

Revista Sextante

ISSN : 2665-3923

Vol: 32 No: 01 (2025)

Artificial Intelligence in Maritime Surveillance: Opportunities and Challenges for Naval Security

Priya Narayanan-Brandt

Centre for Maritime Security and Intelligent Systems, Oslo, Norway

Article History

Received June, 08th, 2025

Accepted June, 09th, 2025

Published June, 10th, 2025



© 2025 The Authors. This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution(CC-BY)license

<https://creativecommons.org/licenses/by/4.0>

Abstract

Maritime surveillance underpins naval security by enabling the detection and understanding of activity across vast and often contested ocean areas, yet the volume and variety of sensor data now exceed what human analysts can process. This article examines the opportunities and challenges of artificial intelligence in maritime surveillance for naval security. Drawing on research in machine learning, anomaly detection, data fusion, human factors and security studies, it analyses data sources, detection and tracking methods, threat assessment, human-machine teaming, strategic implications and governance. The analysis indicates that AI can extend coverage, accelerate detection and reduce operator workload when it is integrated with diverse sensors, tested under realistic conditions and used as decision support under meaningful human oversight. Challenges include data scarcity, brittleness, adversarial manipulation, miscalibrated trust, legal uncertainty and ethical risk. An illustrative figure summarises expected capability profiles under conventional and AI-assisted surveillance.

Keywords: artificial intelligence, maritime surveillance, naval security, anomaly detection, human-machine teaming

INTRODUCTION

The oceans cover most of the planet's surface and carry the great majority of global trade, and they are also arenas of illegal fishing, smuggling, piracy, trafficking, territorial disputes and strategic competition. Naval forces and maritime security agencies are responsible for monitoring vast areas with limited ships, aircraft and personnel, and they must detect and interpret activity at sea with enough speed and accuracy to support decisions. Maritime surveillance is therefore a foundation of naval security, enabling the protection of sea lines of communication, offshore resources, ports and territorial waters (Till, 2013). The volume and variety of maritime data have grown dramatically. Satellite imagery, coastal and shipborne radar, automatic identification systems, electro-optical and infrared sensors, acoustic arrays, aerial and underwater drones and open-source information generate streams of data that no human team can analyse in full. Artificial intelligence, and machine learning in particular, offers means of processing these data at scale,

detecting patterns, classifying objects and highlighting situations that deserve attention (LeCun et al., 2015). Naval organisations around the world are therefore investing in AI-enabled surveillance as part of broader modernisation efforts. This article examines the opportunities and challenges of artificial intelligence in maritime surveillance for naval security. It reviews the conceptual foundations of the technology, the requirements of maritime domain awareness, the data and methods used, and the operational benefits that can be expected. It also analyses technical vulnerabilities, human factors, and ethical, legal and governance questions. The analysis is conceptual and integrative, and the figure presented is an illustrative synthesis rather than a report of new empirical data.

Conceptual Foundations of Artificial Intelligence in Maritime Surveillance:

Artificial intelligence is the field concerned with building systems that perceive their environment and take actions that maximise their chances of achieving defined goals (Russell & Norvig, 2021). In surveillance, the most relevant branches are machine learning, computer vision, pattern recognition, probabilistic reasoning and data fusion. Machine learning allows systems to improve their performance by learning from data rather than following only explicit rules written by programmers, which is valuable in environments where the range of possible situations is too large to specify in advance. Deep learning, a class of methods based on multi-layer neural networks, has transformed tasks such as image recognition, speech processing and sequence analysis by learning useful representations directly from raw data (LeCun et al., 2015; Goodfellow et al., 2016). These advances are directly relevant to maritime surveillance, where images from satellites and aircraft, radar returns and acoustic signals must be converted into meaningful information about vessels and their behaviour. Methods for time-series and trajectory analysis also enable the modelling of vessel movement over days or weeks. It is helpful to distinguish between automation, which executes defined tasks, and autonomy, which involves systems that make decisions with limited human intervention. In maritime surveillance, most current applications are decision-support systems that process data and offer alerts, rankings or recommendations to human operators, rather than fully autonomous systems. This distinction is critical for discussions of responsibility, trust and risk, since the appropriate degree of human involvement varies with the consequences of error and with the legal and ethical context.

