MEUJMAF

Mersin University Journal of Maritime Faculty

e-ISSN 2687-6612

June 2024 Volume: 6 Issue: 1

PUBLISHING BOARD

Prof.Dr. Özcan ARSLAN
Istanbul Technical University, Faculty of Maritime
Türkiye

Prof.Dr. Serpil EROL
Gazi University, Faculty of Engineering
Türkiye

Prof.Dr. Nur Jale ECE
Mersin University, Faculty of Maritime
Türkiye

MERSİN UNIVERSITY JOURNAL OF MARITIME FACULTY (MEUJMAF)

Mersin University Journal of Maritime Faculty (MEUJMAF) is an international, scientific, and multidisciplinary journal which covers all fields of maritime sector. MEUJMAF publishes the articles in English and is being published 2 times a year. The Journal involves both experimental and theoretical studies on the subject area of Maritime Business Administration, Marine Transportation Engineering, Logistics, Supply Chain Management, Logistics Engineering, Naval Architecture Engineering, Marine Operations, Operations Research, Foreign Trade, Maritime Economics, Maritime History, International Trade, Marine Pollution and Port Management. MEUJMAF aims to contribute to the literature by publishing manuscripts at the highest scientific level in each abovementioned field and to convey the latest development in the science and technology to the related scientists and the readers.

AIM AND SOPE

Mersin University Journal of Maritime Faculty (MEUJMAF) is an international blind peer-reviewed open access journal, published twice a year. The Journal covers all fields of Maritime Business Administration, Marine Transportation Engineering, Logistics, Supply Chain Management, Logistics Engineering, Naval Architecture Engineering, Marine Operations, Operations Research, Foreign Trade, Maritime Economics, Maritime History, International Trade, Marine Pollution and Port Management.

PEER REVIEW PROCESS

All submissions will be scanned by iThenticate® to prevent plagiarism. Author(s) of the present study and the article about the ethical responsibilities that fit PUBLICATION ETHICS agree. Each author is responsible for the content of the article. Articles submitted for publication are priorly controlled via iThenticate® (Professional Plagiarism Prevention) program. If articles that are controlled by iThenticate® program identified as plagiarism or self-plagiarism with more than 25% manuscript will return to the author for appropriate citation and correction. All submitted manuscripts are read by the editorial staff. To save time for authors and peer-reviewers, only those papers that seem most likely to meet our editorial criteria are sent for formal review. Reviewer selection is critical to the publication process, and we base our choice on many factors, including expertise, reputation, specific recommendations and our own previous experience of a reviewer's characteristics. For instance, we avoid using people who are slow, careless or do not provide reasoning for their views, whether harsh or lenient. All submissions will be double blind peer reviewed. All papers are expected to have original content. They should not have been previously published and it should not be under review. Prior to the sending out to referees, editors check that the paper aim and scope of the journal. The journal seeks minimum three independent referees. All submissions are subject to a double blind peer review; if two of referees gives a negative feedback on a paper, the paper is being rejected. If two of referees gives a positive feedback on a paper and one referee negative, the editor can be decide whether accept or reject. All submitted papers and referee reports are archived by journal Submissions whether they are published or not are not returned. Authors who want to give up publishing their paper in MEUJMAF after the submission have to apply to the editorial board in written. Authors are responsible from the writing quality of their papers. MEUJMAF journal will not pay any copyright fee to authors. A signed Copyright Assignment Form has to be submitted together with the paper.

PUBLICATION ETHICS

Our publication ethics and publication malpractice statement is mainly based on the Code of Conduct and Best-Practice Guidelines for Journal Editors Committee on Publication Ethics (COPE). (2011, March 7). Code of Conduct and Best-Practice Guidelines for Journal Editors. Retrieved from http://publicationethics.org/files/Code%20of%20Conduct_2.pdf

PUBLICATION FREQUENCY

The MEUJMAF accepts the articles in English and is being published 2 times (December and June) a year.

CORRESPONDENCE ADDRESS

Journal Contact: meujmaf@mersin.edu.tr

Mersin University
Journal of Maritime Faculty

Mersin University Journal of Maritime Faculty (MEUJMAF)
Vol. 6, Issue 1, pp. 1-16, June 2024
e-ISSN 2687-6612, Türkiye
DOI: 10.47512/meujmaf.1418239
Research Article

MARITIME SECURITY IN A TECHNOLOGICAL ERA: ADDRESSING CHALLENGES IN BALANCING TECHNOLOGY AND ETHICS

Md Syful ISLAM*[1]

[1] Ankara University, Sea and Maritime Law Department, Ankara, Türkiye
ORCID ID 0000-0002-3092-0858
syful.au.bd@gmail.com

* Corresponding Author
Received: 11/01/2024 Accepted: 12/05/2024

ABSTRACT
Within the context of rapid technological advancements, the ethical dimensions of maritime security are explored, focusing on the challenges and opportunities brought about by emerging technologies and their implications for maritime security practices. Potential risks related to technology misuse, such as privacy infringement, disproportionate use of force, and the erosion of human judgment and accountability, are emphasized. The importance of adopting a balanced approach that considers both the benefits and risks of technological advancements is stressed, as well as the need for robust governance frameworks and international cooperation to ensure responsible and ethical technology use in maritime security. The research methodology involves a systematic literature review of scholarly articles, policy documents, and relevant case studies in the field of maritime security. Ethical frameworks, including proportionality, necessity, transparency, accountability, and human rights, are applied to assess the ethical implications of technologies like unmanned maritime systems, cyber threats, and surveillance capabilities. The significance of ethical training and education for maritime security personnel in promoting responsible and accountable decision-making is underscored, and the article proposes the inclusion of case studies and simulations as effective tools for examining the practical application and effectiveness of ethical training in real-world scenarios. By advocating for a proactive approach that balances technological opportunities with ethical principles, this article contributes to the ongoing discourse on maritime security ethics, providing valuable insights for policymakers, practitioners, and researchers in the field, and offering a roadmap for fostering a secure, transparent, and rights-respecting maritime domain.

Keywords: *Maritime Security, Maritime Threat, Ethical Challenges, Emerging Technologies, Artificial Intelligence*

1. INTRODUCTION

In an age where the ripples of technological advancement touch every aspect of our lives, maritime security stands at a pivotal junction. Historically, the safeguarding of our oceans has been a tale of battling piracy, securing trade routes, and protecting national borders. Today, this narrative is being rewritten under the influence of groundbreaking technological advancements. The world's oceans have become the lifeblood of global trade, the imperative to safeguard maritime domains has never been more pressing (Moore, 2003). This convergence of new technologies with the longstanding mission of ensuring maritime security presents both remarkable opportunities and formidable ethical dilemmas (Androjna et al., 2020).

In this era characterized by rapid advancements in automation, digitalization, and artificial intelligence (AI), it becomes imperative to rigorously scrutinize the evolving nexus of maritime security, emerging technology, and ethics. The vast and interconnected oceans, spanning over 70% of the Earth's surface, serve as critical arteries for global trade, transportation, and communication, playing an indispensable role in the global economy (Pekel et al., 2016). However, these expansive waters are also vulnerable to an array of threats, including piracy, terrorism, environmental disasters, and illicit activities such as drug trafficking and human smuggling (Bakir, 2007). These threats hold the potential to significantly impact global security and stability. While these traditional maritime security challenges persist, they now share the stage with a new cast of threats and opportunities driven by cutting-edge technology. This article aims to dissect and critically analyze the intricate interplay between these emerging technologies and the ethical considerations they entail in the realm of maritime security.

Recent years have witnessed technological innovations that have revolutionized our understanding and management of maritime security (Hetherington et al., 2006). Autonomous vessels, satellite surveillance, drones, AI, and advanced cybersecurity measures have emerged as potent tools in the maritime security arsenal (Calderaro & Blumfelde, 2022). These technologies promise heightened efficiency, improved response times, and enhanced situational awareness. Yet, their deployment also raises profound ethical questions touching upon human rights, privacy, and environmental concerns. AI can detect and track suspicious vessels, while satellite surveillance can provide real-time information on maritime traffic. Autonomous vessels hold the potential to patrol the oceans without human intervention. While these new technologies offer the potential for significant enhancements in maritime security, they concurrently introduce novel ethical challenges (McKay et al., 2022). Key questions arise, such as how to ethically employ AI in decision-making regarding targets and the accessibility of satellite surveillance data. These inquiries underscore the critical need to grapple with the ethical implications of new technology in maritime security.

This paper comprehensively explores the multifaceted interplay between maritime security, new technology, and ethics, aiming to dissect the shifting dynamics within the maritime security landscape, analyze the impact of technological advancements, and explores the ethical considerations underpinning their responsible use. As maritime stakeholders navigate these turbulent waters, understanding and reconciling these dimensions becomes paramount, with the evolving challenges and opportunities at the intersection of maritime security, technology, and ethics examined. This involves scrutinizing the changing maritime threat landscape, dissecting the latest technological advancements, and exploring the ethical dilemmas they raise within this complex terrain, culminating in a discussion of the challenges and opportunities in striking a delicate balance between leveraging technology to secure maritime domains and upholding the ethical principles that underscore our shared humanity.

Once perceived as boundless and unconquerable, the oceans now confront a myriad of perils, from piracy and smuggling to environmental disasters and territorial disputes. Emerging on the horizon of this intricate maritime landscape are the transformative powers of cutting-edge technology, poised to reshape the very foundations of security at sea. Through the exploration of realms such as AI, satellite surveillance, autonomous vessels, and cyber warfare, an understanding is gained of how these innovations are poised to revolutionize the safeguarding of maritime interests. With new technology come new capabilities, but also new dilemmas. In this era of globalization and interconnectivity, maritime security has never been more critical to the modern world. Our oceans serve as maritime trade and energy routes, repositories of vital resources, and theaters of geopolitical maneuvering. Disruptions in maritime security can send ripples that touch every corner of our world. It is, therefore, imperative that we navigate the challenges and opportunities presented by new technology with the utmost care and responsibility.

