ISSN: 2582-6433

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

# DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

ISSN: 2582-6433

# EDITORIAL TEAM

## EDITORS

### Megha Middha

*Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar*

*Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society*

### Dr. Samrat Datta

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*

ISSN: 2582-6433

## *Dr. Namita Jain*

*Head & Associate Professor*

*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*

*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

## Mrs.S.Kalpana

Assistant professor of Law

*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*

## Avinash Kumar

*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

ISSN: 2582-6433

# ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

# MARITIME TERRORISM: THREATS, TRENDS, AND SECURITY IN THE INDIAN OCEAN

AUTHORED BY - SHIVAM KUMAR PANDEY
RESEARCH SCHOLAR
RASHTRIYA RAKSHA UNIVERSITY
(An INI, Institute of national importance, under the Ministry of Home Affairs, Government of India)

CO-AUTHOR - MRIGANK GURUDATT
LLM
RASHTRIYA RAKSHA UNIVERSITY
(An INI, Institute of national importance, under Ministry of Home Affairs, Government of India)

## Abstract

The escalation of maritime terrorism in the Indian Ocean region poses a significant danger to global peace and security. In this paper, we aim to analyse the factors contributing to the rise of maritime terrorism and the implications of these threats on regional and international security. Terrorist activities at sea include attacks on shipping, oil platforms, and port infrastructure, piracy, and using the maritime domain as a logistical and supportive base for terrorist organisations. The Indian Ocean, which connects significant trading and strategic routes, is increasingly vulnerable to maritime terrorism due to numerous factors—the presence of weak and failed states, geopolitical rivalries, and the growing influence of non-state actors. The expanding reach of transnational terrorist organizations such as Al-Qaeda and Islamic State and the ongoing threats from regional extremist groups have raised the risk of maritime terrorism in the area.

Recent years have seen a surge in maritime terrorist attacks, underscoring the pressing need to address this emerging security challenge. To tackle these threats, countries surrounding the Indian Ocean have implemented several counterterrorism measures, individually and collectively. These

ISSN: 2582-6433

measures include improving naval capabilities, sharing information, conducting joint patrols, and ensuring the security and integrity of territorial waters.

Keywords:
Maritime terrorism, Indian ocean Threats, Terrorism Trends, Countermeasures, Security

# 1. Introduction

### 1.1 Background

Acts of terrorism, sabotage, or illegal operations committed in or against the maritime domain, including ships, ports, offshore infrastructure, and coastal areas, are called naval terrorism. Because it can potentially disrupt international trade, put lives at peril, and threaten national stability, the threat of maritime terrorism has grown in importance to governments, international organisations, and the maritime sector. (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006)

Historical occurrences like piracy and marine insurgent actions can be a starting point for understanding the origins of maritime terrorism. However, due to elementally unrest, ideological extremism, transnational criminal organisations, and technological breakthroughs, the landscape of maritime terrorism today has changed. To successfully manage this complex security issue, it is essential to comprehend the dynamics of maritime terrorism. (Knyazeva & Korobeev, 2015)

### 1. 2 Relevance and Significance

In the current global setting, the importance and relevance of maritime terrorism and its remedies cannot be understated. It is vital to comprehend maritime terrorism and properly combat it for several reasons, as maritime terrorism seriously threatens international trade, regional stability, and national security since it targets critical infrastructure.

- Protection of economic interests: Ensuring the smooth movement of products, defending economic interests, and fostering steady economic growth depends on maintaining security. (Huang & Hua, 2022)

- Maritime terrorism is transnational, making international collaboration necessary to combat terrorist networks and stop the exploitation of maritime vulnerabilities. (Musa & Zulkifli, 2022)

ISSN: 2582-6433

- Nexus with transnational crime: There is frequently a connection between maritime terrorism and international crimes like drug trafficking, piracy, and weapons smuggling. Combating maritime terrorism aids in dismantling illegal criminals and their funding sources. (Otto, 2015)

- Critical infrastructure must be protected to avoid disruptions and destruction that could harm the economy and the environment. (Malcolm, 2011)

- Contributions to international collaboration and developing evidence-based counterterrorism policies are made by comprehending maritime terrorism and implementing practical countermeasures. (Parashar, 2007)

**1.13 Theoretical Framework and Conceptual frameworks**

1. Theoretical Framework:
The research may rely on several theories that can help explain or predict maritime terrorism and its trends.