Maritime Domain Awareness and Naval Security Requirements:

Maritime domain awareness refers to the effective understanding of anything associated with the maritime domain that could affect security, safety, the economy or the environment. It involves collecting, fusing and analysing information about vessels, cargo, people, infrastructure and activities, and sharing it among the organisations that need it. For navies, domain awareness supports tasks such as protection of the exclusive economic zone, counter-piracy and counter-smuggling operations, anti-submarine warfare, mine countermeasures, force protection and the enforcement of sanctions. The requirements are demanding. Surveillance must cover very large areas, including remote and contested waters, over long periods, in all weather and at all hours. It must detect small and deliberately concealed targets such as small boats or vessels that turn off their transponders, and it must distinguish hostile or illicit behaviour from the ordinary activity of tens of thousands of commercial and fishing vessels. It must also be timely, since information that arrives too late has little operational value, and it must be reliable enough to support decisions with serious consequences. These requirements explain the attraction of artificial intelligence. Human operators are limited in attention, can become fatigued, and cannot monitor all sensor feeds simultaneously, whereas algorithms can process continuous data streams without tiring and can cue operators to the most relevant information. At the same time, naval requirements impose strict demands on security, robustness and accountability that exceed those of many civilian applications, which shapes how AI must be designed, tested and employed.

Data Sources and Sensor Integration:

Maritime surveillance draws on many data sources, each with strengths and weaknesses. Automatic identification system data provide identity, position, course and speed for cooperative vessels and are available in large volumes, but they can be switched off, spoofed or misreported. Radar offers all-weather detection of non-cooperative targets but suffers from clutter and limited range. Satellite synthetic aperture radar and optical imagery provide wide-area coverage and can detect vessels that do not broadcast, although revisit times and cloud cover constrain their use. Acoustic and electronic sensors add further information, particularly for subsurface and signal-related activity. Data fusion, the combination of information from multiple sources to produce a more accurate and complete picture than any single source can provide, is among the most important applications of AI. Algorithms can associate observations from different sensors with the same vessel, resolve conflicts, fill gaps and estimate uncertainty. Fusion also allows cross-checking, for instance by comparing a vessel's declared identity with its radar signature or satellite image, which helps to reveal deception and improves confidence in the resulting picture. The quality, labelling and sharing of data are critical constraints. Machine learning requires large volumes of representative, accurately labelled data, and in the maritime domain examples of rare and hostile events are scarce while sensitive data are often classified or restricted. Differences in formats, standards and security rules among agencies and allies complicate integration. Investment in

data infrastructure, common standards, synthetic data generation and secure sharing arrangements is therefore as important as investment in algorithms themselves.

Machine Learning Techniques for Detection, Classification and Tracking:

Computer vision methods based on deep neural networks are widely used to detect and classify vessels in satellite, aerial and shipborne imagery. They can identify ship types, estimate size, recognise features and detect changes over time with an accuracy that often rivals or exceeds that of manual analysis, while operating at far greater speed. In radar and sonar, learning-based methods can help to separate targets from clutter, reduce false detections and classify objects based on their signatures. Tracking and prediction rely on probabilistic and learning-based models of vessel motion. By learning typical routes and behaviours from historical data, systems can predict where a vessel is likely to go, estimate its destination, and recover tracks after gaps in coverage. Studies of vessel pattern discovery from identification data have shown how large archives of movements can be used to build models of normal traffic and to extract routes and behavioural patterns that support route prediction and anomaly detection (Pallotta et al., 2013). Several learning paradigms are relevant. Supervised learning requires labelled examples and works well for well-defined classification tasks, unsupervised learning discovers structure without labels and is useful for identifying unusual behaviour, and reinforcement learning may support planning and sensor management, such as the allocation of limited patrol assets or satellite tasking. Combining these methods in integrated pipelines, with careful evaluation on realistic data, allows surveillance systems to progress from raw sensor data to actionable information.

