MBNA Publishing House Constanta 2026



Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Geospatial Visualization of Maritime Cyber-Physical Threats Using OpenLayers

To cite this article: Mihailescu Marius Iulian, Marascu Valentina, Nita Stefania Loredana, Asalomia Laurentiu Bogdan, Samoilescu Gheorghe, Proceedings of the International Scientific Conference SEA-CONF 2026, pg. 26-38.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-26-004
SEA-CONF© 2025. This work is licensed under the CC BY-NC-SA 4.0 License

Geospatial Visualization of Maritime Cyber-Physical Threats Using OpenLayers

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. As the global shipping industry has gone digital (and vessels and ports have become increasingly efficient at conducting commerce) they also face a higher risk of cyberattacks. Hackers can spoof GPS signals, contaminate AIS ship tracking systems, cause ransomware attacks or infiltrate operational networks. None of the existing monitoring systems can effectively relate security events with geographic information. We created an OpenLayers mapping system that displays maritime cyber threats on a web map. What this system does is it integrates data regarding shipping infrastructure, whereabouts of ships, and cyber incidents at a single platform. This is designed to enable security teams with greater situational awareness and speedier decision-making. We have multiple data layers, threat markers signifying where incidents occur, heat maps reflecting troubled areas in the nation and a filter to sift through threats based on their severity. A working version that would face off multiple simulated data was undergone testing amongst GPS Spoofing attacks, cyberattacks of ports as well as criminal vessel impersonation. Research findings such as these have shown how combining cybersecurity data with location intelligence can significantly enhance maritime security. This can allow us in the global shipping industry to keep on trucking with cargo but at a safer distance by mapping out desired locations of such threats.

Keywords: Maritime Cybersecurity; Cyber-Physical Systems; OpenLayers; Geospatial Visualization; Situational Awareness.

1. Introduction

Maritime domain digital infrastructure has recently underpinned the more interlinked and complex COTS computing system that enables global economy. More than 80 percent of world trade are shipped to ports through here. Smart NavigationSatellite-based communication tools and port equipments automationCloud platforms (public or private)GPS trackersElectronic chartsRemote monitoring technologiesThese are no more part of an experimental lab for test; they have got into the normal core operational environment. And it's similar with ports, where digital platforms help coordinate cargo

flows, vessel schedules and logistics processes between supply chains. Afterwards, ships and ports become vast cyber-physical systems, where things (embedded devices), networks (communication setworks) software services and operational technology communicate data in real-time. This is indeed integration and it does help with efficiency, automation and situational awareness. It also brings complex system architecture bringing along a wider attack surface opening up maritime infrastructures which leads to various new cybersecurity threats (Li et al., 2024). Since ships and ports are well-connected, cyber threat has been one of the key challenges faced by operators across all countries including port authorities (shipping companies and government regulators). Frauds like ransomware, GPS spoofing or the fake identity of vessels or people on board using their details illicitly (hence jamming communication ranges) can lead to financial losses and severe safety implications. In contrast to regular cybersecurity incidents, the maritime cyberattacks can directly impact upon physical operations and vessel movements, connected with cargo operations and port activity. For example, changing heading data on a vessel to guide it off its intended course or attacking port facilities to extend loading times and cut supply chain processes. This shows that maritime cyber security must come out of a fantasy, so that digital compromise and physical safety threats cannot be thought as dichotomous (Vaarandi et al., 2023).

Cybersecurity teams fighting maritime cyber threats need context a combined view that ties in (cybersecurity data) and place, location and context but not singularly yet another alert. But the severity of an incident did depend on what was happening at the time and where it occurred. For example, if the victim ship was close to shipping lanes or far from port facilities, etc. But even so, most of the existing monitoring systems either trigger a cyber alert that lacks sufficient spatial context or keeps a general track of vessel movements with no security information available. As a result, operators cannot quickly identify where a threat is taking place, which assets are at risk, and how the incident could affect nearby maritime operations (Raymaker et al., 2025).

One solution to this challenge is to use map-based visualization that converts complex cyber data and events into easy-to-understand format by using graphs, charts, maps, etc. This lets analysts interpret incidents and determine which is the best strategy to recover from a cyber attack, by viewing threat indicators, heat maps and real-time data on interactive maps. In general, open-source web mapping tools are easy to deploy, and flexible over other systems and integration with various systems. Among these tools, OpenLayers is particularly worth mentioning, because it can be used to display dynamic location information in a browser and it is compatible with maritime formats, including vessel tracking feeds and related infrastructure.

Having this technological context, this paper introduces a map-based visualization platform of maritime cyber threats based on the OpenLayers tool. Its aim is to create and test a single web portal awareness tool, that fuses ship positions, port infrastructure data, and cyber incident data. It is intended to enhance incident comprehension, speed up decision-making and enable resilient maritime operations (Miller et al., 2025). As a result, this paper makes three main contributions, mainly: the geospatial cyber threat model for maritime threats in geographic context, the OpenLayers visualisation platform combining maritime and cybersecurity data, and tests that demonstrate the system value for both maritime operation and emergency response (in a real-word scenario).

2. Background and related work

Nowadays, the reliance on cyber systems is increasing as digital technologies spread through maritime operations, by exposing ships and ports and shipping networks to a growing range of cyber-attacks. Maritime organizations are still contending with a constantly changing threat landscape, including ransomware and phishing attacks, network intrusions, and assaults on operational systems. With ports functioning as sophisticated logistics centers and ships requiring more connectivity-based solutions for navigation or monitoring systems, maritime cyber risks are expanding and increasing in complexity (Miller et al., 2025). These types of cyberattacks that target the maritime sector are especially dangerous as they can influence both cyberspace and lead to physical disruption at sea. Unlike traditional cyber-attacks on computers, attacks in this space can take aim at propulsion systems, onboard navigation software, cargo gear and port control systems. Furthermore, digital navigation and communication

technologies increase operational efficiencies. Furthermore, they are also associated with cyber security risks which could affect vessels and their crew. When attackers interfere with the vessel communications or security monitoring centers, the operators will find serious difficulty in effectively responding to an emergency (Cho et al., 2026; Nganga et al., 2024). Port management systems can be crippled into complete inoperability because of ransomware infiltration systems. Which means large sections of a facility must be shut to bring operations to a halt for loading and unloading, which could cause days of supply chain backups. Piracy with hacking where a hacker can change navigation information to reroute the ship or set that vessel on a collision course with others. Mud masks radar occupies shipping channels and renders neighboring vessels effectively blind to the true situation. It also does not make any of the attack types or defense techniques irrelevant in the era of rising digitization of radar and sensing equipment (Longo et al., 2024). Shipping companies have, meanwhile, been spending big on monitoring systems, improved communications protocols and cyber defenses as whole to lessen these impacts. On the other hand, maritime workers and organizations require better training programs, awareness raising campaigns as well as stricter security standards (Nganga et al., 2024).