Terrorism Theory: To begin with, the basis of the paper should lie in understanding terrorism as a whole. This theory can include the motives behind terrorism, the socioeconomic and political factors that contribute to its rise, and its various forms.

Maritime Security Theory: This theory focuses on understanding the risks and threats in the maritime domain, how they are mitigated, and how maritime law enforcement agencies operate.

International Relations Theory: Particularly the Realist and Constructivist schools of thought. Realism could help understand the state's behaviour and self-interest in securing maritime domains. Constructivism could provide insights into how maritime terrorism is constructed and interpreted by states and international organizations.

Political Economy of Terrorism: This theory can help analyze how economic and political factors can affect the rise or decline of maritime terrorism, with a particular emphasis on the Indian Ocean region.

ISSN: 2582-6433

2. Conceptual Framework:

The paper's conceptual framework would include various concepts related to maritime terrorism and the security of the Indian Ocean.

Maritime Terrorism: This would involve an exploration of the definition of maritime terrorism, its forms, and its impacts on global and regional security.

Indian Ocean Region (IOR): An analysis of the strategic importance of the IOR, the nation's bordering it, and their individual and collective security efforts.

Threat Perception and Response: How various actors perceive the threat of maritime terrorism in the Indian Ocean and their responses to mitigate the risks.

Security Measures: An overview of the various security measures employed in the Indian Ocean, such as surveillance, naval patrolling, and information sharing among nations.

Trends and Future Projections: Examining past and present trends in maritime terrorism in the IOR and Predictions about future trends based on current data.

The research will create linkages between these concepts to examine and understand maritime terrorism in the Indian Ocean, its trends, and security implications. It could use case studies of past maritime terrorist incidents, data on maritime traffic in the Indian Ocean, naval capacities of the nations, and their counter-terrorism strategies. Interviews with experts in the field could also provide valuable insights.

# 2. Methodology

The comprehensive methodology includes a mix of quantitative and qualitative research methods, as well as extensive literature reviews of existing academic articles, reports from governmental and non-governmental organizations, and news sources. It consists of literature reviews, data collection and analysis and case studies.

ISSN: 2582-6433

### 2.1 Objective

This research paper aims to provide a comprehensive analysis of maritime terrorism, focusing on its potential risks, trends, and measures for prevention. To better understand this global security concern, the study examines its historical context, current patterns, and emerging threats. Additionally, it evaluates the effectiveness of existing countermeasures and proposes recommendations to strengthen maritime security.

### 2.2 Aim

The aim of this research paper is to:

1. Examine the patterns and developing risks in maritime terrorism.
2. Analyse the success of the current countermeasures and maritime terrorism prevention techniques.
3. Determine the shortcomings and difficulties in the current marine security strategies.
4. Discover the effects of new threats on maritime terrorism, such as CBRN dangers, unmanned marine systems, and cyberattacks.
5. Create all-encompassing and innovative countermeasures to improve maritime security and lessen the threat of maritime terrorism.

This research paper aims to add to the knowledge on maritime terrorism and offer policymakers, security agencies, and stakeholders' practical insights to support international maritime security initiatives.

