

Research Article

Open Access Journal of Applied Science and Technology

Artificial Intelligence in Maritime Shipping: Applications, Risks, and Mitigation Measures

Mariya Tsimbalyuk*

MGIMO University, Master's Student, Faculty of
International Economic Relations, Russia.

***Corresponding Author**

Mariya Tsimbalyuk, MGIMO University, Master's Student, Faculty of
International Economic Relations, Russia.

Submitted: 2026, Aug 04; **Accepted:** 2026, Sep 30; **Published:** 2026, Oct 05

Citation: Tsimbalyuk, M. (2026). Artificial Intelligence in Maritime Shipping: Applications, Risks, and Mitigation Measures. *OA J Applied Sci Technol*, 4(3), 01- 04.

Abstract

This article examines the integration of artificial intelligence into maritime shipping, evaluating both its transformative potential and the associated risks. The author identifies three primary domains of AI application—navigation, vessel condition monitoring, and port infrastructure—and discusses the operational efficiencies these technologies afford, including route optimisation, predictive maintenance, and automated cargo handling. However, the article also highlights significant vulnerabilities, categorising them as operational risks and compliance risks. Mitigation strategies are proposed, encompassing technical redundancy, multilayered security, sensor fusion, and enhanced regulatory collaboration.

Keywords: Artificial Intelligence, Maritime Shipping, Autonomous Vessels, Cyber Risk, Cybersecurity, Navigation, Operational Risk, Compliance Risk

1. Introduction

Artificial Intelligence (AI) is increasingly being adopted within the maritime shipping sector as a means of enhancing operational efficiency, bolstering safety, and reducing operating costs. As world trade expands and environmental concerns intensify, the shipping industry is turning to AI technologies to streamline logistics and lower carbon emissions. The potential applications of AI in this domain are extensive, spanning navigation, condition monitoring of onboard systems and equipment, and cargo management, as well as the coordination of vessel movements in and around ports.

AI is capable of processing large volumes of data collected from ships, port facilities and meteorological sources in order to predict optimal sailing routes, thereby enabling significant savings in both fuel consumption and voyage duration [1]. The rise of autonomous (unmanned) vessels further broadens the scope for AI deployment: such ships, fitted with advanced sensors and navigation systems, offer the prospect of substantially reducing human error, improving navigational safety, and ensuring uninterrupted operational performance. AI-driven condition monitoring can facilitate timely maintenance interventions, thereby lowering the risk of mechanical breakdowns and costly operational stoppages. Moreover, AI-based systems simplify cargo management, increasing the accuracy of loading and unloading operations, reducing the likelihood of

damage, and shortening overall turnaround times. Despite these considerable advantages, however, the integration of AI into shipping is not without its difficulties and associated dangers. It is therefore incumbent upon stakeholders to continue carefully evaluating the benefits of AI against the potential vulnerabilities that its adoption may engender.

The present study comprises an introduction, three chapters and a conclusion. The first chapter sets out the key definitions required for an informed exploration of the topic. The second examines the principal ways in which AI is currently being used in shipping. The third addresses the main risks to which the industry is exposed as a result of AI use, and puts forward a number of suggested mitigation measures.

2. The Definition of Cyber Risk and AI-Related Risk

Before proceeding further, it is necessary to define the concept of AI-related risk as a sub-category of cyber risk, and to assess its present significance within the maritime shipping sector. Cyber risk refers to the threat of financial, reputational and organisational losses arising from incidents affecting an enterprise's IT infrastructure. Such incidents include cyberattacks (system intrusions, data theft, DDoS attacks), cyberfraud (phishing schemes, social engineering), malware infections, IT system failures, and other similar events.

According to research carried out by CyberOwl, a cybersecurity firm specialising in the maritime industry, cyber risk is a particularly pressing concern for the sector. In 2023, the average cost of losses following an attack rose by 200%, to US\$550,000, while the frequency of ransom payments increased by 357%, reaching US\$3.2 million. Twenty-four per cent of cyberattack victims were deceived into making fraudulent transfers to criminal organisations. Notwithstanding these substantial costs, the majority of shipping companies continue to invest far too little in cybersecurity: one in three spends less than US\$100,000 per year [2]. The development of AI has contributed considerably to improving the efficiency of maritime logistics and port operations, as well as to reducing the risks of collision, delays, idle time, demurrage charges, and onboard accidents. At the same time, however, the integration of AI systems into shipping constitutes a new form of cyber risk. Risks associated with AI may be defined as the potential adverse consequences that may arise from the design, deployment and operation of AI systems, with the capacity to cause harm to an enterprise.