Geographic technology has been the primary tool for monitoring ships for a long time. Ship traffic (Class A) GPS mapping, vessel traffic tracking systems and awareness platforms for ocean vessels. This will show you source ports, port operations, weather at sea and wherever the waters are blocked. Using these tools, operators will be able to monitor routes traffic, pre-plan better routes and identify irregular movement in coastal and oceanic waters (Kiefer et al. 2021). These ship track systems give a tiny view of this. These systems, and today maritime monitoring systems combine data with radar, satellite images and sensor networks to provide an integrated picture of the maritime domain. Such systems are primarily for navigational safety, logistics chain efficiency, border security or environmental monitoring. Instead, cybersecurity data usually runs in its own silo along containing comparable security dashboards, not within geographic interfaces. Information is scattered across various siloed systems (Zhou, 2025), which incident responders must search.

Studies show that maritime cyber security issues are not merely technical, but a major business transformation. As the shipping industry embraces networked, and semi-autonomous systems it is essential that cybersecurity to be included in system design and seamlessly woven into the operational workflow and risk management from acquisition to deployment. This proves that we need to depend on tools uniting technical alerts with operational data (Kanwal et al., 2024; Kanellopoulos, 2024). The fields of maritime cybersecurity and satellite-based tracking may be maturing rapidly, but there is still much ground to cover in research and practice. With TYPO3 current systems they can visualize ships, routes as well as maritime traffic. They are only limited to cyber security threats in territory information in geographical informations. Data that outlines where and how a cyber-attack propagates to affect local vessels or assets has proven far more elusive. This gap is a clear shortfall of cyber-geographic visualization technologies designed for maritime (Harish et al., 2023; Ungureanu & Gasparotti, 2024).

3. Methodology and system design

We built a geospatial visualization platform to visualize maritime cyber threats monitoring. This was only the first step, and we had to create a system that integrated ship operations data, cybersecurity alerts and where a vessel is located all into one view. Therefore, the decision-makers can respond faster and have better situational awareness.

In addition, we developed this tool as web application with independent modules connected to each other for different tasks. It can gather information from multiple locations, and show likely dangers on colorful, easy-to-read maps. Being modular, we will be able to integrate new services or data sources.

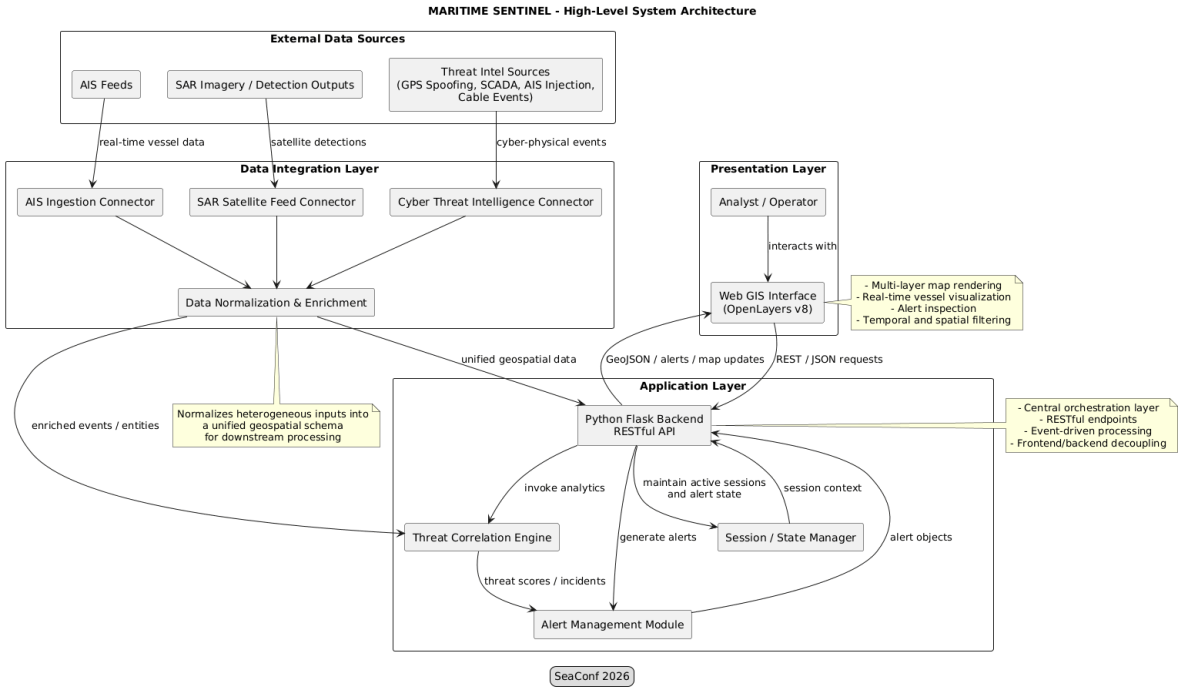


Figure 1. MARITIME SENTINEL – High-Level System Architecture

3.1. High-level architecture overview

Through threat modeling, we determined the main cyber threats to ships and ports. These threats were chosen for their stark effects on the real world, common usage in recent literature describing specific threats that are adjacent to mapping (Li et al., 2024; Miller et al., 2025). GPS spoofing is a commonly risky threat. Attackers broadcast fake satellite signals that mislead ships into thinking they are elsewhere. In these scenarios, vessels begin to operate outside of their course, engage in dangerous operations, run aground or collide with another ship. This is especially dangerous in confined spaces, such as narrow channels or busy shipping routes (Li et al., 2024). One more serious problem is AIS manipulation. Ships use the Automatic Identification System to monitor neighboring vessels and virtually calculate where probable collision types are. Nonetheless, criminals can penetrate this network and send false character signals of themselves. Also, they can coordinate or even impose completely different vessels. Everyone in the world uses AIS data to protect themselves and track traffic, which is why these false signals are misleading for ship operators and coast guards (Raymaker et al., 2025).