To navigate these complex dimensions, the paper is structured systematically. It begins with a historical insight into maritime security, tracing its evolution and highlighting how technological advancements have historically influenced maritime practices. Following this, addressing the contemporary maritime threat landscape, exploring how new challenges are shaping the domain and the role technology plays in this context. Subsequent sections are dedicated to a detailed examination of various emerging technologies and their transformative impact on maritime security. This technical exploration paves the way for a pivotal discussion on the ethical considerations that arise from the deployment of these technologies. The paper culminates in a critical analysis of how to balance the dual imperatives of leveraging technology for security and upholding ethical standards. It's important to clarify the methodological approach of this paper. It adopts a systematic literature review methodology, drawing insights from a wide array of scholarly articles, policy documents, and relevant case studies (Singh, 2015). This approach allows for a comprehensive understanding of the topic, grounding the analysis in a robust theoretical framework while also considering practical implications.

2. HISTORICAL INSIGHT OF MARITIME SECURITY AND TECHNOLOGY

Through conducting a comprehensive historical analysis, this investigation reveals the dynamic interplay between technological progress and the multidimensional

approach of present-day maritime security challenges. It commences with ancient civilizations like the intrepid Phoenicians and seafaring Greeks who braved piracy and tempestuous storms, employing rudimentary yet groundbreaking technologies such as oar-powered vessels and celestial navigation (Cunliffe, 2017; Markoe, 2000; Moser, 2010). Significant technological advances during the Industrial Revolution propelled the modernization of naval fleets and expanded maritime domain awareness (Usluer, 2022). The Age of Exploration introduced audacious European voyages, driving innovation through instruments like the astrolabe and compass, expanding the horizons of maritime endeavor (Jowitt, 1995; Terpsidi et al., 2019). The rise of naval empires, epitomized by the formidable British Royal Navy, underscored the geopolitical significance of maritime security and witnessed technological feats such as copper sheathing and precise chronometers (Bowers & Koh, 2017; Fuller, 2014). The cataclysmic events of the World Wars ushered in submarines, mines, and long-range artillery as unprecedented threats, but also ignited a technological revolution with advancements like sonar, radar, and encryption technologies. The contemporary era grapples with traditional challenges like piracy and smuggling, alongside emerging threats such as maritime terrorism and cyberattacks, met by cutting-edge solutions including satellite surveillance, unmanned underwater vehicles (UUVs), and advanced data analytics, all within the context of a globally connected and geopolitically complex world (Yang et al., 2022).

Throughout history, technological progress and maritime security has maintained a symbiotic relationship. Technological innovations have not only empowered nations and civilizations to protect their maritime interests but have also been instrumental in driving the evolution of maritime challenges themselves. In the modern era, it is recognized that the relentless march of technology continuously shapes the landscape of maritime security, establishing a framework for the exploration of challenges and opportunities in subsequent chapters.

3. THE CONTEMPORARY MARITIME THREAT LANDSCAPE

Navigating the contemporary maritime threat landscape reveals a complex web of challenges, each intertwined with global security, environmental sustainability, and legal boundaries. These threats—ranging from piracy and maritime terrorism to human trafficking and migrant smuggling, environmental degradation, and illicit trafficking—pose significant risks not only to the safety and security of maritime routes but also to global commerce and the ecological balance. Firstly, these issues are identified as the most prevalent and impactful in the maritime domain, representing urgent challenges that significantly affect global trade and security. Their widespread nature necessitates an immediate and detailed examination. Secondly, the historical and ongoing relevance of these threats is seen as crucial. For example, piracy, with its centuries-old history, continues to evolve and adapt, offering insight into the persistent nature of certain maritime challenges. This enduring relevance underscores the need for a dynamic and evolving approach to maritime security.

Moreover, these issues are inherently multidisciplinary, involving aspects of security, legal frameworks, ethical considerations, environmental impact, and political implications. This complexity requires a focused approach to ensure a comprehensive understanding of each aspect. The availability of well-documented cases and incidents related to these threats provides concrete examples for analysis, enabling a deeper exploration of both theoretical and practical implications. Lastly, practical considerations, such as resource limitations and the scope of the study, also play a crucial role in defining the focus areas.

3.1. Piracy: A Persistent Peril

Maritime piracy, a historical challenge that persists into the modern era, presents a complex case study in maritime security. Its ongoing relevance is significantly reflected in international law, particularly under the United Nations Convention on the Law of the Sea, 1982 (UNCLOS). Article 101 of UNCLOS is a pivotal legal instrument in this framework, "defining piracy as illegal acts of violence, detention, or depredation committed for private ends by the crew or passengers of a private ship or aircraft in high seas or outside the jurisdiction of any state". This article categorizes piracy under three distinct activities: illegal acts of violence or detention committed for private ends in high seas, voluntary participation in the operation of a pirate ship or aircraft and inciting or facilitating such acts.

Beyond UNCLOS, other international legal instruments play crucial roles in addressing piracy. The Suppression of Unlawful Acts Against the Safety of Maritime Navigation Convention, 1988 (SUA) specifically targets terrorism at sea, contributing to the broader effort to ensure maritime navigation's safety. Similarly, the Djibouti Code of Conduct 2009, focuses on repressing piracy and armed robbery against ships in the Western Indian Ocean and the Gulf of Aden. This regional agreement is complemented by the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), the first regional government-to-government accord aimed at promoting cooperation against such maritime threats in Asia. Additionally, the International Ship and Port Facility Security Code (ISPS), an amendment to the Safety of Life at Sea Convention, 1974 (SOLAS) and Djibouti Code, sets minimum security arrangements for ships, ports, and government agencies, underscoring the importance of security standards in combating piracy.

The relationship between piracy and technology is inherently multifaceted. Technological advancements have simultaneously facilitated and combated piracy. Pirates have leveraged technology for more effective coordination, navigation, and targeting of vessels, utilizing tools like GPS, satellite phones, AIS, and advanced weaponry. Conversely, technology is integral in fighting piracy, with maritime security bolstered by advanced surveillance systems, tracking technologies like the AIS, and enhanced communication tools. These technologies enable quicker response times and more effective coordination among international naval forces. The development of ship security technologies and

defensive measures, such as non-lethal weapons and secure ship designs, further contribute to combating piracy. Thus, technology serves as a double-edged sword in maritime piracy, enhancing the capabilities of both pirates and those working to counteract piracy. Maritime piracy remains a significant global security issue, as highlighted by several high-profile incidents over the years. Each incident not only underscores the gravity and consequences of piracy but also demonstrates the diverse responses by national and international entities.

3.1.1. Hijacking of MV Maersk Alabama (2009)

This incident gained international attention when Somali pirates hijacked the U.S.-flagged MV Maersk Alabama. It was notably the first successful pirate seizure of an American-flagged ship since the early 19th century, highlighting the growing sophistication of Somali pirates (Shambaugh et al., 2014). The incident raised global awareness about the severity of piracy off the Somali coast, leading to increased international naval patrols in the region. The subsequent legal proceedings in the United States (US) against the captured pirates demonstrated the effectiveness of national jurisdictions in addressing piracy incidents. This incident, famously depicted in the movie "Captain Phillips" underscored the perilous nature of piracy off the coast of Somalia (Danoff, 2017; Luzón-Aguado, 2018).

3.1.2. Hijacking of the oil tanker Sirius star (2008)

The Sirius Star, a Saudi-owned VLCC (Very Large Crude Carrier), was hijacked by Somali pirates far off the coast of Kenya. The incident was notable for its scale: the Sirius Star was one of the largest ships ever captured by pirates, and its cargo was valued at over $100 million. The hijacking highlighted the extensive reach of Somali pirates and the vulnerability of international shipping, even far from the traditional pirate-infested waters. The pirates demanded a ransom, and after two months, the ship and crew were released, presumably after a payment was made (Lennox-Gentle, 2010). This case was primarily dealt with through negotiations and ransom payment, reflecting the complex challenges in resolving piracy incidents without military intervention. The incident highlighted the extensive reach of pirates and the vulnerability of international shipping. The resolution of this incident, predominantly through negotiations and ransom payment, reflects the complex challenges in resolving piracy incidents.

3.1.3. Capture of the yacht quest (2011)

The hijacking of the Quest, an American yacht, by Somali pirates led to a tragic outcome with the death of four American citizens. This incident was particularly impactful due to the loss of life and the involvement of private individuals, rather than a commercial vessel. It brought to light the risks faced by private maritime travelers in piracy-prone areas. The US military intervened in this case, and the pirates were captured and later faced legal proceedings in the US (Crook, 2012). This incident is an example of direct military intervention and subsequent legal action in a piracy case.

In response to the increasing piracy threat, especially in regions like the Gulf of Aden, international naval forces have maintained a sustained presence (Ehizuelen, 2023). This deployment showcases a global cooperative effort to combat piracy and enhance maritime security. These forces have been instrumental in deterring pirate attacks and securing commercial shipping in high-risk areas. The immediate threat of piracy in the 21st century is further emphasized by testimonies from seafarers who have encountered pirates. These accounts provide valuable insights into the challenges and psychological impacts faced by individuals navigating these dangerous waters. Together, these incidents and responses illustrate the varied nature of piracy and the comprehensive approach required to address it. The combination of military, legal, and diplomatic efforts, involving national jurisdiction and international cooperation, has been crucial. Furthermore, these cases have significantly influenced the development of international maritime security policies, leading to enhanced anti-piracy measures and greater collaboration between nations to safeguard maritime routes.

3.2. Terrorism at Sea: A Growing Concern

Maritime terrorism represents a significant and evolving aspect of global maritime security, posing distinct challenges addressed by various legal frameworks. To understand the gravity of this threat, it is instructive to examine notable incidents like the 2000 bombing of the USS Cole in Yemen's port of Aden and the 2002 attack on the French oil tanker Limburg off the coast of Yemen (Peng, 2005). These attacks, carried out with explosive-laden boats, resulted in the loss of life, substantial property damage, and highlighted the vulnerabilities of maritime assets to terrorist acts. The link between maritime terrorism and piracy is a critical aspect of this threat. While piracy is primarily motivated by financial gain, maritime terrorism is ideologically driven and aims to achieve broader political objectives, which can include disrupting international trade. Terrorists may employ similar tactics to pirates, such as hijacking and bombing, but their goals and the implications of their actions are vastly different. Maritime terrorism poses a direct threat to international security and trade, as major shipping routes and ports are potential targets for terrorist activities (Raymond, 2006). The disruption of these routes and ports can significantly impact global trade and economies, given the reliance on maritime transport for the majority of international trade.