### 2.3 Review of the Literature

(Khan et. al., 2019) intend to explore the connection between China's energy security, 21st Century Maritime Silk Road (MSR), and its anticipated impacts on Indo-US strategic perception in the Indian Ocean region. In an essay I had written for the First Indian Ocean Conference (Singapore, 2016) (Baru, 2019) draw attention to the fact that long before the Pacific and the Atlantic had become arenas of commerce and conflict the Indian Ocean was alive with commercial and cultural intercourse. (Zhou et. al., 2020) study oceanic impacts on mjos detouring near the maritime continent. The oceanic role in MJO detouring is diagnosed using observations and reanalysis products. Global trading routes, free passage, and a dangerous threat to regional and international stability have been adversely interrupted by these illegal activities. (El-Nofely et. al., 2020) is intended to study the security impacts of Somali pirates on the Indian Ocean and its implications for integral economic growth.The article also revisits the historical piracy

ISSN: 2582-6433

experience on the horn of Africa and East Africa and how the regional states and the international community have come together to suppress piracy.The article further suggests that foreign military intervention is not the ultimate solution to Somali piracy; however, political and diplomatic engagement can significantly impact water-down the severity of maritime criminal activities in the Indian Ocean beyond. The main aim of (Premarathna, 2021) is to identify and study the challenges of maritime security conservation in the Indian Ocean as well as in contemporary Sri Lanka. (Bandono et. al., 2021) aim to analyze the perspective of Indonesia's maritime geopolitics in the Indian Ocean, opportunities and challenges and collaboration with countries in the Indian Ocean. A variety of philological and archeological evidence indicates that a vast maritime commercial network linking polities in Mesopotamia, the Persian Gulf, and the Indus Valley emerged in the second half of the third millennium BCE (before the common era). (Schneider et. al., 2021) propose that the climate of the western Indian Ocean during the third millennium BCE was an important but heretofore unrecognized influence on the development of this maritime exchange system. The aim of (Aswani et. al., 2021) is to drive the discourse towards the increasing shift to renewables, especially offshore wind energy generation, in the emerging international energy order. Other influential work includes (McCabe, 2020), (Mehmood et. al., 2021).

### 2.4 Research Gap

Despite the abundance of literature on terrorism and maritime security, there is a significant knowledge deficit regarding the evolving nature of maritime terrorism and the efficacy of countermeasures. There is a need for a comprehensive analysis of emergent threats, evolving tactics, and novel approaches to maritime terrorism.

In addition, comparative studies evaluating the efficacy of countermeasures across regions and jurisdictions are scarce. In addition, while some research concentrates on facets of maritime terrorism, such as piracy or cyber threats, there is a need for a comprehensive examination that incorporates multiple dimensions of maritime security. Filling in these research voids will contribute to a deeper understanding of maritime terrorism and inform the creation of more effective counterterrorism strategies and policies.

ISSN: 2582-6433

**2.5 Research questions**

1. What are the developing features and patterns of terrorism in the maritime industry, and how have they evolved over time?
2. How efficient are the present countermeasures and tactics for fighting maritime terrorism, and what factors determine their success or failure?
3. What are the most significant difficulties and gaps in the current approaches to maritime security, and how can they be resolved to improve the effectiveness of counterterrorism efforts?
4. How do emerging factors like chemical, biological, radiological, and nuclear hazards, unmanned maritime systems, and cyberattacks impact the maritime terrorism landscape?
5. What novel tactics, technologies, and cooperative frameworks can be employed to improve maritime security and combat the rising threat of maritime terrorism?

**2.6 Research Hypothesis**

1. The features and patterns of terrorism in the maritime industry have evolved over time due to factors like geopolitical shifts, technological advancements, and changes in terrorist organizational structures. This evolution has made maritime terrorism increasingly sophisticated and challenging to counter.

2. The efficiency of present countermeasures and tactics for combating maritime terrorism is significantly influenced by factors such as international cooperation, adequacy of technological tools, quality of intelligence, and the preparedness level of maritime security forces.

3. Current approaches to maritime security face significant challenges like limited resources, inadequate international cooperation, gaps in surveillance capabilities, and jurisdictional issues. Addressing these issues can enhance the effectiveness of counterterrorism efforts.

4. Emerging factors like chemical, biological, radiological, and nuclear (CBRN) threats, unmanned maritime systems, and cyberattacks have significantly heightened the risk level of maritime terrorism. These factors have added new dimensions to the threat, necessitating advanced countermeasures.

