relationships. Users can interact with the map by performing geographic searches, turning layers on and off, filtering data by time frames, and drilling down to alerts. Which allows analyst to analyse detailed security scenarios on the map, directly. Flask was used as backend framework, due to its lightweight

nature and flexibility, it is most suitable for prototype developing of distributed systems. Flask serves as the main control node, providing the RESTful endpoints for incoming data and reports, some internal processing on that data, and provision of information to the front end. The backend works by using bots to digest different events consuming data from external sources and running algorithms to detect abnormalities and correlations. It write the last alert state with user session, and allows some background processing to be able to write alerts in disk but still immediately answer on mid data loads. The frontend and backend communicate over JSON-based APIs, but sometimes low latence is a requirement and the API supports optional WebSocket connections for real-time updates. This separation of visualisation and processing allows us to keep the architecture simple, scale each component independently, and (if necessary) shift towards microservices in the future.

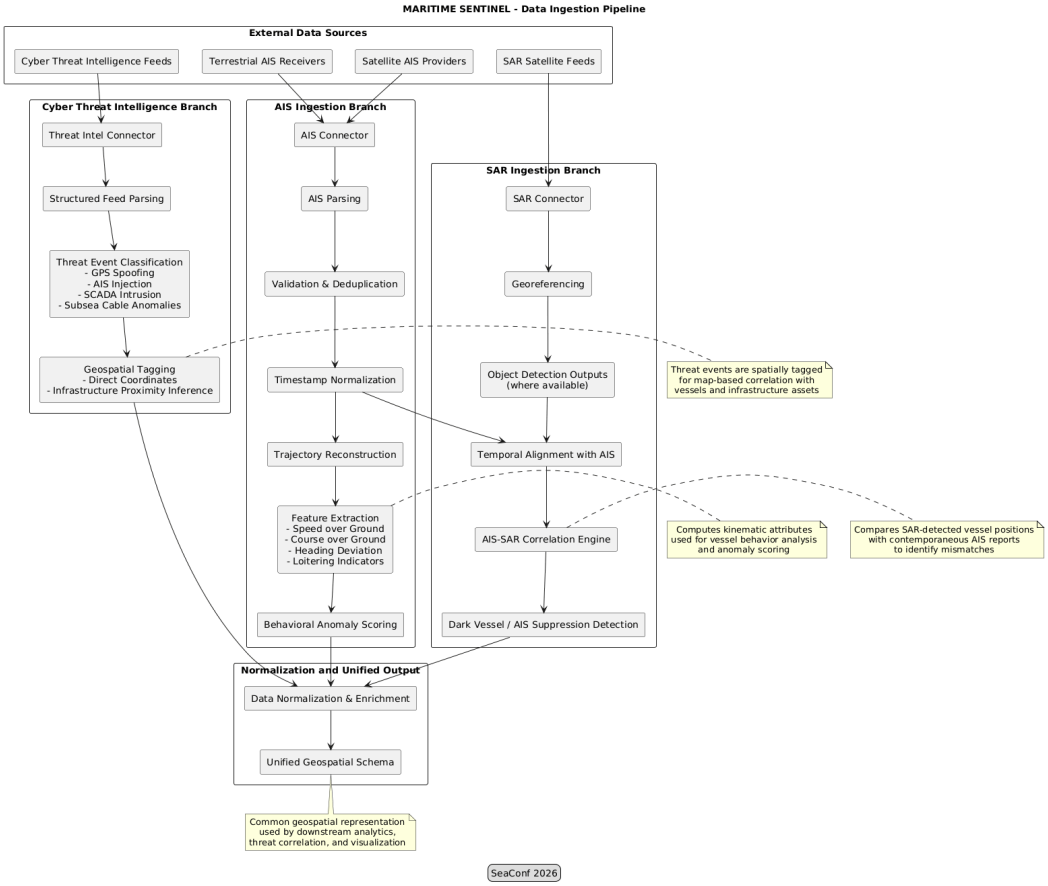


Figure 2. MARITIME SENTINEL – Data Ingestion Pipeline

3.2. Data ingestion pipeline

A native processing structure of the general information sources at different reliability, so structured, and time as it can be seen in Figure 2 is processed by the systems data processing infrastructure. It serves as a common connector, to make all of the incoming data available in a single geographic format, within the framework. An example of direct output from AIS data feeds, is vessel monitoring. These inputs from land based receivers, or satellite AIS services, are analysed by the system without fail. Initially, you execute various simple processing steps, that consist of correct verifications of the data, eliminating duplicated reports, reconstructing timestamps and normalizing ship trajectories. Analysis modules calculate movement features like ground speed, course direction, heading changes and stationary activity measures. These calculations allow for algorithms to analyze rogue behaviour of vessels.

Another monitoring technique that does not rely on vessel collusion is synthetic aperture radar (SAR) satellite intelligence. Satellite data is interpreted without needing the ships to broadcast anything over AIS, creating a uniform snapshot of where vessels are located regardless of AIS transmissions.

Processing of these images involves the assignment of geographical coordinates, identification of detected objects whenever detection results are available and timing synchronisation with AIS information. A matching system compares vessel positions identified in SAR images with simultaneous AIS broadcasts to identify mismatches that may indicate hidden vessels or inactive onboard AIS equipment.

3.3. Multi-layer geospatial model

A high-level layered geospatial structure (see Figure 3) organizes all collected and processed data allowing the users to view and integrate information across multiple operational areas at once. Real-time tracking of ships is produced from AIS data, improved with the help of behavioural analysis the vessel layer. The updated vessel information is collected continuously and an anomaly score is calculated if the movement pattern of a vessel differs from what was expected. Visual indicators such as icon updates and color changes make it easy to spot potentially suspicious activity at a glance, displaying risk levels categorically.

Infrastructure Layer. Geospatial data for critical maritime assets, including LNG terminals, offshore platforms, undersea cables and port facilities. This system associates these assets with protectable zones that can be adjusted and used to measure proximity threats and shows them as point, line or polygons for physical purposes.

It collates cyber-physical events and those are highlighted on the geospatial map using the threat intelligence layer. It collects these incidents and arranges them in a typed time line to help with timeline assessments and groups the types of incidents on how they have been classified (eg. Spoofing, intrusion or signal degradation) and severity level. This layer enables the data link between cyber events to physical infrastructure weaknesses and also transiting physical vessels.

The military and NATO operational layer consists of pre-determined spaces: the no-fly zones, exclusion zones and areas of operational importance. STANAG 5516 specifies that the zones appear as direct-readable NATO symbols on a common map and within alert escalation processes. This ensures that military operational requirements are appropriately considered, where relevant, when threats are assessed.