The international legal response to maritime terrorism includes key instruments like the SUA Convention 1988, and its protocol. These criminalize a range of unlawful acts against maritime navigation and fixed platforms, specifically targeting terrorist acts against ships, offshore platforms, and ports (Karim, 2022). The ISPS Code, part of the SOLAS Convention, establishes frameworks for detecting and assessing maritime security threats, underscoring the need for continuous cooperation and vigilance (Şeker, 2018). United Nations Security Council Resolutions, such as Resolution 1373 (2001), play a pivotal role in establishing global principles for combating terrorism, including its maritime aspects. Regional initiatives like the ASEAN Regional Forum (ARF) have also contributed to enhancing maritime security through cooperative measures.

Legal precedents set by international courts, including the International Court of Justice (ICJ) and the International Criminal Court (ICC), underscore the seriousness of maritime terrorism as a transnational crime (Sands, 2003). Although these courts have not directly adjudicated many cases of maritime terrorism, their frameworks and principles guide the international legal response to such acts. For instance, the Rome Statute of the ICC includes acts of terrorism as part of war crimes in certain contexts, and the ICJ has dealt with cases related to state-sponsored terrorism. Disputes concerning state actions against maritime terrorism, potentially falling under the International Tribunal for the Law of the Sea (ITLOS), highlight the need for a harmonized international legal approach.

Terrorism at sea poses a significant threat to international trade, largely due to the critical role maritime routes and facilities play in the global economy. Major shipping routes, such as the Strait of Hormuz, the Suez Canal, or the Malacca Strait, are essential arteries for the movement of goods worldwide. A terrorist attack in these strategic maritime corridors can lead to closures or heightened security measures, resulting in substantial delays and disruptions in the global supply chain. The example, the Strait of Hormuz, a key transit point for the world's oil supply, is highly susceptible to the impacts of maritime terrorism, where any threat can escalate global oil prices and supply issues. Ports, as crucial hubs in international trade, are also vulnerable targets (Wenning et al., 2007). The 2000 bombing of the USS Cole in Yemen's port of Aden exemplifies how terrorist attacks can cause not only physical damage but also operational disruptions, leading to cargo delays and increased logistical costs (Ban, 2010). Beyond the immediate effects, the persistent threat of maritime terrorism escalates overall shipping costs. Enhanced security protocols, higher insurance premiums, and rerouting away from high-risk areas all contribute to increased operational expenses for shipping companies, with these costs often passed on to consumers (Ganoulis, 2007).

The economic ramifications extend beyond immediate disruptions, leading to increased operational costs for shipping companies due to enhanced security measures and insurance premiums. This escalation in shipping costs, coupled with the potential economic decline in coastal communities reliant on maritime trade, underscores the widespread economic impact of maritime terrorism. Additionally, global supply chain disruptions further amplify the need for a robust and coordinated international response.

Investments in maritime security technologies and infrastructure, though essential, add another layer of financial burden to shipping operations. The cumulative effect of these factors, encompassing disrupted routes, port operations, and global supply chain implications, accentuates the profound impact maritime terrorism has on international trade (Power, 2008). The evolving nature of maritime terrorism, including the use of advanced technologies for attacks and communication by terrorist groups, necessitates ongoing adaptation of legal, security, and diplomatic measures.

3.3. Environmental Concerns: A Comprehensive Legal Perspective

Environmental issues are a critical aspect of maritime security, necessitating a detailed exploration of the legal frameworks and case studies that shape this domain. Key international agreements, such as the International Convention for the Prevention of Pollution from Ships 1973/1978 (MARPOL), are central to efforts aimed at minimizing environmental risks in maritime activities (Julian, 2000). MARPOL, specifically, sets stringent regulations to prevent accidental and operational oil spills from ships, a direct response to historical environmental disasters.

To understand the impact of these regulations, a closer examination of notable incidents is essential. The Exxon Valdez oil spill of 1989, a devastating environmental disaster in Alaska's Prince William Sound, serves as a pivotal case (Knudsen, 2009). This incident led to significant ecological destruction and sparked extensive legal battles, culminating in a critical lawsuit against ExxonMobil. The aftermath of this event played a vital role in shaping subsequent environmental legislation and maritime practices. Another illustrative case is the grounding of the MV Wakashio off the coast of Mauritius in 2020 (Hebbar & Dharmasiri, 2022). This incident not only highlighted the fragility of coastal ecosystems in the face of shipping accidents but also brought to the forefront the legal complexities involved in such disasters. It raised pertinent questions about liability, compensation, and preventive measures under international maritime law.

The legal dimensions of these incidents can be further understood through the frameworks established by the UNCLOS and the United Nations Framework Convention on Climate Change (UNFCCC) 1992 (Tompkins & Amundsen, 2008). UNCLOS, for instance, lays down comprehensive legal norms for protecting the marine environment from human-induced damage, while the UNFCCC addresses broader climate-related impacts on maritime environments. It is important to discuss the cases adjudicated by ITLOS (Keyuan, 2010). ITLOS plays a crucial role in resolving disputes arising from the interpretation and application of UNCLOS. For instance, the ITLOS case "The M/V 'Norstar' Case (Panama v. Italy)" dealt with issues of maritime environmental protection and jurisdiction (Collins, 2019). Another relevant case is "The South China Sea Arbitration (The Republic of Philippines v. The People's Republic of China)", which, among other issues, addressed the environmental implications of maritime activities (Cogliati-Bantz, 2016). These cases exemplify how ITLOS contributes to the evolving jurisprudence in maritime environmental law.

3.4. Illicit Activities: A Comprehensive Legal and Human Perspective

In the realm of maritime security, illicit activities such as illegal fishing, drug trafficking, and human smuggling pose significant threats. Addressing these challenges requires a nuanced understanding of both the legal frameworks and the human impacts involved. Central to the legal dimension is the United Nations Convention against Transnational Organized Crime (UNTOC) 2000,

which establishes a global framework for combating various forms of organized crime at sea, including trafficking and smuggling operations (Rose, 2020). The ITLOS plays a pivotal role in resolving disputes related to illicit maritime activities. Notable cases include the "M/V 'Saiga' (No. 2) Case (Saint Vincent and the Grenadines v. Guinea)", addressing the arrest of a vessel for alleged smuggling, and the "Hoshinmaru and Tomimaru Cases (Japan v. Russia)", involving the detention of Japanese fishing vessels by Russian authorities for suspected illegal fishing (De La Fayette, 2000; Oxman, 2008). These cases highlight the complexities of jurisdiction and the enforcement of maritime law.

The European Court of Human Rights (ECHR) also contributes significantly to this field. In "Medvedyev and Others v. France", the court examined the legality of the detention of a crew on the high seas for suspected drug trafficking, focusing on the balance between state powers and individual rights (Papastavridis, 2010). Similarly, "Rigopoulos v. Spain" addressed the rights violations of a vessel's captain detained for alleged illegal fishing, underscoring the human rights aspect in maritime detentions (Guilfoyle, 2010). Beyond legal proceedings, the perspectives of law enforcement, smugglers, coastal communities, and maritime professionals provide a multifaceted view of the challenges in combating these activities. Testimonies from those on the front lines reveal the strategic and operational difficulties in policing the seas, while the experiences of affected individuals and communities highlight the economic and social tolls.

4. THE TRANSFORMATIVE ROLE OF TECHNOLOGY IN MARITIME SECURITY

In the current era of rapid technological advancement, maritime security is being profoundly transformed. The way maritime threats are perceived, addressed, and mitigated is being revolutionized by new technologies. In this section, the dynamic and evolving role of technology in enhancing maritime security will be delved into. Key areas, including autonomous vessels, satellite surveillance, artificial intelligence, cybersecurity, and more, will be explored. Through the examination of specific examples, how these innovations are reshaping the maritime security domain will be uncovered.

4.1. Autonomous Vessels: Navigating the Uncharted Waters

The integration of autonomous vessels into maritime security operations represents a pivotal shift in how security challenges at sea are approached. This paradigm change is being brought about by unmanned ships equipped with advanced sensors, navigation systems, and artificial intelligence (Trowers, 2023). This transformation is exemplified by the "Sea Hunter," an autonomous surface vessel developed by the US Navy. It is designed for continuous, long-endurance missions, during which submarines can be tracked and trailed, underwater mines detected, and intelligence, surveillance, and reconnaissance missions performed autonomously (Gallup, 2022). Equally significant is the emergence of autonomous technology in the commercial maritime industry, aiming to enhance operational efficiency and safety. "The Yara Birkeland", often cited as the world's first fully autonomous cargo ship, represents a leap towards sustainable maritime trade, utilizing electric power and automation to minimize human error and environmental impact. This shift towards autonomy in shipping promises not only to redefine traditional maritime labor but also to set new benchmarks for environmental stewardship in the industry.

However, the rapid adoption of autonomous maritime systems raises substantial environmental concerns. If not designed with ecological sensitivity, these systems risk disrupting marine ecosystems through increased noise pollution, potential leaks of hazardous substances, and unintended collisions with marine wildlife. For instance, the reliance on batteries in electric autonomous vessels necessitates careful consideration of battery disposal and recycling processes to prevent oceanic contamination. Similarly, the acoustic footprint of autonomous underwater vehicles must be meticulously managed to avoid disturbing marine life, especially sensitive species. By reducing the need for human personnel onboard, not only are operational risks minimized but also more persistent and cost-effective monitoring of vast maritime areas is enabled. Additionally, autonomous ships face cybersecurity vulnerabilities, including the risk of hacking and data breaches, which could compromise navigation systems and the safety of maritime operations.