If one of those ports were attacked, it would only take hours to put the whole system in energy starvation and shut itself down. Malware locks out computer systems in charge of everything from loading cargo, to managing ships, to handling customs paperwork. Because all ports today are in the digital realm, these types of attacks can block movement of cargo, impact revenues from around millions (Miller et al. 2025), and wreak havoc on global supply chains.Topics also include attacks on industrial control systems. These are the computers that control port machines: cranes, fuel systems, power plants, conveyor belts, and environmental controls. Compromising these systems can shut down port operations or create hazardous situations that risk workers and equipment (Cho et al., 2026).

Not the least of which, disruption of communications rounds out our top threats. Ships and ports rely on satellite links, radio equipment, Internet gateways, and other platforms to communicate with each other. If attackers jam these signals, inundate them with fictitious traffic, or create network failures due to equipment faults in other parts of the world and onshore systems (Nganga et al., 2024), it becomes very difficult for maritime authorities to maintain clear visibility and respond in a timely manner to emergencies.

These five threat categories became the foundation for our new visualization system, as shown in Figure 1.

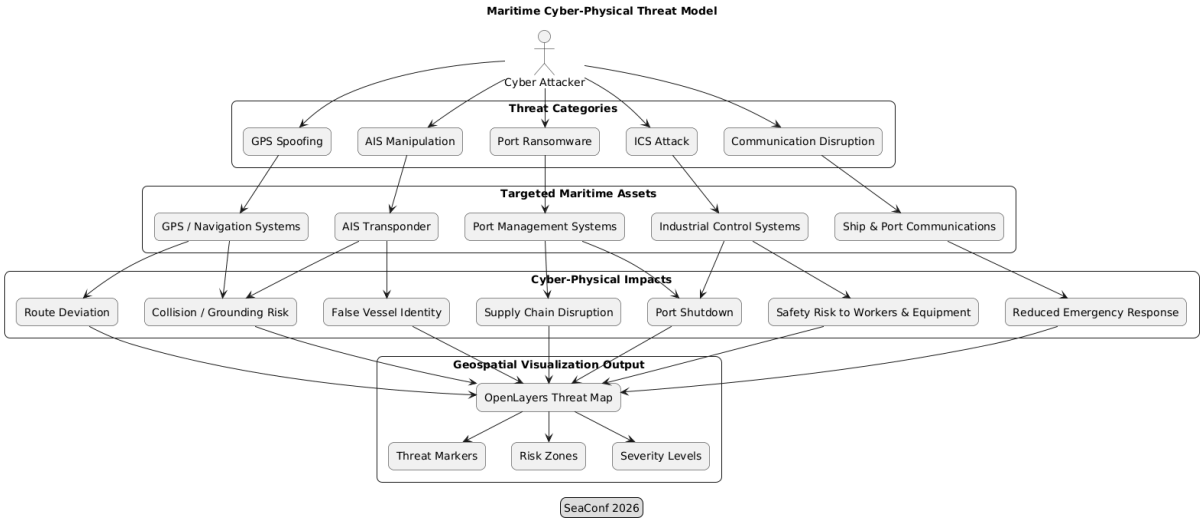


Figure 1. Maritime cyber-physical threat model

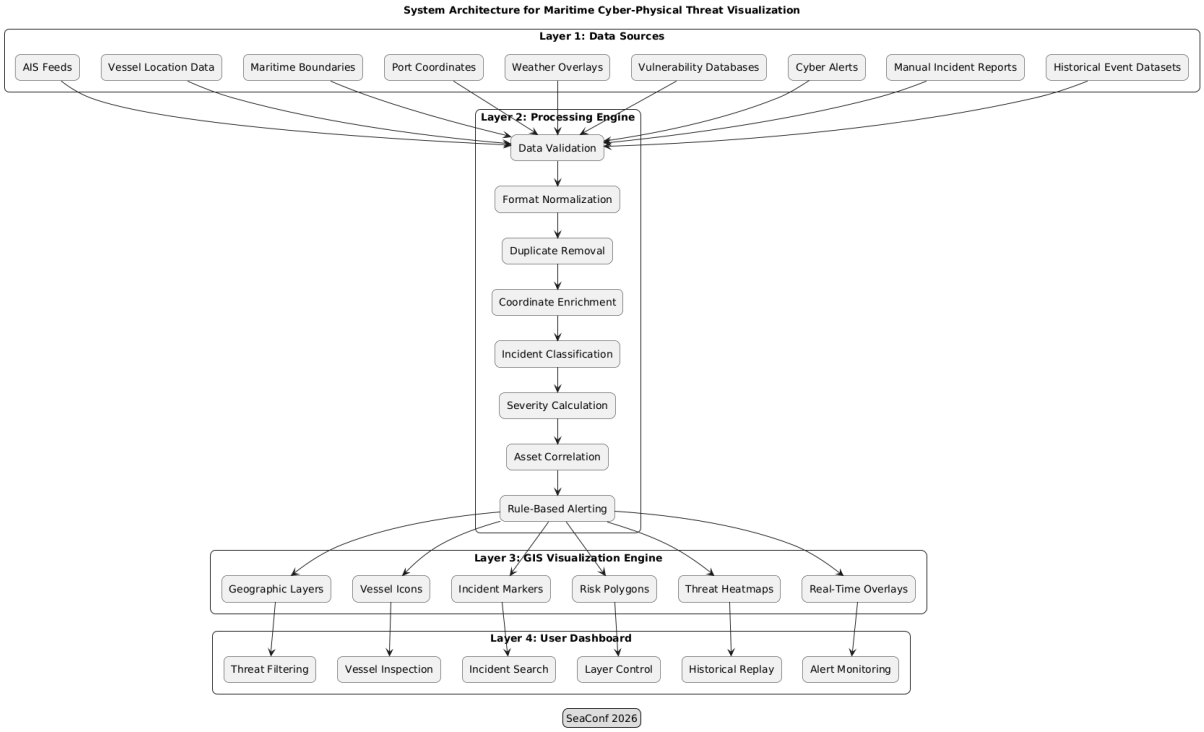


Figure 2. System architecture for maritime cyber-physical threat visualization

3.2. System architecture

The above system architecture is a layered, modular design that scales and provides interoperability. Figure 2 illustrates the entire platform. Four main layers are used. The bottom layer gathers data from many sources. This includes (but is not limited to) satellite data tracking ships, live updates with position feed, nautical maps that outline territorial waters, locations of port facilities and local weather reports. These are also loaded to cover for the past period leading, from historical data. The second layer

organizes all this data and converts the information into knowledge that can be used productively. It validates the data, standardizes everything to the same type, eliminates duplicates from each source, inserts geolocation information into relevant cases, categorizes events by theme, logs the incidence and severity of ongoing threat instances, and calculates proximity and correlation relationships between vessels and occurrences. The preset rules alert the system to trigger when something suspicious occurs, for example, if a ship changes its course suddenly or if several fake ship identities appear in the same area.