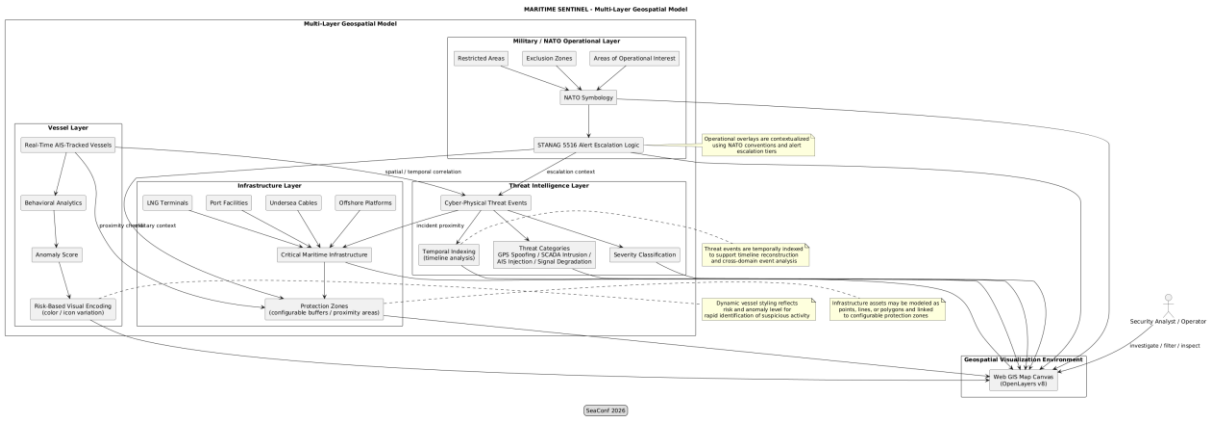


Figure 3. MARITIME SENTINEL – Multi-layer geospatial model

3.4. System Design Principles

Architecture of MARITIME SENTINEL is built on 3 core design principles: interoperability, scalability and modularity. In the modular approach, different components take care of for data ingestion, processing and visualisation. Each functional module including AIS processing, SAR correlation, threat intelligence integration and others operates independently through clearly defined interfaces. The architecture encourages quick addition of further data sources or components of analytics to the system without making fundamental adjustments into its core design.

Asynchronous processing strategies and a completely stateless API architecture solves the scalability issue. This flexibility also translates to horizontal extension of the backend infrastructure to deal with rising data loads, essentially in high-density marine areas or across extended surveillance operations. Even with more tracked entities and data layers, frontend remains efficient because the lightweight web technologies are employed as the required stack.

By using standards both in the geospatial and defence sectors, interoperability is assured. Although spatial data exchange is based on several well-known formats, the alerting procedures and operational protocols comply with NATO standards (i.e., STANAG 5516 for message format and escalation protocols). Such design choices allow smooth integration of thirdparty command-and-control systems, maritime security platforms, both unclassified and allied info-sharing networks.

The holistic system architecture (as shown in figure 4) augments MARITIME SENTINEL from a visualisation tool into a geospatial intelligence platform with the capability of real-time detection of maritime cyber-physical threats and situational awareness capabilities anywhere across civilian and defence applications..

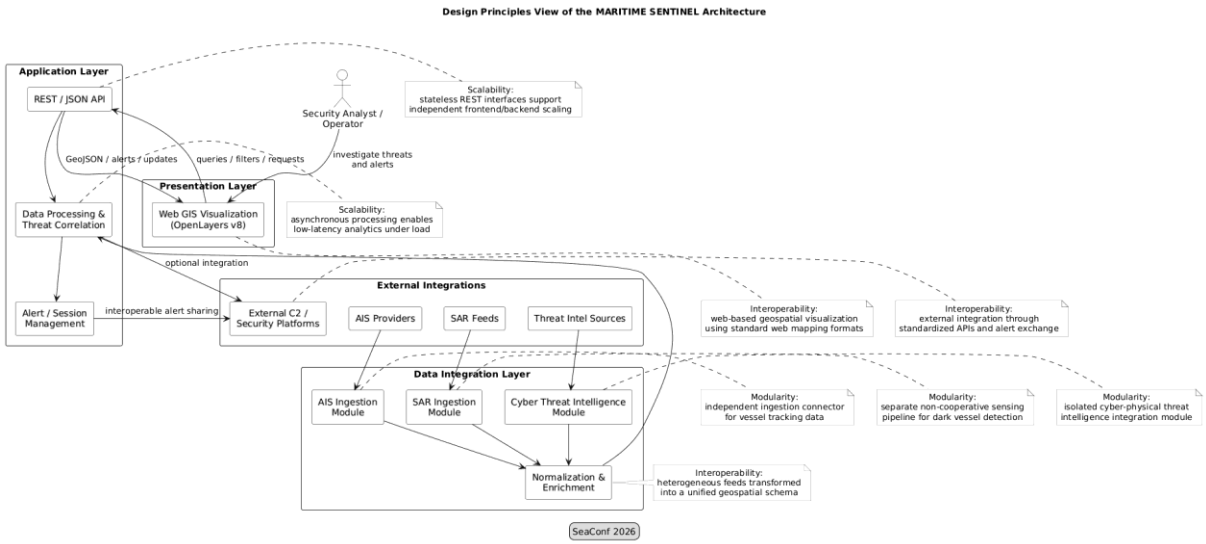


Figure 4. Design principles view of the MARITIME SENTINEL architecture

4. Core functional modules

MARITIME SENTINEL is operationally built on four connected functional modules that convert a range of marine and cyber data streams to actionable geospatial intelligence. The system's designers created these modules to address key detection and analysis challenges affecting threats to critical maritime infrastructure. The challenges refer to the recognition of abnormal vessel signatures, the identification and warning of non-compliant or concealed maritime operations, the integration of cyber and corporeal threat indicators, as well as the consolidation of alert escalation procedures in defense-oriented functions. The modules act like a connected pipeline, not independent analytic tools. Thus, this modelling pipeline draws findings at one level to support or contrast observations at the other.

4.1. Real-Time AIS tracking and behavioral anomaly detection

The primary module leverages Automatic Identification System (AIS) data streams to monitor active vessels. While AIS provides the most easily and pragmatic maritime position information, its capability to be used for security purposes goes beyond just receiving the signals from looming vessels. The system also needs to analyze movement patterns in the right context. As a result, MARITIME SENTINEL handles AIS data that goes further than the fundamental observations of ships only. Following this, each new AIS transmission is fed into an automated behavioural analysis system that recreates ship tracks and calculates time-series movement metrics relevant to security. This method is effective, especially

close to important infrastructure where the system will pick up features that suggest illegal or abnormal marine actions. Ground speed, abrupt heading adjustments, duration stays or loops and accelerations: these parameters. The enforcement of ships that go too slow in restricted waters or decide to accelerate suddenly and other abnormal speed changes are enforced.

Such behaviours could be indicative of reconnaissance, or halted movements and positioning of forces. Course Change metrics then detect routing anomalies (Course Changes) based on methods that look for changes in directions (frequently directed) or identify circular movement directly, such as sequences of extra turns near LNG terminals or offshore structures and undersea cables. How the system distinguishes regular passage from unusually long stay in (e.g. upper and bottom part of Figure 5).