4.2. Satellite Surveillance: Eyes in the Sky

Satellite technology has revolutionized maritime domain awareness, providing an unprecedented view of maritime activities on a global scale. High-resolution satellite imagery, coupled with advanced analytics, offers a comprehensive view of vessel movements and maritime conditions (Lieske et al., 2011). The Global Fishing Watch platform is a prime example of satellite-based technology's application in maritime security (Drakopulos et al., 2022). It utilizes satellite data and artificial intelligence to monitor and combat illegal, unreported, and unregulated (IUU) fishing activities (Zuzanna et al., 2022). By analyzing vessel movements and identifying suspicious behavior, it helps authorities enforce fisheries regulations and protect marine ecosystems. This technology-driven approach enhances transparency and accountability on the high seas, contributing to sustainable fishing practices.

4.3. Artificial Intelligence (AI): Predictive Insights and Decision Support

AI plays a pivotal role in maritime security by providing predictive insights and decision support tools. AI-driven algorithms analyze vast datasets, including vessel traffic patterns, weather conditions, and historical incident data, to identify potential threats and vulnerabilities (Mandal & Ghosh, 2023). The Maritime Safety and Security Information System (MSSIS) is a comprehensive AI application in maritime security. MSSIS integrates data from multiple sources, including AIS signals, radar, and satellite imagery, to create a real-time situational awareness picture. By continuously monitoring maritime traffic and identifying anomalies, it assists in early threat detection and rapid response. This

system enables maritime authorities to proactively address security challenges and deploy resources more effectively.

4.4. Cybersecurity: Demonstrating the Criticality of Maritime Cyber Threats

The maritime sector's increasing reliance on digital technology has simultaneously opened avenues for efficiency and vulnerability. Cyber threats in this domain are not just theoretical; their impacts are real and far-reaching, as several incidents have starkly demonstrated. These examples not only underline the severity of potential threats but also emphasize the crucial need for robust cybersecurity measures. One of the most significant incidents illustrating this vulnerability was the NotPetya cyberattack in 2017 (Lika et al., 2018). Targeting several large organizations, including the maritime giant Maersk, this ransomware attack disrupted global shipping operations, leading to substantial logistical chaos and financial losses (Lim, 1998). The attack's impact on Maersk alone, which included the immobilization of port operations and the necessity for a complete IT systems overhaul, serves as a sobering reminder of the catastrophic consequences of such breaches.

Beyond NotPetya, other instances further highlight the sector's susceptibility. For example, in 2018, the Port of San Diego suffered a ransomware attack that disrupted its IT systems and administrative services, impacting its ability to effectively manage maritime operations (Senarak, 2023). Similarly, in 2019, a cyberattack on the Mediterranean Shipping Company's servers led to significant interruptions in its cargo booking system, showcasing the potential for operational disruption (Alekseenkov et al., 2022). These incidents reveal several key points about maritime cybersecurity. First, they underscore the interconnected nature of digital infrastructure in the maritime sector, where a single breach can ripple through various interconnected systems, causing widespread operational disruptions. Second, they show that cyber threats can have direct financial implications, both in terms of immediate disruption costs and long-term reputational damage. Lastly, they highlight the human element, as these attacks can potentially compromise crew safety and environmental security. Therefore, the maritime industry's investment in cybersecurity - encompassing advanced detection systems, secure communication protocols, employee training, and collaborative efforts among stakeholders - is not just a proactive measure, but a necessary response to a demonstrated and ongoing threat. These steps are vital for safeguarding against the complex and evolving nature of cyber threats, ensuring the continuity of maritime operations and the safety of personnel and assets in this globally critical sector.

4.5. Biometrics and Access Control: Securing Critical Infrastructure

The adoption of biometrics and advanced access control systems is enhancing security at maritime facilities, ports, and vessels. Biometric technologies, such as fingerprint and facial recognition, are being employed for identity verification and access control, ensuring that only authorized personnel gain entry to sensitive areas. Many ports around the world have implemented biometric access control systems for dockworkers and personnel. These systems streamline security procedures, reduce the risk of unauthorized access, and enhance overall port security. Biometric authentication provides a secure and convenient method for verifying the identity of individuals in high-security environments. The integration of new technologies into maritime security operations is ushering in an era of enhanced capabilities, efficiency, and effectiveness. Autonomous vessels, satellite surveillance, artificial intelligence, biometrics, and robust cybersecurity measures are instrumental in mitigating maritime threats, safeguarding marine environments, and ensuring the safety of seafarers and critical infrastructure (Stöhs & Bruns, 2018).

5. ETHICAL CONSIDERATIONS IN MARITIME SECURITY

The use of new technology in maritime security is rapidly evolving, and with it comes several ethical challenges and opportunities. Ethics in maritime security is built on foundational principles. It is an intricate web of accountability, transparency, and a justifiable use of force. It is a commitment to uphold the safety and well-being of individuals and ecosystems, regardless of the means used for their protection. This chapter will delve into the ethical dilemmas posed using new technology, explore questions related to human rights, privacy, and environmental ethics, and discuss the importance of responsible technology deployment.

5.1. Ethical Dilemmas

The maritime industry, once rooted in centuries-old traditions, now finds itself at the precipice of a technological revolution. Unmanned aerial and underwater systems, advanced satellite-based navigation, and data analytics have disrupted the conventional norms. This shift necessitates a profound exploration of ethical dilemmas that unfold, from the emergence of fully autonomous ships to the applications of artificial intelligence and machine learning in maritime security. One of the key ethical dilemmas posed using new technology in maritime security is the potential for misuse (Johansson et al., 2021). For example, autonomous maritime systems could be used by malicious actors to launch attacks on ships or critical infrastructure. Additionally, new technologies such as facial recognition and artificial intelligence could be used to surveil and track people without their consent. Another ethical dilemma is the potential for bias in new technologies. For instance, facial recognition algorithms have been shown to be less accurate in identifying people of color. If these algorithms are used in maritime security applications, this could lead to discrimination and profiling. A third ethical dilemma is the potential for new technologies to violate human rights, privacy, and environmental ethics. According to Hofmann the use of surveillance technology could violate people's right to privacy (Hofmann, 2020). Additionally, the use of autonomous maritime systems could lead to loss of life or damage to the environment if they are not properly designed and operated.

5.2. Human Rights, Privacy, and Environmental Ethics in Maritime Security Technology

The integration of autonomous systems and AI in maritime security raises critical questions about human rights, privacy, and environmental ethics. This integration, while beneficial, must be critically examined, especially when these technologies are involved in piracy suppression, border enforcement, and search and rescue missions. It's essential to consider the ethical implications of life-and-death decisions made by AI and autonomous systems. Such decisions can blur the boundaries between moral responsibility and technological autonomy (Klein, 2021). For instance, under international human rights law, particularly the Universal Declaration of Human Rights (UDHR) 1948, and the International Covenant on Civil and Political Rights (ICCPR) 1954, every individual is entitled to fundamental rights such as the right to life, liberty, and security of person (Article 3, UDHR). When autonomous systems are deployed in maritime security, their programming and operation must align with these established human rights standards, ensuring that the right to life and security is not compromised (Lagdami & Fakhry, 2020).

Moreover, the right to privacy, as enshrined in Article 12 of the UDHR and Article 17 of the ICCPR, becomes paramount when discussing surveillance technologies in maritime settings. The use of such technologies should be limited, targeted, and non-discriminatory. Facial recognition and other surveillance tools must not violate individuals' privacy rights. Data protection laws, like the General Data Protection Regulation (GDPR) 2016, in the European Union, provide a framework for the lawful processing of personal data and could serve as a guideline for handling data collected through maritime security systems. Environmental ethics are also a critical component in the deployment of maritime security technologies. In the domain of maritime security, the integration of technological advancements necessitates strict adherence to the foundational legal frameworks established by the UNCLOS. This pivotal convention governs all oceanic activities, emphasizing the responsible utilization of technology while highlighting the critical need for environmental preservation. The convention's principles, particularly articles 192 to 196, mandate states to actively prevent, reduce, and control marine pollution, thereby guiding the deployment of new technologies in maritime security. These principles are directly applicable to the deployment of modern maritime technologies, such as autonomous vessels and satellite surveillance systems. For instance, satellite surveillance operations, as governed by UNCLOS guidelines, play a crucial role in monitoring environmental threats like oil spills and illegal dumping, thereby facilitating prompt and effective responses to mitigate pollution. This application of UNCLOS principles to technological deployments underscores the convention's significance in maritime technological progress with environmental stewardship in maritime security operations.

With rapid technological advancement, it's vital to emphasize responsible technology deployment, guided by ethical considerations. In maritime security, adherence to ethical frameworks, codes of conduct, and understanding international and domestic legal instruments is crucial. This adherence includes developing and implementing policies and guidelines for technology use, ensuring they align with legal standards like the UNCLOS for environmental protection and the ICCPR for human rights. Moreover, technologies must be designed and operated with safeguards to protect human rights and the environment (Kamila & Jasrotia, 2023). For example, the deployment of AI in maritime security should be accompanied by ethical AI frameworks, such as those proposed by the European Union, which emphasize human oversight, transparency, and accountability. These frameworks can guide the development of AI systems to ensure they are fair, non-discriminatory, and respect the autonomy and rights of individuals. In summary, the deployment of new technologies in maritime security requires a balanced approach, respecting human rights, privacy, and environmental integrity, guided by existing legal frameworks and ethical principles.

5.3. Analysis of Case Studies in Maritime Security Technology: Legal Considerations

Several recent case studies have illuminated the ethical quandaries that arise with the increasing integration of new technologies into maritime security provide a platform to explore specific legal frameworks and their implications.

5.3.1. China's use of facial recognition in the South China sea (2019)

In 2019, China came under international scrutiny for deploying facial recognition technology to track and monitor Uyghur Muslims in the South China Sea (Mooney, 2021). This controversial use of technology allowed the Chinese authorities to identify and monitor Uyghur fishermen even within their traditional fishing grounds, raising alarm bells among human rights advocates regarding privacy and freedom of movement. China's acts conflicts with Article 17 of the ICCPR, which China has ratified. This article explicitly protects individuals against "arbitrary or unlawful interference with his privacy, family, home or correspondence."