3. Applications of AI in Maritime Shipping

In order to identify the most significant AI-related risks facing the shipping industry, it is useful to examine the areas in which the technology is being deployed. The author distinguishes three main spheres of application: navigation, vessel condition monitoring, and port infrastructure.

Autonomous navigation is one of the principal fields in which AI is being actively introduced, with the aim of ensuring the safe movement of unmanned vessels through congested sea lanes and complex navigational channels. According to the European Maritime Safety Agency, between 2014 and 2019 an average of 4,000 collisions and other maritime incidents occurred each year, with the vast majority (up to 96%) attributable to human error. Norway has pioneered the development of autonomous barges, notably the Yara Birkeland, and in April 2022 trials began for the first unmanned container vessel, the ZhiFei, built at the Qingdao shipyard in China. As of 2024, the Russian fleet also includes two autonomous ships: the Marshal Rokossovsky and the General Chernyakhovsky [3].

In addition, AI-based technologies such as computer vision and LiDAR are being used in navigation. Computer vision enables the identification of objects in photographic and video imagery, while LiDAR is a form of echolocation technology that measures distance by detecting reflected light [4]. In 2018, Sea Machines Robotics and the Danish firm AP Moller-Maersk began a joint project to test a system combining computer vision and LiDAR (similar to those used in autonomous road vehicles). The aim was to improve situational awareness at sea, using sensor data to detect and track objects in the vessel's surroundings and to identify potential collision risks. The Japanese shipping company Mitsui OSK Lines (MOL) and the Chinese technology company SenseTime, itself known for its work with Honda on autonomous driving systems, are researching AI-based image recognition for vessel identification [5]. Using ultra-high-resolution cameras and

graphics processing units, the system automatically identifies nearby ships, helping to prevent collisions between large vessels and smaller craft, and potentially also serving as a tool for monitoring maritime traffic. AI is also being incorporated into hydrography to enhance navigational safety. In this context, it contributes to mitigating the risk of extreme weather events. Researchers at the University of Victoria and the Niels Bohr Institute have used AI to analyse 700 years' worth of ocean movement data, developing a mathematical model capable of predicting the emergence of rogue waves—phenomena that can cause catastrophic damage to vessels and offshore installations. Shipping companies may use this model to plan safer routes in advance [6]. AI-based vessel condition monitoring systems are able to assess the operational status of onboard equipment and to send early warnings when maintenance is required, thereby helping to prevent breakdowns and accidents. The Japanese company Furuno Hellas SA has developed the HermAce system, an AI-driven platform that rapidly detects potential defects and irregularities across a range of vessel systems, and transmits the information instantly to experts, even over long distances [7].

Port infrastructure is also being modernised and made more efficient through the adoption of advanced technologies. In Singapore, for example, AI and big data are being used to develop vessel traffic management systems designed to prevent congestion and collisions within the port, as well as to manage traffic in two of the world's busiest waterways, the Singapore and Malacca straits. At Tianjin Port in China, AI combined with 5G and satellite systems has automated crane and truck operations, reducing energy consumption and long-haul driver costs by 20%, while crane productivity has risen to 39 containers per hour [8]. At Qingdao Port, automated loading and unloading systems, together with unmanned suspended systems, have increased container processing speeds to 30 units per hour.

The Port of Rotterdam has developed an AI-driven "digital twin", accessible via mobile devices and laptops, which tracks the real-time movements of ships, containers, inland waterway vessels, trains and trucks. The system analyses meteorological and hydrological data to determine the optimal times for vessel arrivals, reducing port turnaround times by an average of one hour and delivering significant cost savings to operators. Self-learning sensors mounted on buoys, known as "digital dolphins", monitor berth occupancy and port activity, optimising transshipment processes [9]. A similar system, relying on cameras, sensors and detectors, has been operational at the Port of Antwerp since 2021 [10]. This digital twin monitors accidents, perimeter breaches and other events in real time. Its "smart vision" function identifies vehicle types, analyses traffic flows, monitors dock conditions, measures railcar weights, while drones and sensors track water quality. In Russia, the Vladivostok Commercial Sea Port has introduced an automated electronic system that has improved operational efficiency: dockers now use electronic tablets with real-time container movement data and work schedules, replacing traditional radio communications [11].