The third layer generates the visual maps that users are presented with. It processes and displays data on live maps. This can include geographic features such as drawing ARCGIS zones, displaying ship icons, marking incident locations, or creating colored zones, where areas of interest are identified through the delineation of colored zones; heat maps; or additional layers displaying various information.

The first layer is the user interface that the operator interacts with to access the system. Users can also filter by different threats, see targeted vessels, look up past incidents, toggle between a variety of map views (with many notifications appearing on them) and control an event going on during a time-window against current alerts. All of that converges into a singular command center, giving operators an entire picture of what is happening.

3.3. Technology stack

To develop the prototype, we use OpenLayers (see Figure 3) to run the main mapping system, which is very well suited for vector graphics handling, tile-based web map visualization, user interaction and event handling, as well as being able to render large amounts of data in a web browser without any performance issues.

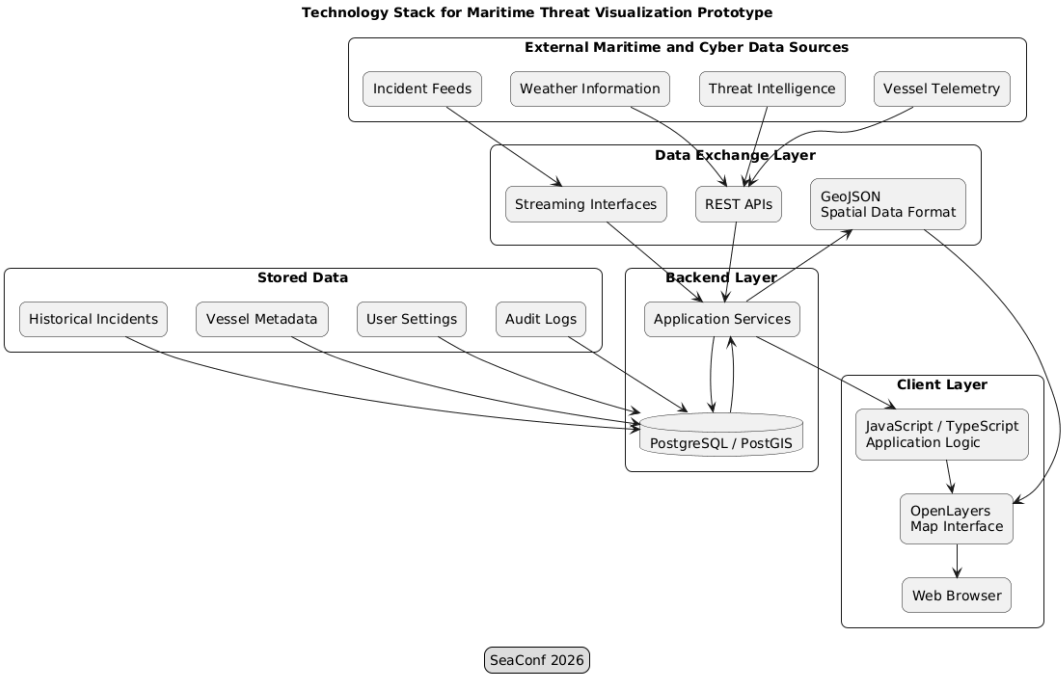


Figure 3. Technology stack for maritime threat visualization prototype

As part of this, there is a GeoJSON location that processes and distributes your data via a chargeable capacity layout along with specifics linked to points, lines, shapes etc. For instance, this is effective for ship and no-go zones, port locations which we currently have as dynamic danger areas on our maps. Through REST APIs and live data streams, it connects to external data sources. Thanks to this connection, it can continuously provide itself with real-time information on the positions of ships, meteorological and environmental conditions, security incidents that happened and threat alerts

generated by other monitoring systems. One specifically is that we have a database management system at the back end, as an incident instances of product information in best practice stored records of information, as well as logging voyaged records with user preference and transaction. This is acceptable in the case of database systems, like PostgreSQL with PostGIS, searchable location data and perform geographic analytics very quickly. The application consists of JavaScript or TypeScript web applications, and as it is being executed in the browser, you can see instant updates and seamless usage with no friction by users.

3.4. Visualization logic

The platform excels at rendering confusing threat data, so that operators can digest it immediately. This is possible by a few visualization tools. Dark blue, purple and other colors represent risk areas as larger-bodied shapes or circles around equipment that are vulnerable to those risks. If someone is trying to spoof GPS signals somewhere near a shipping channel for instance, the system draws a circle that indicates where you might expect a navigational hazard. Targeted attacks such as ransomware attacks at ports will trigger threat icons, communication disruptions on ships will result in a symbol pack being triggered and causing animal behaviour that could damage in-ship-tracker systems. The icon indicates when to do it, what threat you are facing and how disastrous the threat is. Heat maps show where and when cyberattacks cluster. It allows you to visualize these patterns in the form of colored density maps. For example, if hackers send phishing emails to lots of ports simultaneously and signals from ship-tracking vessels behaved strangely in a particular shipping lane.

These data layers show within seconds or in simulated time a vessel's position to its route, speed and heading and based on security events. It enables operators to pinpoint possibly at-risk vessels within range of threats and respond accordingly. Situations with higher perpetual emergency alert levels are colour-coded so that users can quickly comprehend how severe each event is. Green is a simple fact, yellow is a low risk of hazard events, orange events as also high risk for hazards and red events warn significant events needing to be entertained. In tandem with these visual resolutions, self-contained cyber security alerts become fit-for-purpose maritime intelligence that can be operationalized. This allows analysts to examine areas where incidents occurred and determine which ships and facilities may be endangered by these threats, as well as how a threat could spread through nautical environments.

4. Implementation and case studies

We use our real example in this section and explain how we built and tested of our maritime cyber–physical threat visualization platform. This ultimately created a browser-based prototype that integrates ship location accurately, cyber threat notifications and interactive maps generated over the user-friendly interface. It is centered on leveraging mapping capability to enable maritime security teams to detect threats, priorities incidents and retain situational awareness as events unfold at sea.