5.3.2. Iranian drone attack on Saudi oil tanker (2020)

In 2020, concerns were raised about the potential misuse of autonomous maritime systems after an Iranian drone attack targeted a Saudi Arabian oil tanker (Hassib & Ayad, 2023). This incident underscored the dual-use nature of autonomous systems, which can serve both protective and disruptive purposes, intensifying concerns about surveillance and security. The drone attack raises issues under the United Nations Charter, specifically Article 2(4), which prohibits the use of force against the territorial integrity or political independence of any state. Furthermore, under the IMO conventions, specifically SOLAS Chapter XI-2 on Special Measures to Enhance Maritime Security, there is an implied need to regulate and control the use of autonomous systems to prevent such attacks.

5.3.3. US AI surveillance at the Mexico border (2021)

In 2021, the United States government faced criticism for its deployment of artificial intelligence to track and monitor migrants at the US-Mexico border (Boyce & Chambers, 2021). This technology, aimed at identifying and tracing migrants as they crossed the border, prompted a debate on the balance between security and individual rights, particularly regarding privacy and freedom of movement. The US government's use of AI in border surveillance engages the Fourth Amendment of the U.S. Constitution, which protects against "unreasonable searches and seizures." This practice also needs to be aligned with Article 12 of the ICCPR, ensuring the right to liberty of movement.

5.3.4. Israeli surveillance of Palestinian fishermen (2018)

In 2018, the Israeli government came under fire for employing surveillance technology to track and monitor Palestinian fishermen in the Gaza Strip, spotlighting the ethical implications of such technology in a sensitive political context (Loewenstein, 2023). This case falls under the scope of Part VII of the UNCLOS, specifically Articles 87 and 90, which guarantee the freedom of the high seas and the right to engage in fishing on the high seas, respectively. Additionally, Article 17 of the ICCPR on privacy could be relevant here.

5.3.5. EU ai monitoring of immigration in the mediterranean (2020)

In 2020, the European Union was criticized for employing artificial intelligence to track and monitor illegal immigration in the Mediterranean Sea, prompting questions about the ethics of border control and immigration enforcement (Martínez, 2023). The EU's use of AI in monitoring immigration must comply with the Charter of Fundamental Rights of the European Union. This includes Article 7 (respect for private and family life) and Article 8 (protection of personal data). Additionally, under the Schengen Borders Code (Regulation (EU) 2016/399), particularly Article 7 on border checks, the use of such technologies must respect fundamental rights and freedoms.

These case studies demonstrate that while existing legal instruments like UNCLOS, IMO regulations, and international human rights laws provide a framework, they may not fully address the nuances of emerging technologies in maritime security. For instance, UNCLOS, primarily concerned with navigation and environmental protection, lacks specific provisions for AI and autonomous systems in maritime surveillance. Similarly, the IMO Code of Conduct, while addressing shipping and terrorism, does not elaborate on the implications of these technologies on privacy and human rights (Salonio, 2002). The MARPOL and the London Convention, pivotal in environmental protection, do not encompass the broader ethical issues of technological advancements in maritime security. Furthermore, issues such as artificial intelligence, autonomous systems, and AIS were not on the agenda in the year when UNCLOS came into force. This gap underscores the need for the development of specific legal instruments or amendments to address AI, autonomous systems, and surveillance technologies, filling a significant deficiency in the current regulatory landscape.

5.4. Potential Benefits

While ethical dilemmas remain at the forefront, the remarkable benefits that these technological advancements bring to the domain of maritime security cannot be overlooked. The ability to secure maritime territories and respond to crises with greater precision and agility is amplified by the heightened surveillance capabilities, reduced response times, and operational efficiency ushered in by these innovations. Like, large areas of the ocean can be patrolled, and threats detected and responded to more quickly and efficiently than human crews can by autonomous maritime systems. Additionally, screening, and vetting procedures can be improved using new technologies such as facial recognition and artificial intelligence.

Maritime security technology stands as a formidable ally in elevating the surveillance and monitoring of the maritime domain, encompassing coastal waters, vital ports, and bustling shipping lanes. This technological prowess is a beacon for the detection and deterrence of illicit activities, including smuggling, trafficking, and piracy. Its multifaceted utility extends to fortifying capabilities in the detection and response to maritime incidents, such as oil spills, shipwrecks, and critical search and rescue operations. The profound impact of maritime security technology resonates in its potential to mitigate the loss of life and property damage. Additionally, it serves as a safeguard for human life by assuming tasks that are perilous or arduous for human intervention, such as mine clearance and underwater surveillance.

Technology can play an important role in improving transparency, accountability, and compliance in the maritime industry. For instance, satellite-based monitoring can be used to track the movements of ships and identify potential illegal activities. Electronic data interchange (EDI) can be used to streamline communication and information sharing between different stakeholders. Technology can also be used to develop new tools and platforms for auditing and reporting. For example, blockchain technology can be used to create tamper-proof records of maritime transactions. This can help to prevent fraud and corruption. In essence, maritime security technology exemplifies the convergence of technological advancements and ethical imperatives, upholding the values of security, safety, and human well-being in our shared maritime domain.

6. CHALLENGES IN BALANCING TECHNOLOGY AND ETHICS IN MARITIME SECURITY

In the complex and dynamic environment of maritime security, the integration of new technologies such as drones, AI, and autonomous maritime vessels (AMVs) offers significant opportunities for enhancing safety and efficiency. However, this integration also brings forth substantial ethical challenges that require careful

consideration and balancing.

One of the primary challenges is reconciling effective security measures with the protection of individual rights and freedoms. For example, the deployment of facial recognition technology at ports can significantly aid in anti-terrorism efforts but simultaneously raises concerns about privacy and unwarranted surveillance. Similarly, the use of LAWS, which can select and engage targets without human intervention, presents ethical questions regarding accountability and compliance with international law and human rights standards. The development and utilization of AMVs highlights concerns about safety, liability, and moral responsibility. Issues such as who bears responsibility for accidents involving AMVs, or how to ensure their ethical deployment, are at the forefront of this technological integration (Bueger et al., 2020). Additionally, the increased reliance on data collection and surveillance technologies by maritime authorities brings into question the responsible and transparent handling of collected data, emphasizing the need to safeguard privacy and civil liberties (Ismail et al., 2021). Indeed, balancing the challenges and ethics in the cases mentioned within maritime security is a complex undertaking. Let's explore these cases in more detail:

6.1. Lethal Autonomous Weapons Systems (LAWS) in Maritime Security

LAWS represent a significant and complex ethical dilemma in maritime security. These systems, capable of operating with varying levels of human oversight, promise enhanced precision and rapid response in defending against maritime threats (Righetti et al., 2018). However, their deployment raises crucial questions of responsibility, accountability, and compliance with international law and human rights. One of the key legal frameworks governing the use of LAWS in maritime security is IHL. IHL requires that LAWS adhere to the principles of distinction, proportionality, and precaution, as outlined in the Geneva Conventions and their Additional Protocols. These principles ensure that combatants differentiate between combatants and civilians, avoid excessive force, and take precautions to minimize harm to civilians. The United Nations Convention on Certain Conventional Weapons (CCW), particularly its Protocol V on Explosive Remnants of War, is also relevant to the deployment of LAWS. However, the CCW does not explicitly regulate LAWS, creating a significant regulatory gap. Customary International Law, which includes accepted norms and practices, also applies to the use of LAWS. However, its application can be ambiguous and subject to varied interpretations, especially in rapidly evolving technological contexts.

Despite these legal instruments, there are notable gaps and ambiguities in the existing legal frameworks. Current international laws, including IHL and CCW, were established before the advent of LAWS and do not directly address the unique challenges posed by these systems. This lack of specificity leads to uncertainties in how these laws are applied to LAWS, particularly in distinguishing combatants from non-combatants and assessing proportionality. Another challenge is accountability and responsibility. The use of LAWS complicates the determination of responsibility for their actions, particularly in cases of unintended harm or violations of international law. The current legal frameworks do not adequately address the question of who is accountable—the operator, commander, manufacturer, or programmer—when a LAWS operates autonomously.

Furthermore, ensuring that LAWS comply with international human rights standards is challenging. The autonomous nature of these systems raises concerns about their ability to make ethical decisions, particularly those involving the right to life and the prohibition of arbitrary deprivation of life under international human rights law. To mitigate these challenges, there is a growing call for the implementation of human oversight in the form of "human-in-the-loop or human-on-the-loop" systems (Gil et al., 2019). These approaches ensure human judgment in critical decision-making processes, aiming to reduce the risk of unethical or unintended actions. Additionally, there is a pressing need for the development of new international legal instruments or amendments to existing ones, specifically tailored to regulate the deployment of LAWS. These legal reforms should aim to provide clear guidelines on the use, accountability, and oversight of LAWS, ensuring their alignment with international humanitarian and human rights law.

6.2. Data Collection and Surveillance Technologies in Maritime Security

The utilization of data collection and surveillance technologies is vital in maritime security for monitoring shipping traffic and identifying threats, yet it raises significant ethical concerns, particularly around privacy and civil liberties. This situation calls for an in-depth analysis of the relevant data protection laws and identification of gaps in these frameworks. Within the European Union, the GDPR stands as a comprehensive law for personal data processing, emphasizing principles like data minimization, purpose limitation, and individual data rights. However, its specific application in maritime surveillance and data collection remains unclear, leading to potential enforcement ambiguities. Similarly, the ICCPR, especially Article 17, offers broad privacy protections against arbitrary or unlawful privacy intrusions. Yet, its direct application to maritime surveillance technology usage is not explicitly covered, presenting challenges in its interpretation and enforcement in maritime contexts.