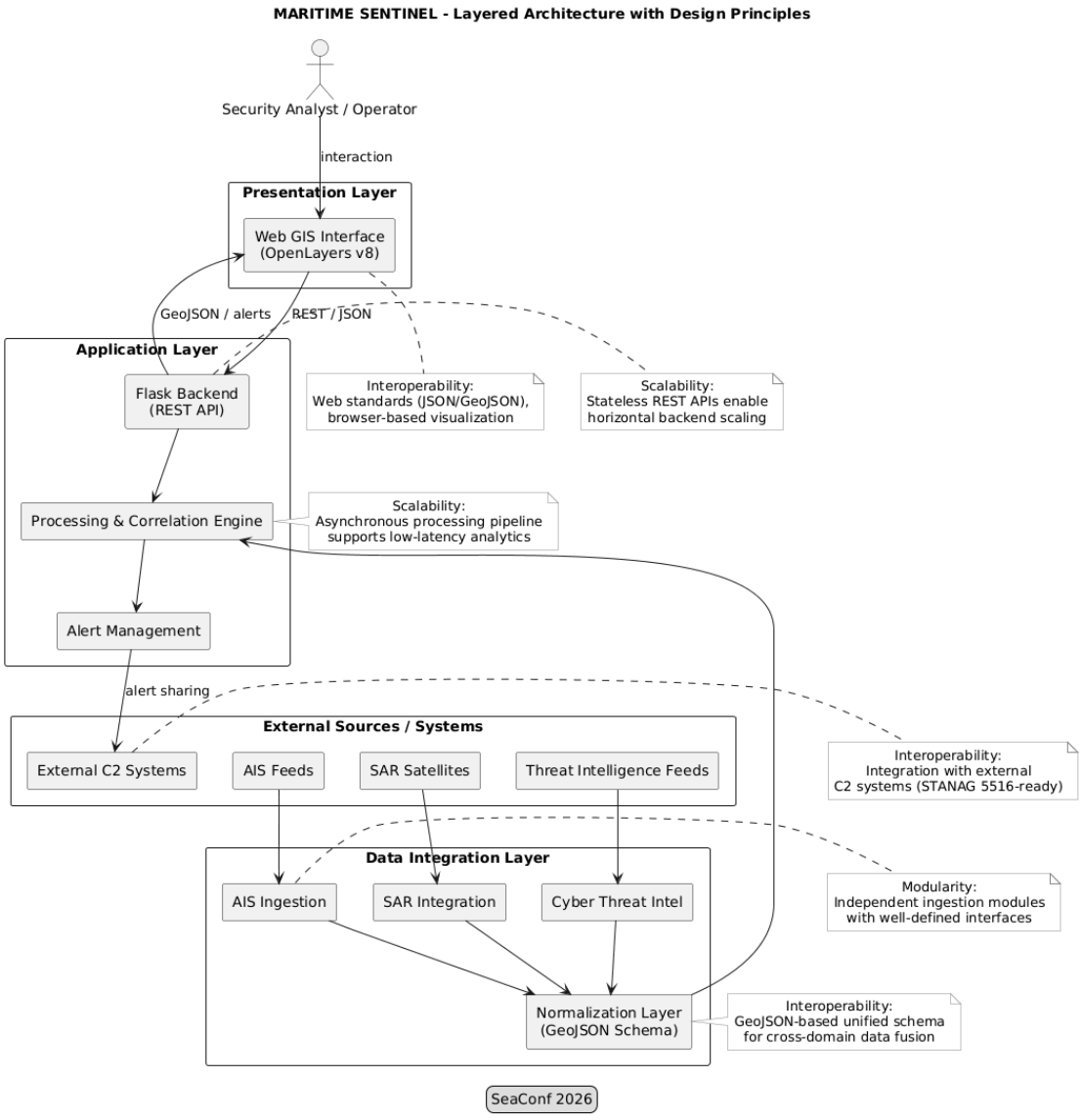


Figure 5. MARITIME SENTINEL - Layered architecture with design principles

The system applies a weighted behaviour anomaly evaluation to reduce false alerts and also prevent the over-reaction of normal shipping activity. Current risk score after assessing the strength of features and time spent travelling in behaviours, how close or far from critical maritime infrastructure the vessel travels in relation a set of situational variables (eg zone restrictions / threat conditions). The scoring methodology we use here is based on rule-based logic which enables an operational understanding and

transparency (in contrast to more complex classification methods). Pointing a degree out on open waters hardly matters; a cable protection area high in direction changes rates, and slow circling, receives an anomaly score boost. This score, which is being derived in real time from incoming AIS data, is then translated into visual risk levels on the mapping interface. Instinctive operator drill allows eyes to go past the vessels themselves, and hone in on ships whose movement patters raise their ghosts, being monitored, intercepted, hiding or positioning for an accident.

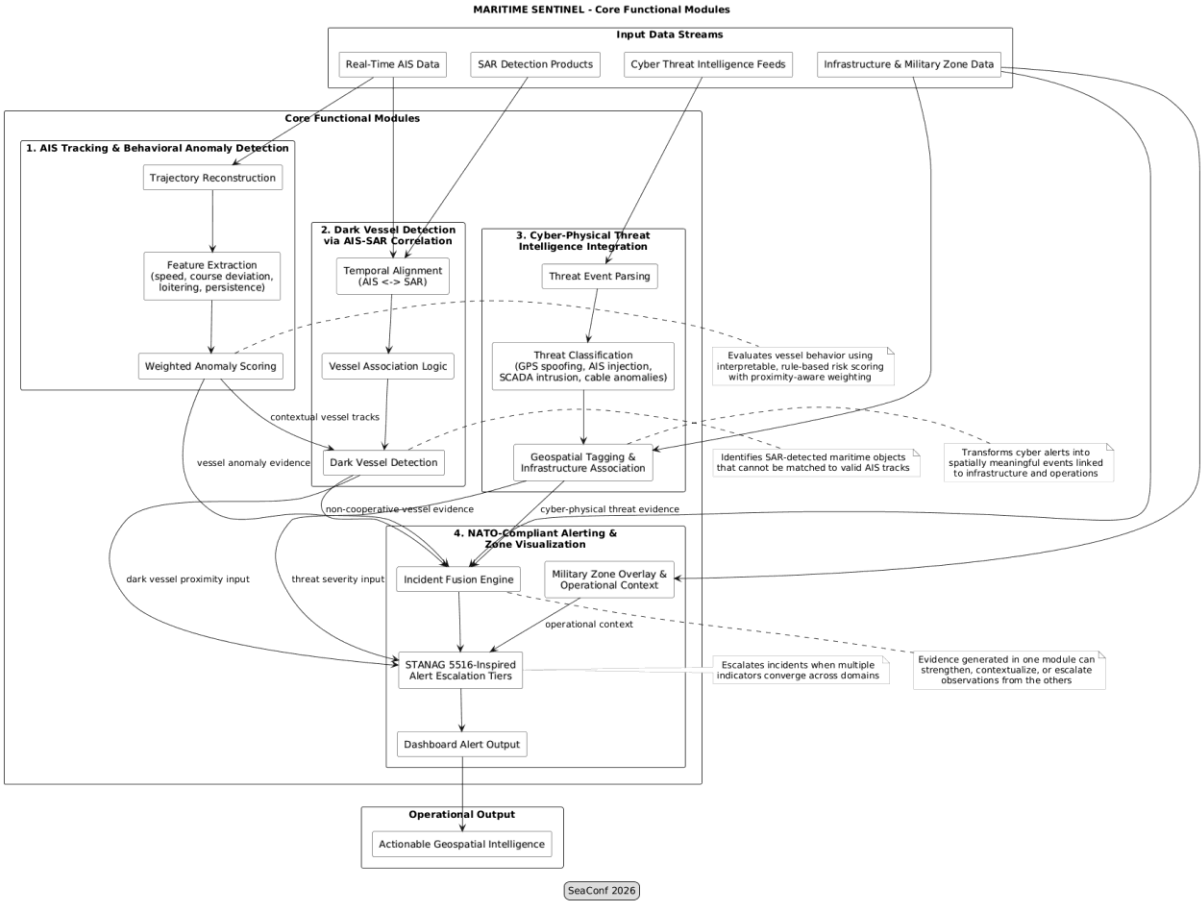


Figure 6. MARITIME SENTINEL – Core functional modules

4.2. Dark Vessel Detection via AIS–SAR Correlation

AIS-based tracking provides near-real-time situational awareness, but inherent limitations were clearly demonstrated when ships turned off AIS or operated outside each collaborative monitoring system, so they stopped transmitting in order to evade detection. MARITIME SENTINEL plugs this gap by correlating dark vessels detected with synthetic aperture radar (SAR) satellite images only to a secondary module of MARITIME SENTINEL via automatic identification system (AIS) data.This module (Figure 6) not only identifies where AIS is absent but also gives us physical geographic evidence that non-cooperative vessels are operating in areas potentially of operational interest.