Anomaly Detection and Maritime Threat Assessment:

One of the most promising uses of AI is the detection of anomalies, meaning deviations from normal patterns of maritime behaviour that may indicate illegal or hostile activity. Such deviations include unexpected changes of course, loitering in unusual areas, rendezvous between vessels at sea, deviations from established routes, gaps in transponder transmissions and mismatches between a vessel's declared identity and its observed behaviour. A comprehensive review of the field describes a range of statistical, machine learning and knowledge-based techniques and emphasises the importance of context and of operator involvement in interpreting results (Riveiro et al., 2018). Threat assessment goes beyond detection by judging the intent and potential impact of observed activity. Models can combine behavioural indicators with information on vessel ownership, history, cargo and the geopolitical setting to rank vessels according to risk, enabling operators to focus limited resources on the most significant concerns. Such assessment is, however, intrinsically uncertain, since behaviour that appears suspicious may have innocent explanations such as mechanical failure, weather avoidance or legitimate fishing practice. The balance between sensitivity and false alarms is a central design problem. A system tuned to detect every possible threat will generate many false alerts, overloading operators and eroding trust, while a system tuned to avoid false alarms may miss genuine threats. Good practice includes presenting alerts with confidence levels and supporting evidence, allowing operators to adjust thresholds according to the mission, and continuously evaluating performance on real operations. Anomaly detection is best viewed as a means of directing human attention rather than as a final judgement.

Decision Support, Human-Machine Teaming and Situation Awareness:

The ultimate purpose of surveillance is to support decisions, and the effect of AI therefore depends on how well it fits into human decision processes. Situation awareness, which involves perceiving the elements of the environment, understanding their meaning and projecting their future status, is the foundation of good decisions in dynamic settings (Endsley, 1995). AI can contribute at each level by detecting objects, highlighting relationships and predicting movements, but it can also degrade awareness if operators become passive, lose understanding of how the system works or fail to notice its errors. Research on automation has long documented the problems of misuse and disuse, in which operators rely too heavily on automated systems when they are unreliable or reject them when they are in fact reliable, as well as the problem of abuse, where automation is designed without sufficient regard to human capability (Parasuraman & Riley, 1997). These lessons apply directly to AI-enabled surveillance. Appropriate trust must be calibrated through transparency about system capabilities and limits, training that exposes operators to system failures, and interface design that makes the reasoning and uncertainty of the system visible. Human-machine teaming offers a constructive framework. In such arrangements, machines handle large-scale data processing, routine monitoring and pattern detection, while humans provide contextual understanding, judgement, creativity and accountability. Explainability is an important enabler, because operators are more able to verify and challenge recommendations that come with understandable reasons (Doshi-Velez & Kim, 2017). Naval organisations should therefore treat doctrine, training and interface design as integral parts of AI adoption, rather than as afterthoughts to technical development.

Operational Opportunities and Strategic Implications:

The opportunities offered by AI in maritime surveillance are substantial. Systems can extend the coverage of limited assets by cueing ships and aircraft to the areas of greatest interest, shorten the time between detection and response, reduce the burden on operators of routine monitoring and improve the consistency of analysis. They can also support efficient use of expensive platforms, enhance the protection of ports and offshore infrastructure and strengthen

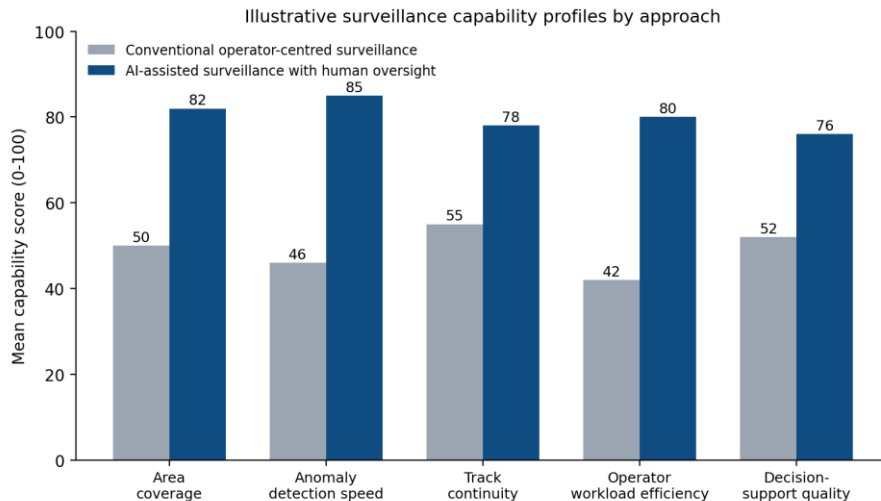
cooperation by enabling shared, interoperable pictures among allied navies, coast guards and civilian agencies. Strategically, AI is part of a wider shift in military competition. States that integrate AI effectively may gain advantages in speed of decision, quality of information and efficiency of operations, which has implications for the balance of power and for deterrence (Horowitz, 2018). At the same time, the diffusion of commercial AI tools and satellite data to smaller states and non-state actors may reduce the information advantage of traditional naval powers, since open-source analysis can reveal activity that was once visible only to a few.