4. AI-Related Risks and Mitigation Measures

The integration of artificial intelligence into maritime shipping, while offering considerable operational benefits, introduces a range of risks that warrant careful examination. These risks may be broadly divided into two categories: operational risks, which relate to the technical performance and reliability of AI systems, and compliance risks, which concern legal, regulatory and contractual frameworks.

5. Operational Risks

The first and most immediate operational risk is system failure. AI systems, like any complex software, are susceptible to malfunctions arising from programming errors, hardware faults or malicious interference. Should such a failure occur during a critical phase of navigation, the consequences could be severe, particularly in congested or hazardous waters. A related concern is the inherent unpredictability of AI behaviour when confronted with novel or unforeseen circumstances; even well-trained algorithms may respond in ways that are difficult to anticipate, creating additional hazards.

Cybersecurity constitutes a further significant operational risk. Autonomous vessels, by virtue of their reliance on digital systems and remote communications, present attractive targets for cyberattacks. A successful intrusion could result in partial or complete loss of control over the vessel, with potentially catastrophic outcomes for the ship, its cargo and the marine environment. The performance of AI systems in navigation also depends critically on the accuracy of their sensory inputs. Technologies such as computer vision and LiDAR are vulnerable to environmental interference: fog, heavy rain, poor lighting and other atmospheric conditions may degrade their effectiveness, leading to misidentification of objects or failure to detect hazards in time. Such limitations increase the likelihood of collisions and groundings. Prediction inaccuracies represent another operational vulnerability. AI models used for weather forecasting, route optimisation or condition monitoring are only as reliable as the data on which they are trained and the algorithms that process them. Errors in prediction, whether due to flawed models, outdated calibration or incomplete input data, can lead to suboptimal decision-making, with implications for safety, fuel efficiency and schedule reliability.

The dependence of AI systems on stable network connectivity introduces further operational risks. Vessel traffic management, remote monitoring and autonomous navigation all require reliable communication links. Disruptions to internet or satellite connections may impair these functions, resulting in delays,

operational stoppages and, in extreme cases, loss of situational awareness.

Finally, the quality of AI outputs is inherently dependent on the quality of the underlying data. Incomplete, inaccurate, outdated or deliberately corrupted data can significantly compromise the performance of AI systems. This data dependency means that even a well-designed algorithm may produce unreliable results if fed with poor-quality information.

6. Compliance Risks

Beyond operational concerns, the use of AI in shipping gives rise to a number of compliance risks, primarily relating to the adequacy of existing legal and regulatory frameworks.

The most prominent of these is regulatory insufficiency. At present, international rules governing autonomous shipping remain underdeveloped. The International Maritime Organization, for example, is not scheduled to issue its Maritime Autonomous Surface Ships (MASS) Code until 2026, by which time the technology may have advanced considerably, potentially rendering the new regulations outdated even before they take effect [12]. While some nations, including Russia, have moved ahead with domestic legislation, such early efforts are often incomplete and may contain ambiguities or gaps that create legal uncertainty for operators [13].

A further compliance risk concerns liability. In the event of an accident involving an autonomous or AI-assisted vessel, it may be far from clear who bears legal responsibility. The manufacturer of the vessel, the operator, the developer of the AI software, or some combination of these parties could potentially be held liable. The absence of clear legal precedents and established frameworks for allocating responsibility creates significant uncertainty for all stakeholders and may hinder the wider adoption of autonomous technologies.

Taken together, these operational and compliance risks highlight the need for a cautious and well-considered approach to AI integration in maritime shipping, one that addresses both the technical vulnerabilities and the legal ambiguities inherent in the use of emerging technologies. Nevertheless, measures can be taken to address the above risks, as set out in Table 1, that illustrates that successful AI integration in this field depends on a comprehensive strategy that takes into account technical, organisational, legal and ethical considerations. The mitigation measures proposed above may contribute to the reliable and safe operation of AI systems.