SAR is a perfect sensor for ocean monitoring since it can penetrate weather noise and carry out in the absence of illumination conditions. The SAR data is processed by the platform using georeferenced detection products which are used to locate vessel-like objects where each product records its coordinates. These detections are associated with AIS data snapshots that are recorded over a user-defined time window. In this way, one generates a dataset that allows you to directly compare the corresponding positions of vessels with the water surface through remote sensing observations.

Mismatch-detection algorithms within the system then determine if any of those objects tracked from SAR videos correspond with a ship that transmitted an AIS message at similar time and place. The matching depends on distance thresholds, the alignment of headings when possible (e.g. an association with a valid AIS trace cannot be made, and in that case the algorithm says this SAR target may have been as result of a dark vessel incident. If the unmatched target has been sighted near critical infrastructure, in an exclusion zone or tie it to other actionable intelligence (e.g. cable degradation / cyber threats impacting adjacent locations). In addition, our system elevates confidence that this is a classification attack. Touching on how operationally significant this ability is for every marine security operation, that it targets one of the most serious flaws in maritime security, "no AIS data" equals no vessels. In bad times, the converse is generally more accurate. MARITIME SENTINEL utilizes both collaborative and non-collaborative detection capabilities which enable it to discover vessels using either passive or active masking techniques. This typically would escape the attention of traditional AIS only monitoring networks. It can also initiate inter-domain linkages as dark vessel module is closely associated with infrastructure and threat intelligence. Many hybrid threats elevate this practice more than any others.

4.3. Cyber-Physical Threat Intelligence Integration

Herein, the third core module increases the system capacity by incorporating cyber-physical threat intelligence sharing within the operational horizon, along with vessel analytics. Part acknowledges that maritime security threats are increasingly transcending physical and digital boundaries. An overall threat proxy assessment may not be doable just by looking at vessel trajectories and their relative positions of view. Both the linked ones, and the cyber anomalies which hit on one or numerous vessels relative to navigation (for example, to distinguish between secondary text-based reports; all cyber alerts & incident indicator in MARITIME SENTINEL were considered initially as first class geospatial objects).

The threat framework in the prototype comprises four broad categories. GPS spoofing -the second scenario to highlight is the knowledge of ships providing false positions which turns a ship off its intended path or provides inaccurate maritime domain awareness as a result of fabricated or coerced navigation signals. The second category of threats falls into that of AIS data injection: (i) Fake vessels which produced phantom ships, (ii) corruption of the record of a vessels movement and (iii) fake identity and location creation using false or repeated broadcasts. The third category consists of SCADA or industrial control system intrusion attempts targeting maritime and offshore infrastructure, such as platforms, terminal facilities and port-based industrial equipment. The fourth category is undersea cable interference, which includes suspected surveillance, physical disruption, signal quality problems or anomalies indicating a planned foreign influence.

This module normalizes the data prior to presenting and analyzing it, because these threat indicators come from disparate sources and formats. Structured event processing normalizes threat intelligence data from external sources into a single normalized format including the timestamp, type, severity, confidence level, source of data and geographic relevance. If the events have been accurately captured with coordinates, you will see location accurate on the map. The confusion about where the sample is physically located (GIS location) is what marking geographic refers too, therefore reporting on data based economic infrastructure connections network structure and reported jurisdiction or proximity to affected maritime resources (IE heavy industrial ports within water that holds of unique plant and animal populations). Even if the first detection is performed by a cyber-geographic device rather than a navigation one, this strategy treats an incursion of an offshore facility as virtually equal to any other geographical event.

The beauty of this module is its ability to provide an integrated analytic environment encapsulating cyber indicators around a maritime activity. SCADA can be hacked into controlling the LNG terminal, and suspicious AIS activity in their neighbourhood may need thorough investigation. By associating cyber-physical alerts with a geolocation, the platform allows digital anomalies to be treated as more concrete indicators, specifically operationally-relevant ones that are co-located with real assets, locales and actual maritime operations.

4.4. NATO-Compliant Alerting and Zone Visualization

Using interconnected observations, the fourth module establishes a support system for decision-making through systematic operational warnings. Such systems monitor critical maritime infrastructure perhaps associated with naval and alliance operations, using NATO-compatible visualisation and escalation protocols. This allows the system to provide threat information in formats suitable for civilian infrastructure oversight as well as defense geospatial situational awareness.

This system triggers alerts from the results generated by all of previous modules. Escalation classifications include intelligence incidents that are captured by recordings of vessel anomaly ratings, dark vessel identifications, cyber-physical threat events and proximity data for critical infrastructure. These classifications are based on alert level modeled after STANAG 5516, that is adapted to operational basis for a prototype dashboard. The low alert levels represent dubious observations that are exceptionally or anomalously correlated events, i.e. unexplained lingering with domain support (e.g. something nearing a sensitive facility but not providing other supporting evidence from several domains). It engages at higher levels when sensors are triggered, unidentifed SAR contact close to cable infrastructure, jamming and physical movement out of safety exclusion zones into the open sea.

Such escalations cannot be properly assessed without the geographic context provided by military zone mapping. This shows, using NATO-standard symbols and mapping practices, any restricted areas, exclusion zones or patrol regions and other operationally sensitive maritime sites. The same exact ship does the same exact actions. However, despite that generalisation of response over similar alert histories not quite turning out to have consistently generated uniform alert reactions which on sometimes too obliquely mixed levels can very greatly vary from essentially having been sequenced under some commercial waters, edge of offshore energy infrastructure or within high military relevance commercialised ocean. So in short, connectivity escalation system is behavioural jurisdictional and should see alerts with an operational relevance rather than being just a deviation.

This module is based on the assumption that ordering dashboard according to a visual simple order of rank improves analyst productivity. Alerts are made up of symbols, colour-coded severity levels, and a textual event description that can be browsed beside their links to particular map regions or a timeline. This enables operators to easily switch from the wider situational awareness to detailed incident investigations with input data specified for every individual alert. Operationally speaking, it allows for rapid prioritisation and decision-making that is crucial to avoiding unnecessary disruption in a context where false alarms could be devastating. Simultaneously, omitted relationships can permit grave occurrences to go unseen.

We could consider the analytical back bone of MARITIME SENTINEL these four core function modules together. Live AIS behavioural monitoring it establishes the benchmark from which all suspicious activity is measured for any vessel. The ability of AIS-SAR correlation expands the coverage range in case of non-cooperative targets. This provides a cross-domain view by integration of cyber-physical threats in. This synthesis of temporal evidence into contextually accurate decisions and the replication of combination supply chain data scenarios (and automated alerting behavior in cybersecurity) around urban infrastructure synthesizes thorough, aggregated marine security insights enabling local responses amid operationally denied maritime environments range.

5. Geospatial visualisation and user interface

MARITIME SENTINEL turns value into operational use by sufficiently collecting this data, analysing it rigorously and communicating complex maritime cyber-physical information in a compact script. Based on an open-source OpenLayers v8 principles, it uses a web GIS visualization system. This chassis opens up to allow analysts to see different real-time data layers, and is all explored through a basic web browser. A nicely crafted interface minimizes the cognitive load for the user, but enables them to consume all of the depth and breadth of spatial, temporal time and threat intelligence necessary to manage incidents.