4.1. Prototype implementation

Our prototype utilized an online dashboard with OpenLayers maps. No proprietary software needed to be installed by the teams. Teams could just use an existing web browser since the interface is native to all reasonably modern ones. It also allows for deployment of maritime operations functions, port security facilities and vessel monitoring stations. Control panels, filters and info windows, neatly aligned around the screen. Display map centered on the screen. You can see ships as moving icons, which indicate the direction in which they came and the direction they go towards. Clicking on a ship reveals its ID, speed, direction and what time it will be imminent or how threatened you are at the present point in time. Colored dots show the severity of cybersecurity incidents around the globe, closer to home. Green dots mean information alerts (heads up on an issue), Yellow signify medium impact, Orange means elevated operational risk, and Red is a critical incident (immediate action required). This enables you to activate heat maps of suspicious activity along shipping routes or coastlines.

The analysis system is an interface for analysts to look at events on multiple time slices. Everything is replayable or shown in whatever time frame you want it. The search facility will enable you to locate

specific ports or vessels on the fly, along with previous alerts. This is extremely helpful for forensic analysis of what has occurred or when you want to know "what else happened after that incident". We filled the prototype with simulated ship traffic data, port location and dummy cyber alerts for testing. This enabled us to replay different scenarios multiple times while keeping ship movements and real maritime geography precise.

4.2. Case study #1 – GPS spoofing

The initial tests examine the scenario when an individual (see Figure 4) attempts to mislead a commercial ship GPS during its journey through a crowded shipping lane. The ship begins following its normal course in this test but is then sent dangerous GPS signals that gradually deceive it into thinking it is at another location compared to where it really.

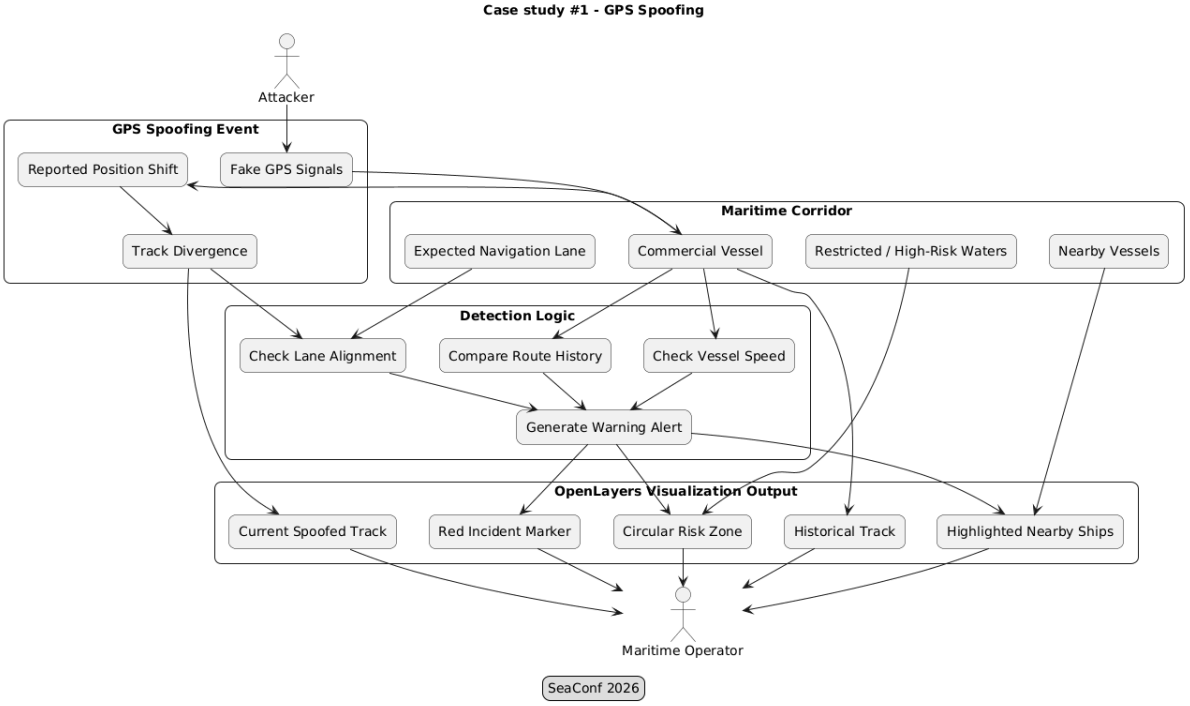


Figure 4. Case study #1 – GPS spoofing

The line indicating the ship's path clearly wanders from where it should be on the screen. The detection software compares the ship's route history, its velocity and ensures that it is sticking close to the right shipping lane, until something doesn't seem quite right. When it senses that something is wrong, it gives an alert. It gently puts a red alert marker on the system where the GPS assault began, and alerts nearby boats that could find themselves in trouble.

Operators can see the map screen of where the ship has traveled in the past on one side compared to what it is doing now and if any failure occurs. This will allow an easy way to see when something isn't going right. It is provided with a map for identifying any ships that may be in the danger zone and letting operators keep track of them. This visual arrangement allows the content to find out whether ships are crashing or if any shipping lanes are being obstructed, or on an approach toward exclusion zones (image credit: MarineTraffic). The Navigation Test shows how visual maps and displays can aid in identifying navigation discrepancies that would likely go unnoticed, if you were merely reading text alerts being displayed on a screen.

4.3. Case study #2 – Port cyberattacks

Figure 5 demonstrates the effects of ransomware targeting computer systems at a container port, being the second example described in this paper. It simulates malware that targets cargo movement

scheduling servers, gate access control systems and loading operations coordination servers. This starts a system-wide issue for the entire terminal. That attack gets tripped, and the status of that port on your dashboard turns sky red to indicate that this is a category one emergency.