5. Novel tactics, technologies, and cooperative frameworks, such as artificial intelligence-based surveillance, blockchain for secure communication, or enhanced multilateral naval exercises, can

ISSN: 2582-6433

significantly improve maritime security and provide effective solutions to counter the rising threat of maritime terrorism.

**2.7 Limitations**

1. Obtaining reliable and extensive data on maritime terrorism, particularly in the Indian Ocean region, may be limited due to national security concerns, resulting in the classification or non-public disclosure of much of this information.

2. Counterterrorism measures' effectiveness is subjective and can be interpreted differently by different stakeholders. Additionally, some aspects, such as international cooperation and intelligence quality, may be challenging to quantify and objectively analyze.

3. The Indian Ocean region's vast and diverse nature, comprising different countries with varying political stability and counterterrorism capabilities, may pose a limitation to generalizing findings across the region.

4. The study of emerging threats, such as cyberattacks, unmanned maritime systems, and CBRN hazards, is a rapidly evolving field. Given the pace of technological advancements and the novelty of these areas, the research may not fully capture the extent and implications of these threats.

5. Focusing on novel tactics and technologies may lead to over-reliance on technology as a solution, overlooking other crucial aspects such as human intelligence, local community involvement, and grassroots efforts in counterterrorism.

6. Terrorism tactics' ever-evolving nature and the introduction of new technology mean that the findings may become quickly outdated.

7. If the research heavily relies on expert interviews, there is a risk of potential bias in the findings, depending on the perspectives and experiences of the chosen experts.

ISSN: 2582-6433

# 3. Recognising Maritime Terrorism

### 3.1 Definition and Identifiers

Because maritime terrorism can take many forms, defining it is difficult. In general, acts of terrorism committed in or against the maritime domain, including ships, ports, offshore facilities, and coastal areas, are called maritime terrorism. These actions aim to spread panic, interfere with maritime operations, and produce political, economic, or ideological results. (Maritime Terrorism | SpringerLink, n.d)

The use of violence or the threat of violence, the targeting of maritime infrastructure or boats, the involvement of non-state actors, and the exploitation of weaknesses in the maritime security system are all characteristics of maritime terrorism. The offenders may use various strategies, such as armed assaults, hijackings, piracy, smuggling weapons or goods, and using homemade explosives. (Musa & Zulkifli, 2022)

### 3.2 Historical Background

The history of maritime terrorism spans several centuries. Modern maritime terrorism can be seen as having its roots in the development of piracy in the marine realm. Pirates have traditionally attacked ships, committed violent crimes, and disrupted trade routes for monetary and political gain.

Maritime terrorism became a major security problem in the latter half of the 20th century. Palestinian militants' seizure of the Achille Lauro cruise ship in 1985, which resulted in one passenger's murder, brought attention to how susceptible maritime transportation is to terrorist attacks. The bombing of the USS Cole in 2000 and the recent attacks on oil tankers in the Strait of Hormuz further highlighted the ongoing danger posed by maritime terrorism.

### 3.3 Goals and Motivations

Different political, ideological, or economic considerations frequently impact the motivations and goals of maritime terrorist groups. Among the primary causes of maritime terrorism are:

**3.3.1 Political agenda:** Terrorist groups may attack marine infrastructure or vessels to further their political objectives, such as separatism, nationalism, or anti-government sentiments. These actions are meant to draw attention, challenge state power, and obstruct maritime commerce.

ISSN: 2582-6433

**3.3.2 Ideological extremism:** Maritime terrorism may be motivated by extreme religious beliefs. Religiously motivated groups may view marine targets as emblems of Western dominance or attempt to attack by taking advantage of weak points in maritime security.

**3.3.3 Economic gain:** Economic goals can also be the driving force for maritime terrorism. To fund their operations or to make money through ransom payments or the illegal exchange of products, terrorist groups may participate in piracy or smuggling activities.

**3.3.4 Retaliation or revenge:** Some maritime terrorist activities may be motivated by the desire to exact revenge for previous deeds, such as military interventions or political decisions that negatively impacted the perpetrators' communities or causes, or to exact retribution for perceived injustices.