Moreover, the UNCLOS governs maritime activities but falls short in addressing the use of surveillance technologies and data protection in maritime environments. This absence marks a significant gap in the international legal framework concerning maritime data protection. The current legal structures provide a foundation for data protection and privacy but reveal several gaps and challenges specific to maritime security. Notably, there's a lack of specific guidelines or regulations in both international and domestic laws for the use of surveillance technologies in maritime security, creating uncertainty in the application of data protection laws in this sector. Balancing security and privacy emerge as a complex issue, with existing laws potentially inadequate in addressing the balance between these competing interests, especially where extensive surveillance is deemed necessary. Issues of accountability and transparency also arise, necessitating stronger

mechanisms for the oversight of data collection, usage, and sharing by maritime authorities. The current frameworks may lack sufficient provisions for ensuring accountability and addressing privacy violations or data misuse.

To tackle these challenges, comprehensive policies and regulations specifically guiding the use of data collection and surveillance technologies in maritime security are essential. These policies should strive to balance security needs with individual rights protection, adhering to principles of transparency, accountability, and ethical data handling. Regular ethical assessments of surveillance technologies can assist in identifying and addressing potential privacy issues. Additionally, developing international guidelines or amendments to existing maritime laws, such as UNCLOS, to include specific provisions for data protection and privacy in maritime surveillance is crucial. In conclusion, while data collection and surveillance technologies are indispensable in modern maritime security, their application must be governed by robust legal and ethical frameworks that ensure responsible, transparent use, and respect human rights and privacy. Collaborative efforts within the maritime community are necessary to define and implement these standards, addressing the ethical dilemmas these technologies present in maritime security.

6.3. Relevant Legal Instruments

In the realm of maritime security, international legal instruments play a vital role. However, they exhibit notable gaps and limitations, especially when addressing modern technological advancements. A comprehensive analysis of these instruments, with specific focus on key articles and the identification of gaps, is essential.

6.3.1. United Nations Convention on the Law of the Sea (UNCLOS)

UNCLOS provides a broad legal framework for maritime activities, including articles like Article 94, which outlines obligations for the safety at sea, and Articles 192 onwards, which focus on environmental protection. However, UNCLOS does not specifically address the challenges posed by newer technologies such as AI and autonomous maritime vessels (AMVs). This lack of specificity leads to uncertainties about how these technologies fit within the existing legal framework, particularly in areas of maritime safety and environmental impact.

6.3.2. International Maritime Organization (IMO) Regulations and Guidelines

The IMO oversees critical maritime conventions like SOLAS and STCW. SOLAS, particularly in Chapter V, Regulation 19, mandates specific navigational and communication equipment but does not fully cover the latest advancements in navigation systems. STCW, especially in Chapter IV, sets standards for seafarer training but lacks detailed guidelines for training in advanced technologies like AI and cybersecurity. Furthermore, the IMO Cybersecurity Guidelines (MSC-FAL.1/Circ.3) provide general recommendations but fall short in offering binding enforcement mechanisms or detailed protocols for different levels of cyber threats.

6.3.3. International Ship and Port Facility Security (ISPS) Code

The ISPS Code, particularly in Part A, Section 4, focuses on security measures and information sharing. However, it does not adequately address privacy concerns related to surveillance technologies. This gap in the ISPS Code means it does not fully cover the ethical implications and privacy issues that arise from advanced surveillance and data collection methods in maritime security (Suppiah, 2009).

6.3.4. Developing Guidelines for New Technologies

The IMO is in the process of developing guidelines for AI and autonomous systems in maritime operations, addressing both safe operation and ethical concerns. Additionally, the proposed convention on AMVs is expected to include provisions on their safe and ethical operation (Durmuş, 2023). However, these guidelines and conventions are still under development, and specific articles or provisions that comprehensively address these new technologies are yet to be established.

The rapid advancement of technology in the maritime sector presents significant challenges for existing legal frameworks. There is a clear need for these frameworks, including UNCLOS, IMO regulations, and the ISPS Code, to evolve and include specific, binding regulations and guidelines for emerging technologies like AI, AMVs, and cybersecurity. This evolution is crucial to ensure that maritime operations remain safe, secure, and ethically responsible while adapting to the technological advancements in the industry. Collaborative efforts from international bodies and industry stakeholders are necessary to develop comprehensive regulations that effectively address the gaps and challenges presented by these new technologies.

6.4. Best Practices and Success Stories

In the pursuit of ethical technology solutions for maritime security, several noteworthy best practices and success stories have emerged, showcasing the successful integration of technology while upholding ethical principles:

6.4.1. Australian Border Force (ABF)

The Australian Border Force (ABF) stands as a paradigm of ethical technology adoption in the realm of maritime security. With a commitment to safeguarding its maritime interests, the ABF deploys a spectrum of advanced technological tools, including radar systems, drones, and maritime domain awareness software (Restall, 2017). Notably, The ABF places a strong emphasis on the ethical use of these technologies, having developed a robust set of guidelines and procedures to govern their application. These guidelines align meticulously with UNCLOS mandates, with a particular focus on environmental preservation and pollution control. For example, the deployment of autonomous vessels by the ABF is based on detailed environmental risk assessments and the integration of technologies designed to minimize

ecological disruption. This approach reflects a harmonious blend of innovation with environmental stewardship. Additionally, the ABF's satellite surveillance operations are specifically tailored to monitor and swiftly respond to environmental threats, embodying a proactive stance towards UNCLOS's pollution control objectives. Recognizing the paramount importance of cybersecurity, the ABF has also instituted stringent security protocols to protect the integrity and reliability of these technological operations, thus ensuring that they enhance maritime security without compromising environmental safety. Through these initiatives, the ABF not only demonstrates the practical application of UNCLOS principles but also sets a benchmark for the global maritime community. This shows that technological advancement in maritime security can be harmoniously achieved alongside environmental protection and legal compliance.

6.4.2. European Maritime Safety Agency (EMSA)

The European Maritime Safety Agency (EMSA) is instrumental in fostering ethical technology practices within the maritime domain, particularly concerning cybersecurity. EMSA has developed a suite of tools and resources designed to assist maritime stakeholders in the implementation of the IMO Cybersecurity Guidelines. EMSA offers a comprehensive suite of tools and resources for enhancing maritime cybersecurity practices. This includes a meticulously designed risk assessment tool, enabling stakeholders to evaluate and mitigate cybersecurity risks, promoting responsible and secure technological integration. Additionally, EMSA provides a cybersecurity incident management plan to ensure a prompt and ethical response to cybersecurity threats, thus bolstering the resilience of maritime systems. To further strengthen ethical technology practices, EMSA maintains a directory of cybersecurity experts, establishing a network of professionals capable of upholding the highest standards in maritime cybersecurity.

6.4.3. Global Maritime Cybersecurity Program (GMCP)

The Global Maritime Cybersecurity Program (GMCP) serves as a testament to the potential of public-private partnerships in advancing ethical cybersecurity practices in the maritime sector. This program is dedicated to improving maritime cybersecurity globally and has been instrumental in forging several key resources. The GMCP has played a pivotal role in promoting ethical maritime security through the development of cybersecurity guidelines for ships, providing a comprehensive framework that underscores responsible technology usage and enhances maritime security by safeguarding vessels against cyber threats. In line with their commitment to ethical practices, GMCP has also established a seafarer training program, specifically designed to equip maritime professionals with the knowledge and skills essential for responsible technology use in their operations, further contributing to the overall ethical integrity of maritime security.

6.4.4. The NCAGS Framework

In the realm of maritime security, the Naval Cooperation and Guidance for Operations (NCAGS) stands out as a model of best practices, embodying the principles of effective naval and commercial maritime collaboration. This framework is distinguished by its comprehensive approach to ensuring safe and secure maritime passages in areas of risk, effectively bridging the gap between military operations and commercial maritime activities. NCAGS adapts to all operation levels from peacetime to crisis, coordinating with other disciplines to address situational demands and significantly impact military and economic planning (Usluer, 2022). Central to the success of NCAGS is its grounding in structured guidelines and protocols, meticulously outlined in various sections and articles of its guiding documents. These documents serve as a blueprint for enhancing maritime safety and security, facilitating seamless interaction and information exchange between military and civilian maritime entities. By aligning its operational directives with the UNCLOS framework, NCAGS not only ensures legal compliance but also fosters a standardized approach to maritime security that transcends national jurisdictions. This legal adherence is particularly evident in sections of the NCAGS guidelines that emphasize environmental protection, piracy deterrence, and the safeguarding of maritime commerce routes.

Moreover, NCAGS's operational model is characterized by its innovative integration of technology, as delineated in specific articles focusing on surveillance, communication, and navigational safety. These articles detail the application of satellite technology, AIS, and other technological advancements that enhance the operational capacity of both naval and commercial vessels, ensuring a proactive and informed response to potential threats. By providing a comprehensive and adaptable model for naval cooperation and guidance, NCAGS sets a benchmark for effective maritime security operations, underscoring the vital importance of unity and shared responsibility in safeguarding the world's oceans.

7. CONCLUSION

In conclusion, the integration of advanced technologies like autonomous vessels, AI, satellite surveillance, and cybersecurity measures into maritime security is thoroughly analyzed. These technologies are found to significantly enhance capabilities in surveillance, threat detection, and operational efficiency, thus bolstering the safety and security of maritime domains. However, their deployment also raises complex ethical challenges and legal intricacies.

A nuanced understanding and balanced approach are required to address concerns surrounding human rights, privacy, environmental impact, and the potential for technology misuse. Questions of accountability and human oversight become paramount, especially in the context of autonomous maritime systems. Privacy infringement and data protection issues are brought to the forefront by advanced surveillance technologies such as AI and facial recognition. Cybersecurity is identified as both a protective measure and a potential threat, emphasizing the need for robust defense mechanisms. The analysis highlights gaps in international legal

frameworks like the UNCLOS, IMO regulations, and the ISPS Code in addressing challenges posed by modern technologies. The development of tailored regulations and guidelines is deemed crucial for aligning technological advancements with ethical standards and international law.

Best practices from entities like the Australian Border Force, European Maritime Safety Agency, and the Global Maritime Cybersecurity Program are examined, serving as models for harmonizing technology with ethical principles. These cases demonstrate effective integration of technology into maritime security that is both ethically sound and legally compliant, underscoring the importance of clear guidelines, ethical oversight, and international collaboration. Historical insights into maritime security reveal a significant evolution, influenced by technological advancements from ancient times through the modern era. This historical context, combined with an understanding of contemporary maritime threats like piracy, terrorism, environmental concerns, and illicit activities, is integral to comprehending the ethical dilemmas in maritime security. Legal frameworks addressing these threats and the ethical implications of technology use in this domain are critical.