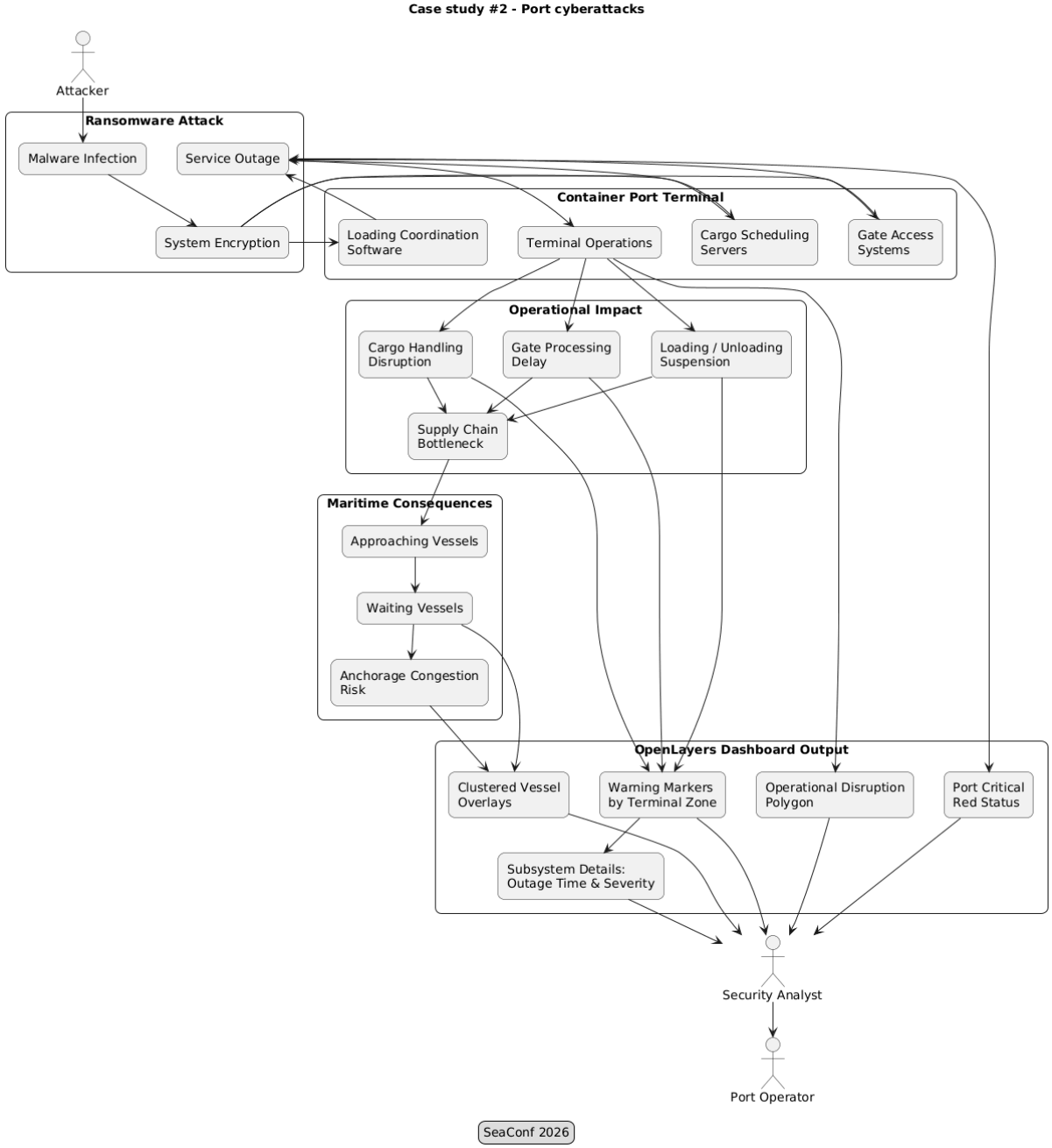


Figure 5. Case study #2 – Port cyberattacks

This component forms the outline of a colored shape, where all the ports with failed services are located, and all affected areas of the terminal flash warning icons. It provides the system that goes down, how long it went down for, and severity level of damage as a warning icon is clicked by a security analyst. It also maps how the assault in question impacts shipping or categories of maritime traffic. It identifies vessels that are arriving at port but holding position for a berth. Visual clusters (where ships could back up, either at anchored or in proximity) are generated by the software. This provides a decision-maker an aggregated view into the operation of the port as designed, and how cyber-attack

delays and/or disrupts ships across multiple ports (Miller et al. 2025). This short example illustrates that when you pair cybersecurity data with geographic visualizations, security teams gain a real-time view into both the technical and economic implications of an attack running side by side.

4.4. Case study #3 – AIS identity fraud

AIS identity fraud (third scenario) occurs when an individual transmits false AIS messages disguising themselves, as a ship that legitimately is already active in the same set of waters. That means that you see two different ship tracks using the same id. This problem is detected by the platform, which searches for duplicate Maritime Mobile Service Identity (MMSI) numbers, that have broadcasted from locations a few kilometers apart that are impossible. In short, if a ship ID is pinged simultaneously in two or more widely separated locations, it flags a medium to high severity alert back into the AISS system.