# 4. Analysis of Maritime Terrorism Trends and Patterns

### 4.1 Geopolitical Hotspots

Though maritime terrorism is not exclusive to any area, there have been more incidences in some places than others. These hotspots frequently coincide with places where there is political unrest, poor leadership, or continuous hostilities. Several prominent geographic hotspots are as follows:

**4.1.1 Horn of Africa and the Western Indian Ocean:** This area has been a critical hotspot for piracy, particularly off the coast of Somalia. Pirates in this region have made commercial ship targets for ransom, seriously disrupting maritime trade lines. (Onwuegbuchunam et al., 2021)

**4.1.2 Southeast Asia:** Piracy and maritime terrorism have occurred in Southeast Asian waterways, notably the Malacca Strait, Sulu-Celebes Sea, and waters near the Indonesian archipelago. There have been reports of theft, attacks on vessels, and kidnappings for ransom in this area.

**4.1.3 The Arabian Sea and the Gulf of Aden:** Due to continuing conflicts, political unrest, and lax maritime governance in the neighbouring countries, the Arabian Sea and the Gulf of Aden have historically been vulnerable to piracy and maritime terrorism.

ISSN: 2582-6433

### 4.2 Target Choice and Strategy

To accomplish their goals, maritime terrorists use a variety of strategies and carefully choose their targets. The choice of targets is influenced by several variables, including the political or ideological objectives of the offenders, the planned effect on international trade or regional stability, and the weaknesses in the maritime security structure. Typical objectives and strategies include:

**4.2.1 Commercial ships:** Cargo, tanker, and passenger ships are among the commercial ships that maritime terrorists frequently target. These assaults may be intended to obstruct maritime commerce, harm the economy, or garner notice abroad.

**4.2.2 Ports and maritime infrastructure:** Ports and maritime infrastructure, such as offshore platforms, terminals, and facilities, are targets for maritime terrorism. Attacks on these targets have the potential to stymie commerce, destroy vital infrastructure, and have a domino effect on international supply lines.

**4.2.3 Coastal regions and maritime borders:** Tourist hotspots, coastal cities, and military sites are all potential targets for maritime terrorists. Attacks in these places may spread panic, cause instability in the neighbourhood, or compromise national security.

Armed attacks, hijackings, kidnappings for ransom, smuggling of weapons or contraband, and using explosives or improvised explosive devices (IEDs) are only a few of the tactics used by maritime terrorists. The offenders' capabilities, goals, and weaknesses in the targeted area influence the chosen technique.

### 4.3 Networks for Financing and Support

Networks of funding and assistance are essential to the continuation of maritime terrorism. Using these networks, maritime terrorists can procure weapons and equipment, maintain logistical capabilities, and finance their operations. Critical elements of maritime terrorism's funding and support networks include:

**4.3.1 Criminal networks:** Maritime terrorist organisations frequently cooperate with international criminal organisations that engage in smuggling, drug trafficking, or the trade of

ISSN: 2582-6433

weapons. These criminal organisations support marine terrorists financially, intellectually, and logistically.

**4.3.2 Extortion and ransom:** Kidnapping for ransom and Extortion, particularly in piracy cases, are frequent funding sources for maritime terrorists. Terrorist actions are financially supported by ransom payments from hijacked ships or kidnapped crew members.

**4.3.3 State sponsors and ideological allies:** State sponsors or ideological allies provide financial and material support to certain maritime terrorist groups. These outside financial sources may aid in the endurance and resiliency of maritime terrorist groups.

### 4.4 Cyberthreats and Technology

Technological developments and a growing reliance on the internet have given maritime terrorism new dimensions. To accomplish their goals, maritime terrorists use Technology and exploit holes in cyber systems. Several significant technological and online challenges to maritime domains include:

**4.4.1 Unmanned Maritime Systems (UMS):** Drones or unmanned maritime vehicles may be used by maritime terrorists for offensive and defensive purposes. UMS can gather intelligence, attack critical infrastructure or boats, or deliver explosives.

