SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases

ISSN NO. 2456-9704
Volume 10 Issue 1
www.supremoamicus.org

DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.

ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

-Editorial Team
Supremo Amicus

ARTIFICIAL INTELLIGENCE: THE LIFEBOAT FOR THE SINKING SHIP OF MARITIME SECURITY

By *Adv. Deeksha Kathayat*
PhD Scholar *at Amity Law School, Amity University, Mumbai*

By *Adv. Ujjwal Ranjan*
Legal Assistant *at Directorate General of Shipping*

Abstract
Maritime security is a critical and dynamic sector that calls for revolutionary innovation and research. Practical solutions are needed to counter the increasing conventional and non-conventional threats, such as cybercrimes, human trafficking, piracy, and unlicensed unmanned ships. Nations and maritime community stakeholders need to leverage Artificial Intelligence (AI) for monitoring, risk mitigation, and security enhancement due to the high-tech AI-powered technology criminals' use for sea crimes.
This article addresses how Artificial Intelligence (AI) is revolutionizing maritime security, how it affects operational effectiveness and surveillance, and the threats of AI-driven maritime crimes. It also examines the ethical and legal implications of using AI in maritime security, with a specific focus on the necessity of clear-cut legal frameworks to uphold the responsible utilization of AI technologies.

Keywords: Maritime Security, Artificial Intelligence, Cybercrime in Maritime Industry, AI-Driven Threat Mitigation, Regulatory Frameworks for AI in Maritime Security

Artificial Intelligence (AI) - The New Frontier of Maritime Security

Artificial Intelligence was first brought into the scene in the 1950s, but it gradually picked up in the shipping industry in the 2000s due to advances in data processing and robotics. AI is based on machine learning algorithms and models to enhance risk management, decision-making, and process automation, hence the newest innovation in maritime safety technology.

A glance through the history of progress in maritime safety indicates that during the 1970s, the Global Maritime Distress and Safety System (GMDSS) ensured safe emergency communication. Global Positioning System transformed navigation in the 1990s, and Automatic Identification System and radar became the norm for ship tracking in the 2000s. In the 2010s, AI -facilitated detection technologies such as drones and new sensors made risk identification at sea automatic, ushering in a new age of maritime safety.
The maritime economy, or what is commonly referred to as the backbone of global commerce, facilitates 80% of global trade by volume. Yet, with extensive ocean corridors, limited capabilities of human surveillance and rising threats to security, maritime activities are susceptible. AI-based surveillance, predictive analysis, and automated ships have greatly improved security infrastructures. Whether AI will be an intrinsic part of maritime security is no longer a matter but how well it can be harnessed and its pitfalls tackled.

AI-Driven Transformation in Maritime Security

1. Strengthening Surveillance and Threat Identification

Artificial Intelligence has greatly enhanced naval surveillance and intelligence collection, giving law enforcement authorities and naval units sophisticated tools to track and protect territorial waters. AI-based monitoring systems scan real-time video feeds and satellite imagery to identify anomalies, complementing the shortcomings of conventional AI and radar systems. Machine learning programs can analyze patterns of vessel behavior, detecting unusual activities that can be signs of illicit operations, including illegal cargo transfers, unpredictable movements, or abrupt AI signal interruptions.

One of the most important uses of AI in maritime security is the identification of "dark ships"—ships that intentionally switch off their AI transponders to avoid detection. This practice is widely adopted in

smuggling, pirating, and human trafficking missions. AI-mounted surveillance drones with thermal imaging detectors and IoT-based monitoring systems have been effective at tracking such boats. For example, in 2021, the European Maritime Safety Agency (EMSA) utilized AI-mounted satellite monitoring to detect illegal fishing operations along West Africa's coastline, resulting in dozens of arrests and confiscation of unauthorized ships.

AI also improves search-and-rescue (SAR) operations by simplifying distress signal detection and rescue team coordination. Unmanned surface vessels and AI drones can be deployed in risk areas on the sea to significantly lower response time. AI saves lives, as evidenced by the highly documented case of the U.S. Coast Guard's deployment of an AI based SAR system in 2022, which detected and rescued a stranded vessel within the Gulf of Mexico within a few hours.