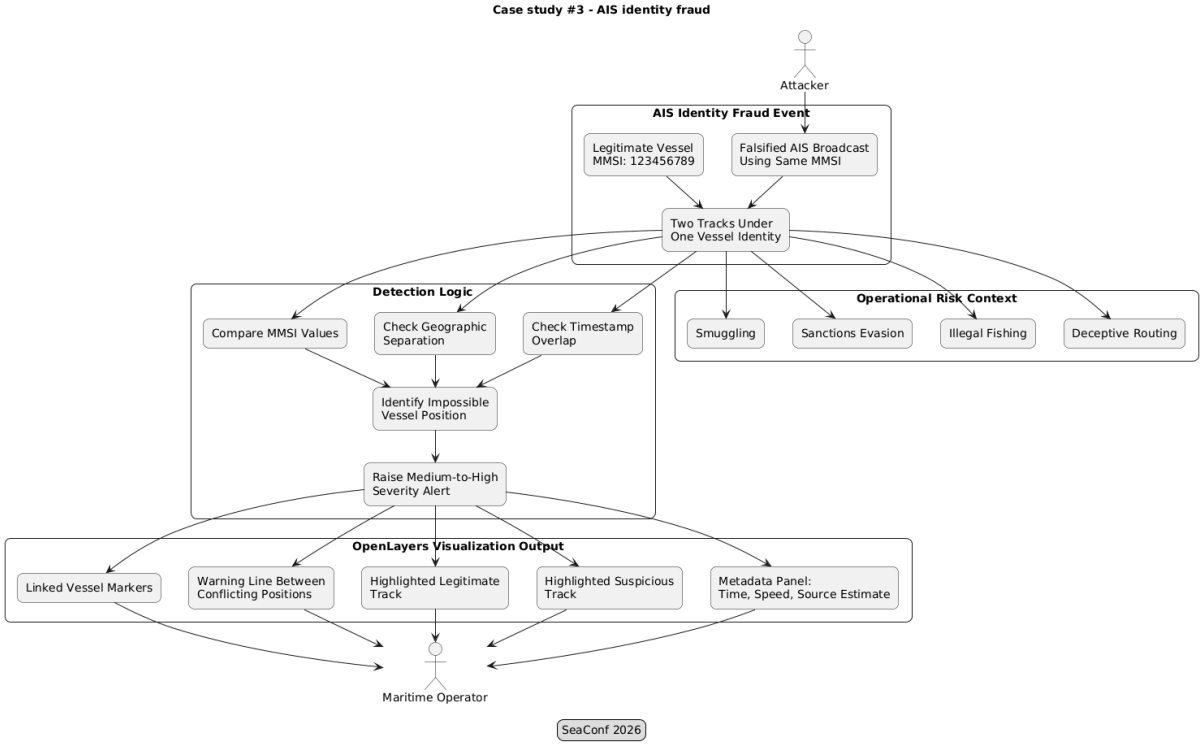


Figure 6. Case study #3 – AIS identity fraud

It shows the two ship tracks on its map and draws markers where they collide, and warning lines connecting them. In addition, it avoids situations where a single ship identity might exist in two places at once. Upper data panels are timestamps, the relative speeds of every observe and a projection of the tracks sounds like our transmission choices. Such fraud is common in case of smuggling, sanction avoidance, illegal fishing or wherever ships attempt to disguise their true marches. However, traditional monitoring tools simply relieve only tables, and lists to detect duplicate identifiers where the map display allows operators to see exactly what is happening (Raymaker et al., 2025).

5. Results and discussion

This section is where we share how our new map-based cybersecurity platform performed and what learnings we gathered while testing it out. The researchers validated it on three potential applications: GPS spoofing attacks, port systems compromised by ransomware, and identity fraud involving ships. We focused on how it allows operators to see events, resolve them faster, and understand where things need to change (the cost of simplicity).

Perhaps the most notable improvement we saw was how much more easily operators could get a clear picture of what was going on during cyberattacks on ships and ports. The majority of cybersecurity

tools present alerts as text or data tables, requiring analysts to interpret each alert and its potential impact on operations. Our map-based system enabled operators to quickly pinpoint where problems were occurring, identify nearby ships and/or facilities, and determine which areas may be affected. In the GPS spoofing example, operators could almost immediately identify that ships had gone off course and detect at-risk vessels. The ransomware test was interesting because operators could see how the computer problems at the port were affecting ship backups and causing delays in the harbor. For example, in the case of a fake identity, operators could directly recognize it was a problem because the same ship appeared in two different locations on the map at the same time. Placing cybersecurity alerts on a map enables people to grasp what the threats look like in real life, as demonstrated by these examples.

It also gave operators the assistance needed to navigate complex scenarios much more quickly. Rather than flipping between screens to see ship traffic, port status, and security alerts, users could get all the information they required briefly. Everything about it was designed for things like markers for threats, color-coded warnings and pop-up info boxes, and understanding events as they unfold. In this line, it becomes a whole lot easier. Inside tests results, the color system was effective. Red alerts denoted high-priority problems, yellow and orange markers were designed to prompt operators about lower-order threats. It is also a necessary tool made useful with analysts deciding what the attackers targeted, and when. Stitching every piece of data together in a single interface enables more efficient decision making, time being of the essence.

One of the biggest advantages for operators was finding out which incidents based on their location should be prioritized. Every vessel is not a cyber-attack, likewise every port. A communication drop-out in the middle of nowhere perhaps not so much than right next to an entrance to your port, chock filled with vessels. Or perhaps GPS jamming right near a key shipping lane or the mouth of an important harbor could require immediate response. By taking a map-based approach, operators were able to assess the proximity of the threats to ships, ports, restricted areas and high-traffic areas to prioritize which alerts required a response first. Heatmaps and risk zones also helped aid resource planning by singing out areas of ongoing suspicious behavior. Coast guards, port authorities and shipping companies don't have an infinite number of people or equipment to solve an unlimited number of problems, and that's where this comes in handy.

The second big takeaway was they could deploy the system using mostly off-the-shelf, open-source technology. Organizations can open the potential of OpenLayers by trying it in web browsers without spending large sums of cash for mapping software patents. This is especially valuable for ports, regional maritime agencies and schools that are not funded. It’s just common web technology built, and it runs natively on your calculator, so no extra hardware. This standards-based approach (adopting open standards like GeoJSON and REST APIs) allows easier integration with other maritime systems down the road, such as ship-tracking feeds or threat-intelligence platforms. In these manners, it will prevents organizations from becoming reliant on a single vendor and drives systems that are sustainable over time.

While the results were promising, we discovered several limitations in testing. For starters, the platform is only as good as the data it receives. To visualize precise ship metrics for the SKA and protect its assets, technologies are often used to automatically derive a ship’s location over time from a mix of positional data. However, incorrect initial positioning of ships, delayed tracking signals, missing port information, and false alerts in mapping data can mislead operators. Use reliable data sources. Secondly, real operational value requires continuous internet feeds that never stop. Simulated data works well for testing, but operating this system would require reliable links to shipping systems, weather services, port sensors, and cybersecurity monitoring platforms. Operators with no live data can only see half the picture. Third, large numbers of ships, alerts, or map layers may make it difficult for web browsers to display them all at once. Highly busy maritime areas containing thousands of moving bodies may require additional techniques, such as grouping recognizable objects, implementing data caching, or processing on the server side, in order for this system to remain efficient.

In general, our prototype demonstrates how mapping cybersecurity information can create an operationally relevant understanding of maritime cyber defense by transforming technical incidents into

operators' usable intelligence. Cyber alerts, ship movements and infrastructure details can now connect the dots to people in a far clearer way than traditional security dashboards. Our research indicates that future maritime security platforms should include cyber and operational awareness as part of a single monitoring tool rather than in independent modules. This is a big deal for cyber resilience, safety and coordinated response, because it enables you to pinpoint where (in terms of geography on land or sea) cyber incidents are taking place as ships, ports and supply chains go digital.