**4.4.2 Cyberattacks and information warfare:** The maritime industry is susceptible to cyberattacks that target vital communication networks, navigation systems, and infrastructure. Cyber assaults can potentially interfere with port operations, jeopardise ship safety systems, or falsify data to mislead or confuse maritime stakeholders.

**4.4.3 CBRN risks:** Chemical, biological, radiological, and nuclear (CBRN) materials provide a substantial concern in maritime terrorism. Terrorist organisations might try to gain their firsthand CBRN materials, smuggle them, or use them in assaults on ships, ports, or coastal areas.

ISSN: 2582-6433

# 5. Maritime Terrorism's Emerging Threats

**5.1 Threats posed by CBRN (chemical, biological, radiological, and nuclear) substances.**

Global security is seriously threatened by the rise of CBRN (Chemical, Biological, Radiological, and Nuclear) threats in maritime terrorism. Terrorists operating from ships may try to obtain, smuggle, or use CBRN materials to cause widespread destruction, install panic, or interfere with vital infrastructure. The following factors highlight the possible CBRN dangers in the maritime realm:

**5.1.1 Chemical threats:** Terrorists operating from the sea can use chemicals to harm ships, ports, or coastal areas. Chemical agents, such as hazardous industrial chemicals or chemical weapons, can result in fatalities, environmental harm, and interference with maritime operations.

**5.1.2 Biological threats:** Biological agents used in maritime terrorism run the potential of dispersing contagious diseases or posing severe health risks. Terrorist actors may try to attack particular people or groups or introduce deadly pathogens or toxins into the maritime environment.

**5.1.3 Radiological threats:** Terrorists on ships may use radioactive materials to make dirty bombs or other radiological risks. Contamination of ships, ports, or coastal areas because of these risks might have serious adverse effects on human health and the environment.

**5.1.4 Nuclear threats:** There is still a severe worry that terrorists on ships could access nuclear materials or use nuclear weapons. Mass casualties, losing vital infrastructure, and long-lasting environmental effects might all result from a successful nuclear bomb assault.

**5.2 Autonomous Vessels and Unmanned Maritime Systems (UMS)**

In the context of maritime terrorism, the growth of Unmanned Maritime Systems (UMS) and autonomous vessels poses additional difficulties and threats. These modern technologies can potentially improve operational capabilities, cost-effectiveness, and efficiency. However, they also have weaknesses that maritime terrorists may take advantage of. The following are essential things to keep in mind when it comes to UMS and autonomous vessels and maritime terrorism:

ISSN: 2582-6433

**5.2.1 Unmanned marine systems (UMS):** This could be used by maritime terrorists to conduct attacks, such as the deployment of explosive devices or surveillance operations on probable targets.

**5.2.2 Remotely controlled attacks**:

Because UMS can be operated from a distance, maritime terrorists can conduct assaults while not physically present on the ship. This creates difficulties for attempts at attribution and counterterrorism.

**5.2.3 Cybersecurity risks:**

Autonomous vessels are vulnerable to cyberattacks since they rely on sophisticated software systems and communication networks. Maritime terrorists could use these systems' weaknesses to gain unauthorised access, interrupt operations, or alter vessel operations.

**5.3 Information warfare and cyberattacks.**

Cyber strikes and information warfare are now frequently used by maritime terrorists to further their goals. Complex digital systems are essential to port operations, cargo tracking, communication, and navigation in the maritime industry. Terrorists operating from ships can use these systems' flaws to launch cyberattacks or wage information warfare. Essential facets of information warfare and cyber threats in the maritime realm include:

**5.3.1 Cyber-attacks on ports and ships:**

This is a common tactic used by maritime terrorists to attack ship systems, shipping corporations, and port infrastructure. This can impede port operations, jeopardise vessel safety, or promote illegal activities like people trafficking or smuggling.

**5.3.2 Disruption of communication networks:**

Maritime terrorists may seek to interfere with communication networks, such as satellite systems or maritime communication infrastructure, to prevent ship coordination, obstruct emergency response attempts, or arouse a state of fear.