The responsibility to ensure that technological advancements in maritime security are utilized ethically and responsibly is emphasized. The future of maritime security hinges on maintaining a balance between leveraging technology for enhancements and adhering to ethical principles. Continuous adaptation of legal and ethical frameworks, alongside proactive international cooperation, is essential. This approach ensures a secure and efficient maritime domain that respects human rights, privacy, and environmental integrity. Stakeholders are urged to remain vigilant and committed to upholding these standards, ensuring maritime security remains a bastion of safety, efficiency, and ethical integrity in the technological era. Understanding the historical and current contexts in maritime security is crucial for developing strategies and policies that balance technological benefits with ethical integrity and legal compliance.

In conclusion, as we advance into an era where technology profoundly reshapes maritime security, the responsibility lies in ensuring that these advancements are harnessed ethically and responsibly. The balance between leveraging technology for enhancing maritime security and upholding ethical principles is delicate yet achievable. This paper contributes to the ongoing discourse in this field, offering valuable insights and a framework for stakeholders to navigate these turbulent waters. As we forge ahead, it is imperative that we remain vigilant, adaptive, and committed to fostering a maritime domain that is secure, transparent, and respectful of our shared human rights and environmental heritage.

REFERENCES

Alekseenkov, A., Klyuchnikova, D., Dedova, N., & Sokolov, S. (2022). Cyberattacks in the Water Transport Industry: Types and Diversity. In A. Manakov & A. Edigarian, *International Scientific Siberian Transport Forum TransSiberia - 2021* Cham.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, *8*(10), 776. https://www.mdpi.com/2077-1312/8/10/776

Bakir, N. O. (2007). A Brief Analysis Of Threats And Vulnerabilities In The Maritime Domain. In I. Linkov, R. J. Wenning, & G. A. Kiker (Eds.), *Managing Critical Infrastructure Risks* (pp. 17-49). Dordrecht: Springer Netherlands.

Ban, K.-J. (2010). The Clash of David and Goliath at Sea: The USS Cole Bombing as Sea Insurgency and Lessons for the ROK Navy. *Asian Politics & Policy*, *2*(3), 463-485. https://doi.org/https://doi.org/10.1111/j.1943-0787.2010.01203.x

Bowers, I., & Koh, C. (2017). Navies, Coast Guards, the Maritime Community and International Stability. *Singapore: RSIS Rajaratnam School of Internationa l Studies*(March), 96. https://core.ac.uk/download/225935065.pdf

Boyce, G. A., & Chambers, S. N. (2021). The corral apparatus: counterinsurgency and the architecture of death and deterrence along the Mexico/United States border. *Geoforum*, *120*, 1-13. https://doi.org/https://doi.org/10.1016/j.geoforum.2021.01.007

Bueger, C., Edmunds, T., & McCabe, R. (2020). Into the sea: capacity-building innovations and the maritime security challenge. *Third World Quarterly*, *41*(2), 228-246. https://doi.org/10.1080/01436597.2019.1660632

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, *31*(3), 415-434. https://doi.org/10.1080/09662839.2022.2101885

Cogliati-Bantz, V. P. (2016). The South China Sea Arbitration (The Republic of the Philippines v. The People's Republic of China). *The International Journal of Marine and Coastal Law*, *31*(4), 759-774. https://doi.org/https://doi.org/10.1163/15718085-12341421

Collins, R. (2019). The M/V "Norstar" Case (Panama v. Italy) (ITLOS). *International Legal Materials*, *58*(4), 673-737. https://doi.org/10.1017/ilm.2019.30

Crook, J. R. (2012). Continuing U.S. Efforts to Combat Piracy; Piracy Now Spreading to Gulf of Guinea. *American Journal of International Law*, *106*(1), 160-163. https://doi.org/10.5305/amerjintelaw.106.1.0160

Cunliffe, B. (2017). *On the Ocean: The Mediterranean and the Atlantic from prehistory to AD 1500*. Oxford University Press. https://shorturl.at/swFM4

Danoff, B. (2017). "I'm the Captain Now": Power, Justice, and Tragedy in "Benito Cereno" and Captain Phillips. *American Political Thought*, *6*(1), 30-53. https://doi.org/10.1086/689855

De La Fayette, L. (2000). The M/V "Saiga" (No.2. Case (St. Vincent and the Grenadines v. Guinea), Judgment: International Tribunal For The Law Of The Sea. *International and Comparative Law Quarterly*, *49*(2), 467-476. https://doi.org/10.1017/S0020589300064241

Drakopulos, L., Silver, J. J., Nost, E., Gray, N., & Hawkins, R. (2022). Making global oceans governance in/visible with Smart Earth: The case of Global Fishing Watch. *Environment and Planning E: Nature and Space*, *6*(2), 1098-1113. https://doi.org/10.1177/25148486221111786

Durmuş, A. N. (2023). The Intersection Between Law and Technology in Maritime Law. In K. Noussia & M. Channon (Eds.), *The Regulation of Automated and Autonomous Transport* (pp. 107-166). Springer International Publishing. https://doi.org/10.1007/978-3-031-32356-0_5

Ehizuelen, M. M. O. (2023). Assessing the national and regional effectiveness of countering maritime piracy in the Gulf of Guinea. *GeoJournal*, *88*(4), 3549-3574. https://doi.org/10.1007/s10708-022-10823-0

Fuller, H. J. (2014). *Empire, Technology and Seapower: Royal Navy crisis in the age of Palmerston*. Routledge. https://shorturl.at/ozM01

Gallup, S. P. (2022). Future War at Sea: The US Navy, Autonomy in War at Sea and Emergent Behaviors. In *Emergent Behavior in System of Systems Engineering* (1st ed., pp. 65-92). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003160816-6/future-war-sea-shelley-gallup

Ganoulis, J. (2007). Environmental And Human Security In The Mediterranean. In I. Linkov, R. J. Wenning, & G. A. Kiker, *Managing Critical Infrastructure Risks* Dordrecht.

Gil, M., Albert, M., Fons, J., & Pelechano, V. (2019). Designing human-in-the-loop autonomous Cyber-Physical Systems. *International Journal of Human-Computer Studies*, *130*, 21-39. https://doi.org/https://doi.org/10.1016/j.ijhcs.2019.04.006

Guilfoyle, D. (2010). Current Legal Developments European Court of Human Rights. *The International Journal of Marine and Coastal Law*, *25*(3), 437-442. https://doi.org/https://doi.org/10.1163/157180810X520327

Hassib, B., & Ayad, F. (2023). The Challenges and Implications of Military Cyber and AI Capabilities in the Middle East: The Geopolitical, Ethical, and Technological Dimensions. In M. Eslami & A. V. Guedes Vieira (Eds.), *The Arms Race in the Middle East: Contemporary Security Dynamics* (pp. 49-65). Springer International Publishing. https://doi.org/10.1007/978-3-031-32432-1_4

Hebbar, A. A., & Dharmasiri, I. G. (2022). Management of marine oil spills: A case study of the Wakashio oil spill in Mauritius using a lens-actor-focus conceptual framework. *Ocean & Coastal Management*, *221*, 106103. https://doi.org/https://doi.org/10.1016/j.ocecoaman.2022.106103

Hetherington, C., Flin, R., & Mearns, K. (2006). Safety in shipping: The human element. *Journal of Safety Research*, *37*(4), 401-411. https://doi.org/https://doi.org/10.1016/j.jsr.2006.04.007

Hofmann, B. (2020). Progress bias versus status quo bias in the ethics of emerging science and technology. *Bioethics*, *34*(3), 252-263. https://doi.org/https://doi.org/10.1111/bioe.12622

Ismail, M. A., Ali, S., Khan, S., Babar, Z., & Mazhar, M. (2021). A Survey of Indian Ocean Region Maritime Security: Technological Advancements and Innovative Solutions. In *2021 International Conference on Frontiers of Information Technology (FIT)* (pp. 66-71).

Johansson, T. M., Dalaklis, D., & Pastra, A. (2021). Maritime Robotics and Autonomous Systems Operations: Exploring Pathways for Overcoming International Techno-Regulatory Data Barriers. *Journal of Marine Science and Engineering*, *9*(6), 594. https://www.mdpi.com/2077-1312/9/6/594

Jowitt, C. E. (1995). *Old worlds and new worlds: Renaissance voyages of discovery* [Doctoral, University of Southampton]. http://eprints.soton.ac.uk/id/eprint/459245

Julian, M. (2000). MARPOL 73/78: the International Convention for the Prevention of Pollution from Ships. *Maritime Studies*, *2000*(113), 16-23. https://doi.org/https://doi.org/10.1080/07266472.2000.10878605

Kamila, M. K., & Jasrotia, S. S. (2023). Ethical issues in the development of artificial intelligence: recognizing the risks. *International Journal of Ethics and Systems*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/IJOES-05-2023-0107

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, *143*, 105138. https://doi.org/https://doi.org/10.1016/j.marpol.2022.105138

Keyuan, Z. (2010). The International Tribunal for the Law of the Sea: Procedures, Practices, and Asian States. *Ocean Development & International Law*, *41*(2), 131-151. https://doi.org/10.1080/00908321003733121

Klein, N. (2021). Maritime autonomous vehicles and international laws on boat migration: Lessons from the use of drones in the Mediterranean. *Marine Policy*, *127*, 104447. https://doi.org/https://doi.org/10.1016/j.marpol.2021.104447

Knudsen, S. (2009). A precautionary tale: Assessing ecological damages after the Exxon Valdez oil spill. *U. St. Thomas LJ*, *7*(1), 95-129. https://heinonline.org/HOL/Page?handle=hein.journals/usthomlj7&div=10&g_sent=1&casa_token=&collection=journals

Lagdami, K., & Fakhry, A. (2020). The Application of Human Rights and Ethics Principles to Self-protection Measures by the Ship Against Pirates and Armed Robbers. In P. K. Mukherjee, M. Q. Mejia, & J. Xu (Eds.), *Maritime Law in Motion* (pp. 389-412). Springer International Publishing. https://doi.org/10.1007/978-3-030-31749-2_18

Lennox-Gentle, T. (2010). Piracy, sea robbery, and terrorism: Enforcing laws to deter ransom payments and hijacking. *Transportation Law Journal*, *37*(3), 199. https://heinonline.org/HOL/P?h=hein.journals/tportl37&i=205

Lieske, D. J., Mahoney, M., Wilhelm, S. I., Weir, L., & O'Hara, P. (2011). Eyes in the sky: a comparative spatial analysis of aerial and satellite surveillance of East Coast Canadian oil pollution. In *Proceedings of the 34th AMOP Technical Seminar on Environmental Contamination and Response* (pp. 244-258).