5.1. OpenLayers implementation details

The development team selected OpenLayers v8 to use for frontend mapping due its ability to handle live geospatial data responsibly and appropriately, and being flexible yet robust. This library also enables fast display of vector and raster layers, while allowing users to modify features on the fly, change visual styling or read from standard geospatial formats like GeoJSON, WMS or XYZ tiles. Nothing else compares to such abilities that involve the orchestration across layers of map features, the moving records of fleet vessels and maintenance of extensive stretches of geography for maritime uses. Your particularly large desktop is, above and beyond a map of the browser. Ship movements, security threats, construction objects and military lines can be distinguished on different map layers with unique graphical symbols. The data is fetched live from the Flask app (via API requests). No page refreshes, and vessel positions, risk evaluations and warning alerts all update seamlessly. The front end is event-driven so that user actions such as zooming in and out, click dimensional features, toggle layers visibility or navigating through the alert notifications get instant feedback.

One of the key aspects we used to design our system was performance optimisation. Because vessel data streams are always changing marker, we use aggregation and very simplified geometry representation with precise steps in refresh time to promise an application responsive performance. This allows you to identify features with high risk while the remaining display of the map doesn't become visually distracting.

5.2. Layer management and rendering strategy

MARITIME SENTINEL offers a layered visualisation, where each information category exists on its own visual layer. This allows analysts to highlight, hide or showcase certain data based on their goals. A foundational layer provides a nautical or satellite mapping context (maritime borders, underwater topography, coastlines, etc. From this base layer other layers of operations are built upon.

Visualizing live AIS tracking data, the vessel layer includes ships icons representing their position and relative direction, as well as alerts for any anomalous behaviour. Using colour-coded behavioural risk level icons, these symbols are designed to help operators quickly identify potentially suspicious vessels. The infrastructure layer shows vital maritime assets like LNG terminals, offshore drilling platforms, commercial harbors and subsea cables. These assets are visualized as a point, line or polygon based on their physical form. Distance from a risk allows the activation of Protective zones, and Proximity corridors on demand for hazard assessment.

Cyber physical security incidents are: cable damage warning, GPS spoofing attempt, SCADA system intrusion attemptand AIS data tampering (under threat intelligence layer). Risk levels of each threat are signified using icons and colour gradients. Military operations in an Integrated Common Environment (ICE) NATO related information overlays, like the exclusion boundary lines and restricted zones and patrol areas are residing within this layer of their ICE. This stratum provides the operational and jurisdictional context that allows for an interpretation of suspicious activity.

Only renders what it needs so trojan alerts and moving objects are always drawn in front of a darkened background layer. We maintain visibility of significant geographic relations by keeping the base transparency settings. This multi-layer design allows operators to move quickly from high-level strategic data views to tactical insight as a whole with one, unified interface.

5.3. User workflow for threat investigation

The user protocol is extracted from reality about how maritime security operations are performed. Threats must be identified, authenticated, triaged and respond swiftly. Operational overview that is generally reviewed over time to trigger the process. Operators deliver a real-time dashboard used for tracking vessel movements, status of infrastructure and assessing alerts. Any anomalous or serious behaviour that your system detects can be flagged up as an alert, and this usually is clickable so it will take the analyst directly to the corresponding alarm displacement in the map.

The operator then analyses the supporting data by toggling on or off different layers of data. They can monitor a suspect ship while also monitoring nearby undersea cables, new GPS interference warnings, or closed military zones. Time-based replay options will identify whether the ship was at

another important event, turned and went away unexpectedly, stopped transmitting its position or stayed in one place. After it has collected enough context an analyst classifies the incident as benign, vulnerable, or needing urgent remediation. Notifications of major incidents may be sent to port authorities, coast guard units, naval operational centers or infrastructure operators depending on the case and user clearance.

MARITIME SENTINEL aims to collate distributed maritime and cyber security intelligence data into a single landscape/architecture, providing decision-makers with the information they need to respond better and faster to threats. This workflow exemplifies this objective.

6. Experimental setup and evaluation methodology

Researchers performed a number of controlled tests to verify how MARITIME SENTINEL would actually perform. They used realistic maritime threat scenarios that closely mimicked actual cyber-physical attacks on critical maritime infrastructure to run the tests. The test was to see if the platform could rapidly detect suspicious behavior, consume hundreds of unique threat signals from multiple sources, and filter out blind spots that can leave critical operational environments unsusceptible. Due to the intrinsic difficulties of accessing real hostile incident data (Dimakopoulou & Rantos, 2024; Vaarandi et al., 2025), scenario-based simulation was chosen by the team as it is considered both a pragmatic and repeatable validation approach.

Researchers derived five attack scenarios from patterns at open-source intelligence reports, standard NATO red-team training exercises, and actual events reported by the maritime security community. In each case, the platform's ability to connect information across different domains was put to the test, which in turn focused on a specific threat category. The first test was in relation to a commercial vessel that suspiciously loitered on an underwater communication cable route and then, for unexplained reasons, stopped transmitting box messages via AIS. The second scenario portrayed a dark vessel operating in a designated offshore energy zone with no corresponding AIS signals. The ship was identified on synthetic aperture radar (SAR) imagery (Li et al., 2025). The third experiment used coordinated GPS spoofing attacks that produced spurious vessel positions in close proximity to a major port entry (Agrebi, et al., 2025). In the fourth case, an alert of a cyberattack to industrial control systems (ICSs) at an LNG terminal and anomalous maritime traffic nearing the facility's protected zone was issued (Alvarez & Moreno 2025). By amalgamating diverse alerting indicators into one test omitting widespread forms of sabotage or espionage, e.g. deteriorated cable signals, inconsistent AIS identities, and an unwavering boating proximity all awareness were triggered in the fifth test (Dumitrescu & Ionescu 2025).The MARITIME SENTINEL prototype was tested using a conventional workstation together with a Python Flask backend and browser-based OpenLayers interface (Ferraro et al., 2025). The researchers created realistic artificial AIS data streams from the recording of real vessel movements, with embedded position coordinates, speed, course and unique identification numbers for the vessels available in real-time. The vessel demonstrates menacing behavior, including course changes, slow speed, standing still places where normal commercial trafficking is tracked (Mixture Normal Traffic), and signal breaks. We treated SAR detections as periodic location based vessel observations coincide with particular scenario events in time. Cyber threat intelligence (Raza & Mahmood, 2025) was introduced with the integration of structured alerts in terms of timestamps, severity ratings, and references to underlying infrastructure.

The simulation included important marine data used by offshore platforms, LNG terminals, underwater cable pathways & commercial port areas. Using adjustable polygon overlays (military zone plus no-go zone) also allowed us to define usable polygons for the purpose of testing proximity detection and alert escalation. Buffer zones were implemented, according to scenario requirements, surrounding target facilities for the vessels and IPLM to warn them when they come too close.

Three main metrics were used to assess the performance of the system, namely correlation precision, classification accuracy and detection speed. Detect speed: the duration it takes to deliver dashboard alerts after detection of relevant source data. This is particularly operationally critical with regards to demand as response time or if threat situations are influenced by vessel movements in the context of

maritime security. Consequently, this measurement was selected. We assessed classification accuracy by deriving false positives, false negatives, thresholds for triggers relative to nearby infrastructure and behavioural anomalies. Because this had been the most critical concern (false negatives were extremely costly with respect to failing to detect an attack close to strategic targets). Specifically, correlation precision (Romero & Mitsis 2025) indicated the capacity for multiple independent indicators to be fused together (e.g. SAR detections, AIS anomalies as well as cyber alerts and physical infrastructure events), creating one actionable operational event in an integrated platform.