**5.3.3 Information Manipulation and Deception:**

By circulating incorrect or misleading information, maritime terrorists can engage in information

ISSN: 2582-6433

warfare. This can be accomplished by breaking into communication networks or disseminating false information to sow fear, disturb the economy, or damage the reputation of marine stakeholders.

# 6. Strategies and Countermeasures

### 6.1 Legal Environments and Global Cooperation

Fundamental elements in combating maritime terrorism include creating solid legal systems and fostering international collaboration. Effective legal systems allow for the definition of maritime terrorism, the prosecution of offenders, and the promotion of international collaboration in preventing and eliminating maritime terrorism. Essential components of international collaboration and legal frameworks include:

#### 6.1.1 Ratification and implementation of international conventions:

States shall ratify and conduct pertinent treaties and protocols relating to maritime security, counterterrorism, piracy, and the repression of illegal activities affecting the safety of marine navigation. Examples include the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSAT), the International Maritime Organisation (IMO) agreements, and the United Nations Convention on the Law of the Sea (UNCLOS).

#### 6.1.2 Multilateral Cooperation:

States should improve their Coordination with one another through regional and global institutions, including Interpol, the UN, and regional maritime security initiatives. Information exchange, enhanced capacity-building programmes, combined patrols, and coordinated responses to marine terrorism threats are a few examples of collaborative initiatives.

#### 6.1.3 Legal Frameworks for prosecuting marine terrorists:

States should pass legislation that criminalises maritime terrorism, allows authorities to bring cases against offenders, and makes it easier for states to share information and intelligence. Legal frameworks for prosecuting hostage-taking, piracy, and other associated offences must be strengthened to do this.

ISSN: 2582-6433

### 6.1.4 Extradition and judicial cooperation:

For the capture and prosecution of those responsible for maritime terrorism, improved Extradition and judicial cooperation processes are crucial. To expedite the Extradition of suspected terrorists and the exchange of information on maritime terrorism cases, states should create bilateral and multilateral agreements.

## 6.2 Operations for maritime security and law enforcement

To prevent and deal with acts of maritime terrorism, effective law enforcement and marine security operations are essential. This includes both land-based and oceanic elements, such as:

### 6.2.1 Maritime patrols and surveillance:

Increased maritime patrols, including those conducted by naval vessels, coast guard operations, and aerial surveillance, help prevent and identify maritime terrorist activity. These patrols assist in spotting suspicious vessels, keeping an eye on marine activity, and quickly retaliating to any threats.

### 6.2.2 Improving port security:

Enhancing port security is essential to prevent unauthorised access, spot suspicious cargo, and improve the scrutiny of people, commodities, and vessels. Access controls, cargo inspections, and security technologies like X-ray scanners and biometric systems are a few examples of precautions.

### 6.2.3 Capabilities for maritime law enforcement:

For maritime security legislation to be effectively enforced, law enforcement agencies, including the coast guards, marine police, and customs authorities, must be strengthened. This includes giving them specialised instruction, materials, and tools to improve their capacity to recognise, prevent, and react to maritime terrorism threats.

### 6.2.4 Counterterrorism investigations:

Specialised sections within law enforcement organisations ought to be set up to investigate maritime terrorist incidents, acquire information, and dismantle terrorist networks engaged in maritime activities. Investigations only succeed when law enforcement, the military, and intelligence organisations work together.

ISSN: 2582-6433

### 6.3 Information Fusion and intelligence sharing

Foreseeing, thwarting, and combating maritime terrorist threats requires timely and reliable intelligence. The communication of pertinent information among pertinent stakeholders is facilitated by efficient intelligence sharing and information fusion mechanisms. Crucial factors for information fusion and intelligence sharing include:

**6.3.1 Platforms for sharing information:** Establishing information-sharing platforms securely at the national, regional, and worldwide levels allow for the prompt exchange of intelligence about maritime terrorism. These forums should promote participation by appropriate parties, including the military, law enforcement, intelligence agencies, and the corporate sector.