Technical Vulnerabilities and Reliability Challenges:

AI systems have technical weaknesses that are especially significant in a security context. Models trained on one set of conditions may perform poorly when conditions change, for example in a different sea state, a new region or against a vessel type absent from the training data. Rare events are poorly represented in data, so that systems may fail on exactly the cases that matter most. Errors may also be difficult to predict or detect, because neural networks can make confident mistakes without any obvious warning. Adversarial threats add a further dimension. Research has shown that small, deliberately crafted perturbations of inputs can cause neural networks to misclassify objects with high confidence (Goodfellow et al., 2015). In a naval setting, adversaries may attempt to deceive sensors and algorithms through spoofing of transponder data, camouflage, decoys, manipulation of imagery or poisoning of training data, and cyber attacks may target data links and software. Defences require robust model design, adversarial testing, secure data pipelines, redundancy across independent sensors and the ability to revert to manual procedures. Reliability also depends on engineering and operational factors. Naval platforms may have limited computing power, bandwidth and connectivity, particularly at sea, so that edge processing and efficient models are often necessary. Systems must be tested and certified under realistic conditions, monitored for performance drift and updated in a controlled manner. Without disciplined testing, evaluation and lifecycle management, enthusiasm for AI risks producing systems that appear impressive in laboratories but prove brittle in operations.

Ethical, Legal and Governance Challenges, and Future Directions:

Ethical and legal questions accompany the use of AI in naval security. Surveillance of vessels and coastal areas raises issues of privacy, proportionality and the protection of lawful commercial and fishing activity, and algorithmic bias may lead to certain vessels, flags or communities being unfairly targeted. Accountability must remain clear, so that identifiable people retain responsibility for decisions based on AI recommendations. Debates on autonomy in weapons highlight the importance of meaningful human control over decisions involving the use of force (Scharre, 2018). The legal framework for maritime operations, including the law of the sea, the law of armed conflict and national legislation, applies to AI-enabled activities, but its application to new technologies can be uncertain. Questions arise about the legality of interdiction based on algorithmic suspicion, the sharing of data across jurisdictions and the responsibility for errors. Governance responses include national and organisational policies on responsible AI, standards for testing and documentation, independent review, international dialogue on norms and confidence-building measures among navies. Future directions are likely to include more capable multi-sensor fusion, the use of foundation models and generative methods for analysis and synthetic training data, greater use of autonomous surface and underwater vehicles as sensor platforms, and distributed processing at the edge. Research priorities include robustness, explainability, uncertainty quantification, human-machine teaming and the evaluation of operational impact. Naval institutions should invest in people as well as technology, developing personnel who understand both maritime operations and data science, and should pursue cooperation with allies and academia to share data, methods and good practice.



Summary:

Artificial intelligence offers significant opportunities for maritime surveillance and naval security. By fusing data from satellites, radar, identification systems and other sensors, detecting and classifying vessels, predicting movements and flagging anomalous behaviour, AI can extend the reach of limited assets, shorten the time to detection and reduce the burden of routine monitoring on operators. Its greatest value arises when it is designed as decision support within a human-machine team, with transparent outputs, calibrated trust and clear accountability. These opportunities are accompanied by serious challenges. Data scarcity, sensitivity to changing conditions, adversarial manipulation, high false-alarm rates, legal uncertainty and ethical concerns about privacy, bias and human control can undermine performance and legitimacy. Naval organisations should therefore combine technical investment with realistic testing, secure data infrastructure, doctrine and training, responsible AI governance and international cooperation. Future research should focus on robustness, explainability, human-machine teaming and the measurement of operational impact.

References:

- Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*.
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32–64.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *International Conference on Learning Representations*.
- Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36–57.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521, 436–444.
- Pallotta, G., Vespe, M., & Bryan, K. (2013). Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction. *Entropy*, 15(6), 2218–2245.
- Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), 230–253.
- Riveiro, M., Pallotta, G., & Vespe, M. (2018). Maritime anomaly detection: A review. *WIREs Data Mining and Knowledge Discovery*, 8(5), e1266.
- Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton.
- Till, G. (2013). *Seapower: A guide for the twenty-first century* (3rd ed.). Routledge.