Risk	Mitigation Measures
System Failure	• Building in redundancy: employing multiple independent AI systems that operate concurrently, so that if one fails, another can seamlessly take over. • Continuous system monitoring to detect signs of degradation before they lead to failure. • Providing for manual override: ensuring that control can be handed back to human operators when needed. • Rigorous pre-deployment testing: subjecting algorithms to exhaustive trials across a wide spectrum of conditions, including extreme and edge-case scenarios, and making extensive use of simulation to validate system behaviour in complex navigational situations.

Cybersecurity	- Implementing layered defences: building a security architecture that combines hardware-based and software-based protections, so that no single point of failure compromises the whole system. - Ongoing network surveillance to identify and neutralise threats at the earliest possible stage. - Keeping software current: applying patches and updates regularly to close known vulnerabilities as they emerge.
Sensor Limitations	Fusing data from multiple sensor types: combining computer vision, LiDAR and radar to create a more robust perceptual system that is less easily disrupted by fog, rain, poor lighting or other environmental interference.
Prediction Inaccuracies	- Drawing on diverse data sources: incorporating information from satellites, shore-based weather stations and other vessels in the vicinity, so that forecasts are grounded in as broad an evidence base as possible. - Recalibrating predictive models periodically, using fresh data to ensure that they remain accurate as conditions change.
Network Dependency	Maintaining backup communications: ensuring that satellite and radio links are available as fallbacks should primary internet connections fail.
Data Dependency	Enforcing strict data governance: putting in place robust quality-control procedures and relying only on verified, trustworthy data sources, since the reliability of AI outputs is only as good as the data on which they are based.
Liability	- Drafting clear contractual provisions that explicitly allocate responsibility among manufacturers, operators and AI developers in the event of an incident. - Developing specialised insurance products tailored to the unique risks that arise from the use of AI in autonomous shipping.
Regulatory Gaps	Fostering close dialogue between regulators and industry professionals, ensuring that those with technical and operational expertise are actively consulted during the drafting of legislation and rules.

Source: Compiled by the author

Table 1: Mitigation Measures for AI-Related Risks in Maritime Shipping

7. Conclusion

While the adoption of AI in shipping offers substantial advantages, it also gives rise to new cyber risks. Cyber risks in general constitute a serious threat to the industry, entailing significant financial and reputational damage. Although more traditional cyber threats, such as hacking and malware, are already a major concern, the integration of AI introduces further challenges.

AI is being actively deployed in maritime shipping, particularly in navigation, where it enhances safety and efficiency through autonomous control, hazard detection, route optimisation and the forecasting of extreme weather events. AI is also capable of monitoring vessel technical condition and of streamlining port operations.

In short, while AI represents a powerful tool for process optimisation, it simultaneously becomes a potential vector for cyberattacks and carries specific risks that require careful attention. At the same time, current levels of investment in cybersecurity within the shipping industry appear manifestly inadequate, leaving the sector particularly exposed to cyberattacks and the risks associated with AI.

References

1. Law, F. (2023). On Amendments to Certain Legislative Acts of

the Russian Federation. *Sobranie zakonodatel'stva Rossiiskoi Federatsii*.

- 8 Uncomfortable Questions About the Law on Autonomous Ships. *Morskije Vesti*.
- "A Digital Twin for the Port of Rotterdam by Esri." Ditto.
- "AI Finds Formula for How to Predict Monster Waves." University of Victoria.
- "HermAce." *Furuno*.
- "How AI Poses Threats to the Maritime Industry." *Sea and Beyond*.
- "Maersk Selects Sea Machines for World's First AI-Powered Situational Awareness System Aboard A Container Ship." *Sea Machines*.
- "Maritime Cyber Risk Report: Shipping Industry Remains 'Easy Target', Pays Average US\$3.2m In Cyberattacks." *CyberOwl*.
- "MOL Introduces AI-Powered Vessel Image Recognition System." *Ship Technology*.
- "Report of the MSC MASS Correspondence Group." *International Maritime Organization*.
- "Smart Port." *Port of Antwerp-Bruges*.
- "Tianjin 5G Smart Container Port – Automated Trucks." *Huawei*.
- "Vladivostok Commercial Sea Port Adopts a Digital Twin: How It Works." *WWW1*.

Copyright: ©2026 Mariya Tsimbalyuk. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.