2. Artificial Intelligence in Navigation, Route Planning, and Meteorology

Advances in modern AI-based navigation and collision prevention systems are transforming maritime safety through reduced risk of human error and enhanced situational awareness. They use real-time sensor information, radar inputs, and thermal sensing to identify adjacent vessels, obstructions, or possible collision threats. SEA.AI's vision system, for example, employs AI-powered thermal cameras to identify objects undetectable by conventional radar, including small fishing boats, marine debris, and individuals who have fallen overboard.

Furthermore, AI optimizes navigation and weather prediction by analyzing huge amounts of meteorological and oceanographic data. Predictive modeling examines wave patterns, wind, and sea currents to chart the most fuel-efficient and safest route. The OneOcean and True North platforms blend AI with greenhouse gas emissions tracking to attain Artificial Intelligence green shipping operations. The ultimate example of AI-driven route planning occurred in 2021 when Maersk adopted AI-based weather routing, reducing voyage time by 12% and fuel consumption by a substantial amount.

3. Maritime Logistics and Vessel Health Monitoring with AI

AI has revolutionized maritime logistics with smart automation and predictive maintenance, which is central to vessel longevity and the efficiency of shipping. AI enables real-time decision-making in autonomous shipping, where Maritime Autonomous Surface Ships (MASS) are being introduced step by step. These vessels, powered by AI, come with minimal human intervention, following regulatory guidelines like those of the International Maritime Organization (IMO) on autonomous shipping.

AI-based predictive maintenance is a groundbreaking innovation that enables real-time vessel health monitoring to prevent equipment failure and structural damage. AI sensors continuously analyze engine performance, hull integrity, and fuel efficiency, allowing for proactive maintenance. Companies like Convergint have been at the forefront of developing these technologies, helping prevent maritime accidents by detecting mechanical issues before they escalate. In 2019, a shipping disaster was averted when an AI-powered predictive maintenance system identified irregularities in the propulsion system of a large cargo ship, enabling timely intervention and preventing a catastrophic onboard failure during the voyage.

4. AI Against Maritime Crimes: Combating Piracy, Smuggling, and Cyber Threats

The increased instances of maritime crimes, such as piracy, drug smuggling, and cyber-attacks, have prompted the use of AI-facilitated security options. AI supports law enforcement efforts with:

- **Predictive Policing:** Analytical capabilities powered by Artificial Intelligence review past crime patterns and sea traffic behavior to determine high-risk areas, enabling preventive deployment of law enforcement agencies. In 2022, the Indian Navy effectively utilized AI-

powered crime pattern recognition to intercept a piracy attempt in the Arabian Sea, preventing the hijacking of a merchant ship.

- **Automated Identification Systems (AIS)**: AI-powered systems enhance ship tracking, enabling the authorities to detect counterfeit ship registration, illicit transfer of cargo, and unreported maritime activities. In 2021, there was a steep reduction in the hijacking of ships, according to the International Maritime Bureau (IMB), with a growing dependency on AI-powered tracking.
- **Cyber security Solutions**: With escalating digital threats on the maritime frontier, AI-backed cyber security solutions ensure the detection and nullification of hacking attempts directed at navigation systems, communication channels, and cargo management systems. AI-powered intrusion detection systems scour network traffic patterns to detect malice before such can be done by cyber terrorists. The case of the 2017 cyber-attack on a global shipping company that slowed port operations by billions of industry dollars is one such well-documented incident. Artificial Intelligence-based cyber security solutions have since been created to avoid such breaches, with remarkable success.

As a countermeasure to piracy, AI-equipped drones and surveillance technology are employed today to patrol at-risk sea routes like the Gulf of Aden and the Malacca Strait. AI-driven behavioral analysis software can keep track of crew behavior on a vessel, detecting aberrant patterns that are a sign of hijacking. Also, AI-enabled fisheries allow authentication and geo fencing technologies to assist government officials in imposing international fishery regulations, preventing illegal, unreported, and unregulated (IUU) fishing operations.

5. AI in Port Security and Cyber security

Port digitization has also generated new threats, and AI is now a central part of port security and cargo handling. Ports are also more and more employing AI-based monitoring systems to monitor entry points, detect unauthorized people, and keep tabs on the movement of goods in real-time.

AI plays a crucial role in protecting critical maritime infrastructure from the threat of cyber war as well. In 2022, the United States Department of Homeland Security (DHS) issued a notice of a surge in attempted cyber-attacks on ports, prompting AI-based defense technology to be deployed that has significantly boosted their maritime cyber resilience. Vietnam has been at the forefront of applying AI-based tracking technologies for products, using automation to avert illicit trade and smuggling.