Since latency from rendering to browser and the populating of our data takes time due to its asynchronous nature, each scenario was executed a number of times within an interval. It also means that all of the trigger timestamps for the alerts, rules fired and the results seen by operators are logged automatically on the backend for later analysis. The investigators examined exceptional situations where associations were delayed or simultaneous alerts were turned off through calculated means across runs. This methodology elucidated the assessment of the platform as an operational decision-support tool versus merely a classification algorithm. Detection speed and raw, ground-truth accuracy (to compare how the analysts actually did) were among success measures but also alert clarity, location relevance, and analyst usability. This illustrates the MARITIME SENTINEL core tenet that effective maritime cybersecurity requires digital fusion of relevant cyber-physical threat evidence, infrastructure vulnerabilities risk data and vessel behaviour through a common geographical reference timeframe for timely and easy interpretation (Marinakis & Petrou, 2025).

Then, the experimental setup is described in Table 1 such as air simulated threat event, utilized data sources, target infrastructure of experiment, its main validation objective for each scenario and indicated analyzed performance metrics.

Table 1. Experimental setup and scenario design

Scenario ID	Simulated Threat Event	Data Sources Used	Target Asset / Zone	Primary Objective	Metrics Evaluated
S1	Vessel loitering followed by AIS silence	AIS	Subsea cable corridor	Detect suspicious proximity behaviour	Latency, False Negatives
S2	Dark vessel without AIS transmission	SAR + AIS	Offshore energy platform	Validate dark vessel correlation	Correlation Accuracy, Latency
S3	GPS spoofing with false vessel positions	AIS + Cyber Alerts	Port approach channel	Detect navigation deception	Detection Accuracy
S4	SCADA intrusion with approaching vessel traffic	Cyber Alerts + AIS	LNG terminal	Cross-domain threat fusion	Correlation Accuracy
S5	Hybrid sabotage / espionage scenario	AIS + SAR + Cyber Alerts	Cable + Restricted Zone	Multi-indicator escalation logic	Full System Performance

To ensure a structured and reproducible evaluation of MARITIME SENTINEL, the assessment campaign focused on five typical maritime cyber-physical threat scenarios. Employing real-life documented events, maritime risk patterns and defence-based exercise models, each scenario was formulated to produce a realistic operational environment. The scenarios aimed at modelling realistic attacker behaviour for critical maritime infrastructure including, but not restricted to, underwater communication cables, offshore energy facilities, LNG terminals and high value port installations (Dimakopoulou & Rantos, 2024; Liu & Amri, 2025) rather than only generating synthetic anomolies.

Cases selected (S1-S5) in Table 1, and the nature of threat they encompass, ranging from industrial cyber-attack + hybrid sabotage incident (+ rusting ship) background to non-cooperative maritime activity to suspicious vessel-operation activities. Having the ability to detect isolated anomalies, which was recently reported (Li et al., 2025; Romero & Mitsis, 2025), we further tested the platform's capability of fusing multiple sources of evidence into a single operational warning. Geospatial proximity rules, AIS data, warnings from SAR observations and cyber alerts were all extracted together.

7. Results

Tests showed that, for all five maritime threat simulation scenarios conducted during the tests, MARITIME SENTINEL offered reliable real-time detection, as well as geospatial correlation capabilities. Right down the line from its core operational objectives, which is generation of alerts in real-time and correlation of events across different data streams with high precision. The platform has delivered where it had to fast dashboard displays while hundreds of types of data flow into them live and threat detection against infrastructure.

Overall time to complete the entire threat detection process from receipt of first-level AIS, SAR, or cyber intelligence data to alert shown on a dashboard was <12 sec (S1 to S5) (see Table 2). Average response times ranged from 4-8 seconds for simpler cases such as vessels that remain in extremely close vicinity to protected infrastructure, or GPS spoofing events. However, we incur a little larger processing overhead in scenarios where multiple sources need to be correlated (e.g., dark vessel detection and infrastructure anomaly is happening at the same time).

Table 2 details MARITIME SENTINEL performance against the five threat simulation scenarios including inspection on detection latencies, false negatives, correlation outcomes and classifications by alert echelon.

Table 2. Experimental results summary

Scenario ID	Threat Type	Mean Detection Latency (s)	False Negatives	Correlation Success	Alert Tier Reached
S1	Loitering + AIS silence	5.8	0	N/A	Medium
S2	Dark vessel detection	9.6	0	Yes	High
S3	GPS spoofing	4.9	0	Yes	Medium
S4	SCADA intrusion + vessel proximity	8.7	0	Yes	High
S5	Hybrid sabotage / espionage	11.4	0	Yes	Critical

The Anomaly Detection part of the Vessel Behaviour worked appropriately for ship-based cases. Using the defined threshold parameters for its own and other ships, it was able to continuously identify and escalate behaviours such as continued loitering, abrupt changes in course, stopping AIS transmission when near a restricted area, and repetitive passing patterns near sensitive resources. Thus, this specific rule-based scoring approach based on weights was particularly successful at identifying which maritime commercial vessel activity was normal and could be automated as opposed to what would need an analyst review. In the end, all scenarios involving true suspicious activity close to protected maritime foundation deserved appropriate notices being provided. The success criteria for evaluation was zero false positives on all of the key infrastructure proximity events.

An example of this is the excellent performance we achieved with the AIS-SAR correlation component. For dark vessel scenarios where suspected non-cooperative maritime operations are classified as search and rescue (SAR) detections, they were accurately identified without any associated AIS data. It used a combination of AIS information on vessels onboard and synchronisation with the timing of satellite detections to identify targets that did not correspond with known high probability

persistent contacts (AIS transmitting vessels). The findings from those analyses showed the advantage of utilising both cooperative and non-cooperative techniques to monitor maritime traffic, particularly for environment that could be susceptible to deliberate jamming of AIS signals.

Incorporated cyber-physical threat intelligence during the testing process. Way checking know rightly an all of and this operationally normalisation, geospatial identifiers, and processed them GPS spoofing SCADA intrusion attempts monitoring smart artificial intelligence sensors manipulate nothing these within simulated alerts for it. In instances where these alerts were associated with suspicious vessels or infringements of secure areas, the fusion engine automatically elevated the alert to higher levels. Analysts can now make better-informed decisions by bridging the gap between maritime operational awareness and cyber monitoring outputs. The hybrid case that examined the prospect of a cable interfering with operations yielded the greatest commercial benefit. That was how the system, during this same time frame in this region, had detected an undersea cable being degraded as a result of a simultaneous event and practicing the whole area to determine the cause emanating from some dark vessel that it had found responsible. Each incident on its own was not so alarming to indicate hostile action in and of itself but the convergence of multiple incidents at one location with no apparent reason that would lead to such movement warranted a greater level of alarm. This is a reiteration of the primary value proposition of MARITIME SENTINEL, which is the discovery of hidden linkages between indicators from ship behaviours through to infrastructure issues and cyber events. It is hard to identify in traditional isolation-monitoring systems.