Lika, R. A., Murugiah, D., Brohi, S. N., & Ramasamy, D. (2018). NotPetya: Cyber Attack Prevention through Awareness via Gamification. In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 1-6).

Lim, S.-M. (1998). Economies of scale in container shipping. *Maritime Policy & Management*, *25*(4), 361-373. https://doi.org/10.1080/03088839800000059

Loewenstein, A. (2023). *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*. Verso Books. https://shorturl.at/dtAST

Luzón-Aguado, V. (2018). Who are the Pirates? Somali Piracy and Environmental Justice in Alakrana, Stolen Seas and Captain Phillips1. *ISLE: Interdisciplinary Studies in Literature and Environment*, *26*(1), 189-210. https://doi.org/10.1093/isle/isy087

Mandal, A., & Ghosh, A. R. (2023). AI-driven surveillance of the health and disease status of ocean organisms: a review. *Aquaculture International*. https://doi.org/10.1007/s10499-023-01192-7

Markoe, G. (2000). *Phoenicians* (Vol. 2). Univ of California Press. https://shorturl.at/glnqS

Martínez, M. A. (2023). Eu borders and potential conflicts between new technologies and human rights. *Peace & Security-Paix et Sécurité Internationales (Euromediterranean Journal of International Law and International Relations)*(11), 7. https://dialnet.unirioja.es/servlet/articulo?codigo=9115695

McKay, F., Williams, B. J., Prestwich, G., Bansal, D., Hallowell, N., & Treanor, D. (2022). The ethical challenges of artificial intelligence-driven digital pathology. *The Journal of Pathology: Clinical Research*, *8*(3), 209-216. https://doi.org/https://doi.org/10.1002/cjp2.263

Mooney, M. (2021). Our Collective Failure: Why the International Community Has Not Intervened to Protect China's Uighur Muslims. *International Research and Review*, *11*(1), 45-64. https://eric.ed.gov/?id=EJ1334449

Moore, M. (2003). *A world without walls: freedom, development, free trade and global governance*. Cambridge University Press. https://rb.gy/2q4mp

Moser, S. C. (2010). Communicating climate change: history, challenges, process and future directions. *WIREs Climate Change*, *1*(1), 31-53. https://doi.org/https://doi.org/10.1002/wcc.11

Oxman, B. H. (2008). The "Tomimaru" (Japan v. Russian Federation). Judgement. ITLOS Case No. 15. *American Journal of International Law*, *102*(2), 316-322. https://doi.org/10.2307/30034542

Papastavridis, E. (2010). II. EUROPEAN COURT OF HUMAN RIGHTS MEDVEDYEV ET AL V FRANCE (GRAND CHAMBER, APPLICATION NO 3394/03) JUDGMENT OF 29 MARCH 2010. *International and Comparative Law Quarterly*, *59*(3), 867-882. https://doi.org/10.1017/S0020589310000345

Pekel, J.-F., Cottam, A., Gorelick, N., & Belward, A. S. (2016). High-resolution mapping of global surface water and its long-term changes. *Nature*, *540*(7633), 418-422. https://doi.org/10.1038/nature20584

Peng, D. C. K. (2005). OIL SPILL PLANNING AND RESPONSE IN A TERRORIST ENVIRONMENT REAL LIFE EXPERIENCES1. *International Oil Spill Conference Proceedings*, *2005*(1), 953-955. https://doi.org/10.7901/2169-3358-2005-1-953

Power, J. (2008). Maritime terrorism: a new challenge for national and international security. *Barry Law Review*, *10*, 111-134. https://heinonline.org/HOL/P?h=hein.journals/barry10&i=113

Raymond, C. Z. (2006). Maritime Terrorism in Southeast Asia: A Risk Assessment. *Terrorism and Political Violence*, *18*(2), 239-257. https://doi.org/10.1080/09546550500383225

Restall, G. (2017). An investigation into learning for ethical leadership in a law enforcement environment. *University of South Australia*, 1-166. https://www.researchgate.net/profile/Haydn-Mccomas/publication/353070654_An_investigation_into_learning_for_ethical_leadership_in_a_law_enforcement_environment/links/60e695121c28af345851337c/An-investigation-into-learning-for-ethical-leadership-in-a-law-enforcement-environment.pdf

Righetti, L., Pham, Q., Madhavan, R., & Chatila, R. (2018). Lethal Autonomous Weapon Systems [Ethical, Legal, and Societal Issues]. *IEEE Robotics & Automation Magazine*, *25*(1), 123-126. https://doi.org/10.1109/MRA.2017.2787267

Rose, C. (2020). The Creation of a Review Mechanism for the UN Convention Against Transnational Organized Crime and Its Protocols. *American Journal of International Law*, *114*(1), 51-67. https://doi.org/10.1017/ajil.2019.71

Salonio, L. J. (2002). The role of the IMO in the maritime governance of terrorism. *World Maritime University*. https://commons.wmu.se/cgi/viewcontent.cgi?article=2264&context=all_dissertations

Sands, P. (2003). *From Nuremberg to the Hague: the future of international criminal justice*. Cambridge University Press. https://shorturl.at/kvOP4

Senarak, C. (2023). Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases. *Maritime Economics & Logistics*. https://doi.org/10.1057/s41278-023-00276-8

Shambaugh, G., Huberts, A., & Zlotnick, A. (2014). Know your enemy: The changing sophistication and success of maritime piracy. *Seton Hall J. Dipl. & Int'l Rel.*, *15*(2), 9. https://heinonline.org/HOL/Page?handle=hein.journals/whith15&div=16&g_sent=1&casa_token=&collection=journals

Singh, K. D. (2015). Creating Your Own Qualitative Research Approach: Selecting, Integrating and Operationalizing Philosophy, Methodology and Methods. *Vision*, *19*(2), 132-146. https://doi.org/10.1177/0972262915575657

Stöhs, J., & Bruns, S. (2018). Maritime Security in the Eastern Mediterranean: Kiel International Seapower Symposium 2017.*ISPK Seapower Series* Baden-Baden.

Suppiah, R. (2009). International Ship and Port Facility Security (ISPS) Code and Crew Welfare. *Maritime Affairs: Journal of the National Maritime Foundation of India*, *5*(1), 57-72. https://doi.org/10.1080/09733150903122057

Şeker, B. Ş. (2018). Maritime Security: Prevention of Maritime Terrorism By International Ship ond Port Security (ISPS) Code. *Journal of Turkish Studies*, *13*(3), 673-690. https://doi.org/https://dx.doi.org/10.7827

Terpsidi, F., Nikitakos, N., & Papachristos, D. (2019). Maritime industry revival through systems digitalization. *J. Multidiscip. Eng. Sci. Technol*, *6*(12), 12. https://www.jmest.org/wp-content/uploads/JMESTN42353215.pdf

Tompkins, E. L., & Amundsen, H. (2008). Perceptions of the effectiveness of the United Nations Framework Convention on Climate Change in advancing national action on climate change. *Environmental Science & Policy*, *11*(1), 1-13. https://doi.org/https://doi.org/10.1016/j.envsci.2007.06.004

Trowers, S. N. (2023). Uncharted Legal Waters: "The Applicability of the Law on Seaworthiness & Good Seamanship to Autonomous Vessels.". In K. Noussia & M. Channon (Eds.), *The Regulation of Automated and Autonomous Transport* (pp. 203-242). Springer International Publishing. https://doi.org/10.1007/978-3-031-32356-0_7

Usluer, H. B. (2022). Development of Naval Cooperation and Guidance for Shipping, Maritime Security Concept in Real Life. *Uluslararasi Akademik Birikim Dergisi*, *5*(3), 100-112. https://doi.org/10.53001/uluabd.2022.33

Wenning, R. J., Apitz, S. E., Baba, A., Citron, M., Elliott, K., Al-Halasah, N., Kapustka, L., Lazarescu, M., Mohamed, M., & Rutjes, R. (2007). Understanding Environmental Security At Ports And Harbors. In I. Linkov, R. J. Wenning, & G. A. Kiker, *Managing Critical Infrastructure Risks* Dordrecht.

Yang, Z., Yu, X., Dedman, S., Rosso, M., Zhu, J., Yang, J., Xia, Y., Tian, Y., Zhang, G., & Wang, J. (2022). UAV remote sensing applications in marine monitoring: Knowledge visualization and review. *Science of The Total Environment*, *838*, 155939. https://doi.org/https://doi.org/10.1016/j.scitotenv.2022.155939

Zuzanna, K., Tomasz, U., Michał, G., & Robert, P. (2022). How High-Tech Solutions Support the Fight Against IUU and Ghost Fishing: A Review of Innovative Approaches, Methods, and Trends. *IEEE Access*, *10*, 112539-112554. https://doi.org/10.1109/ACCESS.2022.3212384

MEUJMAF

Mersin University Journal of Maritime Faculty

CONTENTS

Volume 6 – Issue 1

ARTICLES

MARITIME SECURITY IN A TECHNOLOGICAL ERA: ADDRESSING CHALLENGES IN BALANCING TECHNOLOGY AND ETHICS

Md Syful ISLAM 1

June 2024 Volume: 6 Issue: 1