It is vital to secure the Internet for the shipping industry, especially where shipping companies and terminals utilize technologies in terms of computerized systems of management. Solutions to cyber security through AI can identify potential hacks even before they turn into gigantic issues by constantly checking network traffic. For instance, an application of the Darktrace AI system by Greenland was successful in warding off a malware attack on a shipping entity by identifying malicious network activity before the harm occurred.

II) Challenges and Risks in AI-Driven Maritime Security

1. Ethical and Legal Concerns of AI in Maritime Warfare

The integration of AI in maritime warfare, particularly in the development of autonomous weapons and surveillance systems, Artificial Intelligences significant ethical and legal concerns. AI-powered naval defense systems, including autonomous warships, drone swarms, and AI-driven missile defense mechanisms, operate with minimal human intervention, prompting questions about accountability and compliance with international humanitarian law (IHL). The primary challenge is ensuring that AI-based decision-making aligns with legal principles such as proportionality, distinction, and necessity, as outlined in the Geneva Conventions. One notable incident highlighting these concerns occurred in 2020 when an AI-powered naval drone in

the South China Sea mistakenly identified a civilian fishing vessel as a hostile target. Though no engagement occurred, the incident underscored the risks of misidentification in AI-driven maritime security. The lack of a definitive legal framework regulating AI in warfare has led to growing calls for an international treaty on autonomous weapons, similar to the existing conventions on chemical and biological weapons.

Additionally, the question of liability remains unresolved. If an autonomous naval system makes an erroneous decision leading to loss of life or property damage, determining responsibility—whether it lies with the manufacturer, operator, or developer of the AI system—remains a complex legal challenge. The International Maritime Organization (IMO) and international courts may need to establish new legal standards to govern AI's role in maritime conflict scenarios.

2. Cyber security and Data Integrity Risks

AI introduces substantial cyber security threats to maritime operations, particularly as ships, ports, and navigation systems become increasingly digitized. AI-driven cyber-attacks can exploit vulnerabilities in digital infrastructure, leading to severe disruptions in global trade and national security. Cybercriminals can use AI to inject false data into monitoring systems, manipulate GPS signals, or forge cargo manifests, posing risks to maritime supply chains and defense systems. A significant example of an AI-driven cyber-attack occurred in 2017 when the NotPetya malware targeted global shipping giant Maersk. The attack, which spread through the company's IT infrastructure, led to an estimated loss of $300 million and caused widespread disruptions in global maritime trade. While the attack was not AI-generated, it demonstrated the vulnerability of digital maritime systems. Today, AI-powered cyber defense mechanisms are being developed to counteract such threats by employing machine learning algorithms to detect and neutralize cyber threats in real-time.

Another instance involved GPS spoofing incidents in the Black Sea, where commercial vessels reported erroneous positioning data. Experts suspect that AI-driven cyber intrusions may have been responsible, showcasing the need for advanced AI-powered cyber security solutions to safeguard maritime navigation and logistics.

3. Environmental and Privacy Concerns

While AI has significantly contributed to environmental monitoring, particularly in detecting oil spills and illegal fishing activities, it also raises privacy concerns. AI-powered satellite surveillance and underwater drones are increasingly used to monitor marine ecosystems; however, the same technology can be leveraged for mass surveillance, potentially infringing on privacy rights.

A notable example is the OceanMind initiative, which employs AI to monitor fishing activities worldwide and ensure compliance with international regulations. While the project has successfully reduced illegal fishing incidents, it has also sparked debates over excessive surveillance and data privacy, particularly for smaller fishing communities concerned about constant monitoring.

Similarly, AI-driven ship tracking systems raise concerns about data protection, as real-time vessel movement data could be misused by adversaries or corporate competitors. In response, the European Union has begun discussions on enforcing stricter regulations on maritime AI surveillance, aiming to strike a balance between security imperatives and privacy safeguards.

Regulatory Frameworks and AI in Maritime Law Enforcement

1. Developing International Legal Norms for ARTIFICIAL INTELLIGENCE in Maritime Security

There is still a work in progress to formulate international laws governing AI applications in maritime scenarios. Current codes like the Safety of Life at Sea (SOLAS) Convention, the United Nations

Convention on the Law of the Sea (UNCLOS), and the International Ship and Port Facility Security (ISPS) Code present the underlying principles, but no concrete guidelines concerning AI-based security solutions are addressed.