All of the evaluations were carried out using a web interface based on OpenLayers, which apparently continued to be usable overall. The functions we tested for live ship monitoring, alerts notifications, toggle layers visibility and navigation on the map against simulation traffic situations events worked as expected. But even in that case, multiple thousand alerts with eveery entitiy activated did not slow down visualization or interaction performance of the dashboard. It suggests that the selection of web framework is fairly appropriate for light business workloads and would handle heavier use cases given a small backend scaling or feed distribution enhancement.

For example, a flexible modular design is used to process different data streams in an efficient manner (e.g., scalability tests executed over several test sessions). It was the higher event volumes that led to increased correlation process times rather than instability of the interface, as all elements in the elements (ingestion, scoring, correlation and visualisation etc) were kept discrete. This makes good sense for the existing architecture to be viable and very easily be scaled with the transformations of microservices-based or distributed systems where individual processing modules could be separate in scaling up.

The results presented here confirm the core argument in this paper that an open source maritime geospatial intelligence platform can integrate and process AIS data, satellite detections (as well as analysing their suitability to work with), cyber threat intelligence, and cyber infrastructure data in a matter of minutes to create actionable situational awareness for maritime security. The combination of this with quick detection response to individual events, its exceedingly good accuracy for cases at critical proximity. Achievement in correlation of hybrid-events and a stable performance of the dashboard finally provides proof-of-value functionality MARITIME SENTINEL can offer for the protection of high priority maritime assets, even under such unfavorable circumstances.

8. Discussion

These results implies that, with MARITIME SENTINEL, a enabling geospatial situational awareness to extend your maritime cybersecurity strategy over all of the waters at risk. Utilizing and integrating their experience for nearest infrastructures knowledge, cyber threats intelligence based analytics, awareness spots of AIS, dark vessels detection and identification to sick the rapid detection of the most anomalous activities that concern ports offshore platforms LNG terminals & subsea cable networks.

The proposed system is sort of a bonus, as it ties back to the information within its industry. Rather than treating vessel traffic or cyber alerts in isolation (as is often the case with more traditional solutions). MARITIME SENTINEL merges data from various sources in order to construct a

comprehensive operational picture. What this allows for is still a connection of seemingly disconnected events (the correlation between cable degradation events and dark vessel activity) with detection speeds appropriate for real time mitigation. However, some limitations persist in light of these advantages. The dependability of the platform is dependent on an integrity (and coverage) onto which external data sources can be placed upon it (e.g. AIS coverage, revisit rates of satellite assets and real time cyber threat intelligence feeds). In those scenarios, air detection performance might be driven down as insufficient sensor tracking directly leads to lower data assimilation where needed. The one we have is also only a research prototype, not production-ready. Future development entails scale, live data streams seamlessly integrating into the platform, verification systems and stability during high volume trading times.

Right now, it suffers a kind of morass of dependence on how much garbage we put in like AIS coverage, SAR imagery and real-time cyber intelligence. Currently, the implement is also a research prototype so further work on operational robustness and integrated secure live-feed integration at scale will be required. Last, MARITIME SENTINEL deploys a recent maritime observation approach that is based upon distilling the cyber-physical intelligence information awareness with regard to an infrastructure-aware strategy in considering hybrid threat discovery capabilities looking in the future.

9. Future work

MARITIME SENTINEL is just a prototype and there are countless ways its capabilities can be expanded. The biggest potential for innovation is around the integration of multiple different sensing technologies to enhance maritime domain awareness and minimise dependence on a single data feed. Future iterations of the platform may include proposed platform upgrades to earlier versions of the satellite environmental sensors, unmanned aerial surveillance dataset, coastal radar networks and underwater acoustic monitoring. All these improvements would improve detectability in regards to threats against ocean infrastructure, vessels operating inside the low-visibility envelope or missions outside the traditional AIS range of collectablity.

Predictive analysis and enhanced anomaly detection through machine learning is also another big area of improvement. While an operationally explicit (and interpretable) rule based systems might detect one or two deviations from the static thresholds, future models could learn the historical traffic patterns of moving vessel behaviour over time with a means to subsequently auto flag such minor deviations which would otherwise pass unnoticed. Trajectory clustering coupled with graph based behavioural analysis and either supervised threat classification is one such method for improving identification whilst concurrently reducing false alerts. Besides that, this platform can help in moving it ahead with its predictive analytics features. Whereas recognition of current events is all well and good. Future systems would score probability within the context of trajectory profiles across multiple decades, a growing sense around re-occuring event type patterns (not unlike forest fire) geography/politics seasonality as well known infrastructure first or last responses. Such an approach may give operators a much more proactive posture in security where instead of acting reactively after escalation has taken place, they can take preventive measures.

The operational implementation perspectiveFuture development needs to take into consideration real world deployment requirements of NATO´s and national maritime security agencies. This encompasses the secure integration of real-time data, interoperability among command-and-control architectures (including a significant degree of content and protocols), information security controls for user authentication, measures designated as role-based access control that also govern sharing abilities, flexible deployment infrastructures (cloud or periphery), and compliance with standards established by defence agencies to enable trusted interconnectivity. This would confirm how the system worked in the field and execute additional fieldtests in an authentic naval environment.

All future development project should focus on a long-term vision to use MARITIME SENTINEL in an operationally viable and scalable infrastructure (step above a research prototype system) which enables command-and control backbone for advanced maritime cyber-physical defence operations.

10. Conclusion

This paper described the concept of MARITIME SENTINEL, a prototype Web GIS platform developed for increasing effective security on critical maritime infrastructure by integrating geospatial monitoring and cyber capabilities. The system incorporated the following capabilities in one streamlined operational architecture, built on a Python Flask backend and OpenLayers v8: real-time AIS vessel tracking, behavioural anomaly detection, dark vessel detection using AIS-SAR correlation from GSAT radar satellite information via NATO compatible alert visualisation of cyber threat intelligence.

The conclusion was that maritime cyber-physical situational awareness can indeed be supported by open-source geospatial technologies. It issued proximity alerts for infrastructure with high reliability, rapid detection response time and good quality event correlation between indicators (cable signal drop in health and suspicious vessel behaviour). Such results confirm the necessity of integrating maritime traffic information, remote sensing data, cyber alerts and infrastructure characteristics into an overarching operational context. As maritime infrastructure grows increasingly important from a strategic perspective and is therefore also more vulnerable to hybrid threats, geospatial fusion technologies are likely to become a key foundational element of future defence and resilience frameworks. These results highlight how the adoption of a modern Web GIS framework like MARITIME SENTINEL towards its future development will translate to better detection speed and operational awareness in civilian/military maritime security operations. Additionally, it provided assistance in decision-making support processes.

Conflict of interest: The Author's declare no Conflict of interest.