6. Conclusion and future work

The shipping industry now needs connected digital systems for everything from directing vessels to cargo movement and operating automated ports. While these technologies drive operational efficiency, they also introduce entirely new classes of vulnerability. They can jam GPS, disrupt maritime vessel tracking signals, launch ransomware and denial-of-service attacks, or attack control systems directly to operate equipment in ports. Solutions in maritime security, much like military instruments that connect technical alerts to actions on the water, are prudent because these cyberattacks can result in real world physical consequences. This research developed a method for visualizing maritime cyber threats using an open-source mapping technology (OpenLayers). They offer unique services in a browser-enabled platform combining ship locations, port infrastructure and cyber incidents system. It gives a wider lens for security teams to better align their actions. GPS spoofing, ransomware of port systems and criminals masquerading as ships were among three real-world applications on which the system was tested. These threats were mapped which showed that security teams can easily get a clearer picture of incidents in minutes. In this way, they can decide which was easily the greatest threat and learning more about how would these problems likely spread to nearby boats and terminals.

This research indicates that advanced cyber-maritime monitoring systems can be built at low development cost and without reliance on expensive licensure of proprietary software, using free open-source mapping tools. However, this research also pointed to some of the tough challenges. This system needs highly reliable data, and very responsive execution to operate on a lot of real time updates. The platform must have real-time updates on ship tracking, alerts to possible cyber threats and the ability to convey this information quickly among congested shipping lanes where dozens of vessels may be operating. What comes next should make the platform even more intelligent and informative. The hot spots are to apply Artificial Intelligence (AI) for behavioural anomalies detection, real time data exchange between actual ship and live ship-tracking feeds, risk behaviours development from vessel behaviour. As an outcome towards smart ports, building digital twin of a super smart ports for effective simulation. Finally, scholars should study the systems in connection to Coast Guard missions and autonomous vessels as well as alternative regional maritime protection systems.

Mapping cyber threats is a giant leap for maritime security. As e-commerce drives the digitization of shipping, and as hyperbolic naval ag operations find themselves in need of every possible tool to mitigate threats, coupled with spatial data and cybersecurity analysis in geospatial platforms. This will be required to ensure that safety is kept intact all so that the wheels of global commerce can keep turning.

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

References

1. M. Li, J. Zhou, S. Chattopadhyay, and M. Goh, “Maritime Cybersecurity: A Comprehensive Review,” arXiv preprint arXiv:2409.11417, 2024. doi: 10.48550/arXiv.2409.11417.
2. R. Vaarandi, L. Tsiopoulos, G. Visky, M. U. Rehman, and H. Bahşi, “Literature Review: Cyber Security Monitoring in Maritime,” arXiv preprint arXiv:2503.18173, 2025. doi: 10.48550/arXiv.2503.18173.
3. A. Raymaker, A. Kumar, M. Y. Wong, R. Pickren, A. Chhotaray, F. Li, S. Zonouz, and R. Beyah, “A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners,” arXiv preprint arXiv:2506.15842, 2025. doi: 10.48550/arXiv.2506.15842.

4. 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.
5. T. Miller, I. Durlik, E. Kostecka, S. Sokołowska, P. Kozlovska, and R. Zwolak, “A Systematic Review of AI-Driven Threat Detection and Response in Maritime Cybersecurity,” Electronics, vol. 14, no. 9, p. 1844, 2025. doi: 10.3390/electronics14091844.
6. H. Cho, J. Shin, and B. Choi, “Analysis of Security Vulnerabilities in S-100-Based Maritime Navigation Software,” Sensors, vol. 26, no. 4, p. 1246, 2026. doi: 10.3390/s26041246.
7. A. Nganga, G. Nganya, M. Lützhöft, S. Mallam, and J. Scanlan, “Bridging the Gap: Enhancing Maritime Vessel Cyber Resilience Through Security Operation Centers,” Sensors, vol. 24, no. 1, p. 146, 2024. doi: 10.3390/s24010146.
8. A. Nganga, M. Lützhöft, and J. Scanlan, “Cyber Risk Communication During Vessel Incident Management,” Computers & Security, vol. 145, p. 104607, 2025. doi: 10.1016/j.cose.2024.104607.
9. S. G. A. Rakka and M. R. Hussin, “Maritime Cybersecurity Readiness and Training Standards in Higher Education,” Global Journal of Information Systems and Analytics, vol. 3, no. 1, 2025. doi: 10.57233/gisa.v3i1.930.
10. K. Kanwal, W. Shi, C. Kontovas, Z. Yang, and C. H. Chang, “Maritime Cybersecurity: Are Onboard Systems Ready?” Maritime Policy & Management, vol. 51, no. 3, pp. 484–502, 2024. doi: 10.1080/03088839.2022.2124464.
11. A.-N. Kanellopoulos, “Enhancing Cyber Security and Counterintelligence in the Shipping Industry,” National Security and the Future, vol. 25, no. 1, pp. 137–154, 2024. doi: 10.37458/nstf.25.1.6.
12. A. V. Harish, K. Tam, and K. Jones, “Literature Review of Maritime Cyber Security: The First Decade,” Maritime Technology and Research, vol. 7, no. 2, 2025. doi: 10.33175/mtr.2025.273805.
13. C. Ungureanu and C. Gasparotti, “Assessing Cyber Risks Onboard Ships: A Literature Review,” Annals of Dunărea de Jos University of Galați, vol. 47, pp. 33–40, 2024. doi: 10.35219/AnnUgalShipBuilding/2024.47.04.
14. J. Zhou, “Maritime Cybersecurity: A Big Change Ahead,” IEEE Security & Privacy, vol. 23, no. 4, 2025. doi: 10.1109/MSEC.2025.11163526.
15. B. Kiefer, L. Žust, J. Muhovič, M. Kristan, and J. Perš, “3rd Workshop on Maritime Computer Vision (MaCVi) 2025: Challenge Results,” arXiv preprint arXiv:2501.10343, 2025. doi: 10.48550/arXiv.2501.10343.
16. G. Longo, E. Russo, A. Armando, and A. Merlo, “Attacking (and Defending) the Maritime Radar System,” IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3575–3589, 2024. doi: 10.1109/TIFS.2023.3284195.
17. I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, and S. Nosheen, “Cyber Security Threats in IoT-Enabled Maritime Industry,” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2677–2690, 2024. doi: 10.1109/TITS.2022.3164678.
18. G. Kavallieratos, V. Diamantopoulou, and S. K. Katsikas, “Shipping 4.0: Security Requirements for Cyber-Enabled Ships,” IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6617–6625. doi: 10.1109/TII.2020.2976840.
19. M. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, “Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends,” Information, vol. 13, no. 1, p. 22, 2024. doi: 10.3390/info13010022.
20. F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, “Cybersecurity Challenges in the Maritime Sector,” Network, vol. 2, no. 1, pp. 123–138. doi: 10.3390/network2010009.