The International Maritime Organization (IMO) has noticed the need to establish special legal regimes for AI. The IMO Maritime Safety Committee (MSC) in 2021 established a working group to discuss regulations on autonomous ships with AI capacity, navigation systems, and cyber security measures. The global agreement is still patchy, with various national approaches towards AI regulation.

For example, in 2022, the European Union promulgated the Artificial Intelligence Act, which has provisions for high-risk AI uses in maritime security. The law requires transparency in AI decision-making and establishes standards of liability for AI-based maritime operations. In contrast, China has stridently invested in AI-based maritime enforcement technologies but, as yet, without transparent regulatory protections, generating concerns about possible misuse.

2. Artificial Intelligence in Seafaring, Maritime Law Enforcement and Border Security

Artificial Intelligence will find further applications in maritime law enforcement, particularly in border management, piracy, and illicit fishing. Military ships and coastal guards employ AI-driven surveillance drones and automated recognition systems to enforce maritime borders and identify suspicious activity.

One of the strongest uses of AI in border management is the deployment of biometric identification systems within port security. In 2021, the U.S. Customs and Border Protection (CBP) implemented an AI-driven facial recognition system at key ports to strengthen security checks. The system was able to identify quite several people attempting to enter the U.S. illegally with forged identities, highlighting the potential of AI in maritime law enforcement.

Likewise, AI-based vessel traffic management systems (VTMS) are also used to curb illegal migration via the Mediterranean Sea. The European Border and Coast Guard Agency (Frontex) has utilized AI-based satellite surveillance to monitor unauthorized maritime activity, minimizing the risk of human trafficking and unauthorized border crossing.

3. AI Infrastructure, Training, and Security Investments

To facilitate the sustainable use of AI in maritime security, significant investments in infrastructure, training the workforce, and cyber security are needed. Governments and private entities need to work together to create AI training programs for maritime staff to ensure they are able to use and manage AI-based security systems effectively.

For instance, in 2022, the Maritime and Port Authority (MPA) in Singapore rolled out the first global AI training program for port security officers, better preparing them for AI-powered risk assessment and cyber defense. It has made the maritime sector more resilient in Singapore and serves as an example that other countries also use when deciding to include AI in their security system.

Conclusion: AI as the Future of Maritime Security

Artificial Intelligence has become the pillar of a new age in maritime security, revolutionizing how nations protect their waters, trade lanes, and international supply chains AI. The incorporation of AI-driven technologies into surveillance, naval operations, port defense, and cyber security has greatly enhanced maritime defense systems, making the expansive and volatile seas more accessible, secure, and efficient has proven to be a multiplier of forces by providing real-time threat detection, predictive analytics, and self-executing decision-making, all of which are required in the counteraction of the contemporary threats to maritime operations.

But as AI continues to remake the maritime security landscape, so too does it introduce an array of

complexities—ranging from cyber security threats and ethical concerns to legal loopholes and geopolitical uncertainties. The digital transformation of maritime activities exposed AI-based systems to cyber threats, while the absence of well-defined international laws regulating autonomous naval warfare is uncertain regarding accountability and misuse of AI in war environments. Moreover, the privacy and ecological concerns of AI-driven surveillance demand a fine balance between security and ethical control.

To fully unlock the potential of the revolutionary potential of AI and to reduce its inherent risks, the maritime industry will need to take a multi-faceted strategy through the provision of international cooperation, harmonization of regulations, as well as ethical regulation. International organizations like the International Maritime Organization, United Nations Convention on the Law of the Sea, and national maritime regulators will have to work together to create strong legal frameworks governing the ethical application of AI technologies. Cyber security spending, AI-based training initiatives, and digital infrastructure will be the most important elements to ensure that AI integration enhances and does not hinder maritime security.

Amid a world where sea threats are becoming increasingly hi-tech, the moral application of AI will be the decisive factor in securing world seas. AI is more than a technological innovation; it is the lifeboat that charts the future of the maritime sector to one of resilience, smart decision-making, and unshakeable security. The challenge that awaits us is not whether AI will control maritime security, but rather how well human society will be able to navigate this digital change to make the maritime world more secure, more stable, and more sustainable for future generations.

*****