References

1. A. Dimakopoulou and K. Rantos, “Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0,” *Journal of Marine Science and Engineering*, vol. 12, no. 6, p. 919, 2024, doi: 10.3390/jmse12060919.
2. I. Progoulakis, I. K. Dagkinis, A. Dimakopoulou, T. Lilas, N. Nikitakos, and P. M. Psomas, “Cyber–Physical Security Assessment for Maritime Vessels: Study on Drillship DP System Using American Petroleum Institute Security Risk Analysis and Bow-Tie Analysis,” *Journal of Marine Science and Engineering*, vol. 12, no. 10, p. 1757, 2024, doi: 10.3390/jmse12101757.
3. M. V. Clavijo Mesa, C. E. Patiño-Rodríguez, and F. J. Guevara Carazas, “Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains,” *Information*, vol. 15, no. 11, p. 710, 2024, doi: 10.3390/info15110710.
4. U. Son and J.-H. Huh, “A Survey of Cyber Security for Maritime Autonomous Surface Ships: Opportunities, Challenges, and Future Directions,” *IEEE Transactions on Intelligent Transportation Systems*, early access, 2025, doi: 10.1109/TITS.2025.3560809.
5. I. Agrebi, N. K. Popli, and M. S. I. Mamun, “Synthetic GPS Data Generation and AI Detection-Response for Spoofing on Maritime Autonomous Surface Ships,” *IEEE Access*, vol. 13, pp. 212867–212876, 2025, doi: 10.1109/ACCESS.2025.3637541.
6. G. Liu and A. Amri, “Survey and Future Trends for Cybersecurity in Maritime and Port Sectors: A Discrete Event Systems Perspective,” *Mathematics*, vol. 13, no. 22, p. 3650, 2025, doi: 10.3390/math13223650.
7. R. Vaarandi, L. Tsiopoulos, G. Visky, M. Ur Rehman, and H. Bahsi, “Literature Review: Cyber Security Monitoring in Maritime,” *arXiv preprint* arXiv:2503.18173, 2025, doi: 10.48550/arXiv.2503.18173.

8. C. Maganaris, E. Protopapadakis, and N. Doulamis, “Outlier Detection in Maritime Environments Using AIS Data and Deep Recurrent Architectures,” *arXiv preprint* arXiv:2406.09966, 2024, doi: 10.48550/arXiv.2406.09966.
9. Z. Xie, E. Tu, X. Fu, G. Yuan, and Y. Han, “AIS Data-Driven Maritime Monitoring Based on Transformer: A Comprehensive Review,” *arXiv preprint* arXiv:2505.07374, 2025, doi: 10.48550/arXiv.2505.07374.
10. C. Isbaex, F. dos R. F. Costa, and T. Batista, “Application of GIS in the Maritime-Port Sector: A Systematic Review,” *Sustainability*, vol. 17, no. 8, p. 3386, 2025, doi: 10.3390/su17083386.
11. F. Li, K. Yu, C. Yuan, Y. Tian, G. Yang, K. Yin, and Y. Li, “Dark Ship Detection via Optical and SAR Collaboration: An Improved Multi-Feature Association Method Between Remote Sensing Images and AIS Data,” *Remote Sensing*, vol. 17, no. 13, p. 2201, 2025, doi: 10.3390/rs17132201.
12. S. Kavallieratos, E. Katsikas, and P. Kotzanikolaou, “Cybersecurity Challenges in Smart Ports: A Survey of Threats, Vulnerabilities and Countermeasures,” IEEE Access, vol. 12, pp. 14522–14544, 2024, doi: 10.1109/ACCESS.2024.3354120.
13. J. Park and M. Gerla, “Secure Maritime IoT Architectures for Port and Vessel Monitoring,” IEEE Internet of Things Journal, vol. 11, no. 7, pp. 11854–11867, 2024, doi: 10.1109/JIOT.2024.3361182.
14. A. Boulmakoul, N. Karim, and H. Lahrichi, “Artificial Intelligence for Maritime Traffic Anomaly Detection: Recent Advances and Future Trends,” Sensors, vol. 24, no. 9, p. 3882, 2024, doi: 10.3390/s24093882.
15. T. Nguyen, R. Sutton, and L. Wang, “GNSS Spoofing Detection for Autonomous Maritime Navigation Using Multi-Sensor Fusion,” IEEE Transactions on Vehicular Technology, vol. 74, no. 1, pp. 944–956, 2025, doi: 10.1109/TVT.2025.3481021.
16. M. El-Hajj, P. Tsakalides, and Y. Andreopoulos, “Satellite-Based Maritime Surveillance Using Deep Learning and SAR Imagery,” Remote Sensing, vol. 16, no. 3, p. 921, 2024, doi: 10.3390/rs16030921.
17. F. Zhou, Y. Li, and H. Chen, “Port Infrastructure Cyber Resilience Assessment Through Digital Twin Modeling,” Journal of Marine Science and Engineering, vol. 13, no. 2, p. 277, 2025, doi: 10.3390/jmse13020277.
18. R. M. Hassan and J. B. Cruz, “Machine Learning Methods for AIS Trajectory Classification in Congested Coastal Waters,” arXiv preprint arXiv:2408.11852, 2024, doi: 10.48550/arXiv.2408.11852.
19. D. Romero and K. Mitsis, “Hybrid Threat Detection in Maritime Supply Chains Through Cyber-Physical Event Fusion,” IEEE Access, vol. 13, pp. 55412–55429, 2025, doi: 10.1109/ACCESS.2025.3518214.
20. L. Ferraro, M. Giordano, and E. Rossi, “Web GIS Architectures for Real-Time Critical Infrastructure Monitoring,” Future Internet, vol. 17, no. 1, p. 44, 2025, doi: 10.3390/fi17010044.
21. H. Singh and P. Sharma, “Dark Vessel Detection Using SAR and Optical Data Fusion in Maritime Security Operations,” IEEE Geoscience and Remote Sensing Letters, vol. 22, pp. 1–5, 2025, doi: 10.1109/LGRS.2025.3471188.
22. E. T. Mensah and J. K. Boateng, “Cybersecurity Risk Propagation in Maritime Logistics Networks,” Information, vol. 16, no. 1, p. 33, 2025, doi: 10.3390/info16010033.
23. M. Raza and A. Mahmood, “Open-Source Intelligence Integration for Maritime Domain Awareness,” Sensors, vol. 25, no. 4, p. 1650, 2025, doi: 10.3390/s25041650.
24. C. Dumitrescu and V. Ionescu, “Critical Undersea Cable Protection Through Geospatial Risk Analytics,” Sustainability, vol. 17, no. 5, p. 2122, 2025, doi: 10.3390/su17052122.
25. K. Petersen, O. Johansen, and A. Larsen, “Operational Dashboards for NATO Maritime Situational Awareness Systems,” IEEE Systems Journal, vol. 19, no. 2, pp. 1640–1651, 2025, doi: 10.1109/JSYST.2025.3497713.

26. Y. Tanaka and M. Ito, “Explainable AI for Vessel Behavior Anomaly Detection in Maritime Security,” arXiv preprint arXiv:2502.07411, 2025, doi: 10.48550/arXiv.2502.07411.
27. P. Hoffman, S. Lee, and G. Wang, “Real-Time Stream Processing for Large-Scale Maritime AIS Analytics,” IEEE Access, vol. 12, pp. 99221–99236, 2024, doi: 10.1109/ACCESS.2024.3380112.
28. N. Alvarez and F. Moreno, “Cyber-Physical Threat Modeling for LNG Terminal Security,” Journal of Marine Science and Engineering, vol. 13, no. 4, p. 611, 2025, doi: 10.3390/jmse13040611.
29. B. O’Connor and T. Blake, “Detection of AIS Identity Manipulation Using Probabilistic Vessel Profiling,” IEEE Transactions on Intelligent Transportation Systems, early access, 2025, doi: 10.1109/TITS.2025.3529001.
30. G. Marinakis and A. Petrou, “Maritime Security Decision Support Systems Based on Multi-Layer Geospatial Intelligence,” Applied Sciences, vol. 15, no. 6, p. 2877, 2025, doi: 10.3390/app15062877.
31. J. Wu, H. Zhao, and P. Sun, “SCADA Intrusion Detection for Offshore Energy Platforms Using Deep Temporal Models,” IEEE Access, vol. 13, pp. 77110–77124, 2025, doi: 10.1109/ACCESS.2025.3546129.