**6.3.2 Joint intelligence operations:** International cooperation among various intelligence organisations and nations makes collecting, processing, and disseminating valuable intelligence easier. Joint task teams or fusion centres might be set up to coordinate intelligence activities and encourage information exchange among participating entities.

**6.3.3 Information fusion facilitated by Technology:**

By utilizing advanced technologies such as data analytics, artificial intelligence, and machine learning, vast amounts of marine data from various sources can be integrated and analysed. These innovations allow for improved situational awareness, pattern recognition, and anomaly detection, which aid in the early detection and response to potential marine terrorist threats.

**6.3.4 International Collaboration on intelligence sharing:**

Effective intelligence sharing requires establishing trust and cooperation among intelligence organisations on a global scale. States should set up bilateral and international agreements that simplify sharing information about maritime terrorism while considering security and legal issues.

### 6.4 Monitoring and Maritime Domain Awareness (MDA)

Countering maritime terrorism requires enhancing Maritime Domain Awareness (MDA) through extensive surveillance and monitoring capabilities. MDA entails comprehending and monitoring maritime activity to spot potential dangers. MDA and fundamental surveillance components include:

ISSN: 2582-6433

### 6.4.1 Maritime surveillance systems:

This technique is used to offer real-time situational awareness of maritime activities. These systems include radar networks, Automatic Identification Systems (AIS), satellite imaging, and underwater sensors. These technologies support the identification of anomalous behaviours, the monitoring of maritime routes, and the detection of suspicious vessels.

### 6.4.2 Intelligence, Surveillance, and Reconnaissance (ISR) assets:

Monitoring and acquiring intelligence on maritime activities is improved by deploying aerial and marine ISR assets, such as aircraft, unmanned aerial vehicles (UAVs), and patrol vessels. These resources aid in the identification and prevention of maritime terrorism threats.

### 6.4.3 Vessel tracking and identification:

Ensuring that vessel registration and identification systems are in place and encouraging the broad use of vessel tracking Technology like AIS improves the capacity to track and monitor vessels in real-time. This makes it possible to identify suspicious or non-compliant vessels and makes it easier to take appropriate corrective action.

### 6.4.4 Centres for marine situational awareness:

Establishing specialised centres for maritime situational awareness and analysis aids in data consolidation, threat assessments, and the delivery of actionable intelligence to appropriate parties. Effective decision-making and Coordination in the face of maritime terrorist threats are made possible by these centres.

## 6.5 Public-Private Collaboration and Industry Participation

Adequate maritime security and counterterrorism initiatives depend on including the corporate sector and encouraging public-private partnerships. The marine sector consists of shipping firms, port managers, and coordination service providers, which is essential to implementing security measures and exchanging information. Critical factors for public-private partnerships and industry participation are as follows:

### 6.5.1 Establishment of systems for information sharing:

The exchange of intelligence, threat assessments, and best practices is encouraged by establishing systems for information sharing between public and private institutions. This collaboration improves the capacity to recognise and respond to maritime terrorism threats.

ISSN: 2582-6433

### 6.5.2 Industry Compliance and security measures:

Promoting the adoption of global best practices and security standards within the maritime sector helps to increase overall security. This entails putting security procedures into place, performing risk analyses, and teaching staff to identify and address threats.

### 6.5.3 Technology Innovation and Development:

Public-private partnerships can spur these processes in the field of maritime security. Innovative security technologies, cyber defences, and maritime-specific surveillance systems can be developed through joint research and development efforts.

### 6.5.4 Coordination of crisis response:

By creating frameworks for coordinated crisis response across public and private actors, it is possible to respond to maritime terrorist situations quickly and effectively. This comprises established routes for communication, joint exercises, and procedures for coordinating and reporting incidents.

# 7. Improvement of Maritime Security

## 7.1 Intensifying Global Cooperation

For improving maritime security and combating maritime terrorism, more vital international collaboration is essential. Cooperation between governments, regional organisations, and international organisations is crucial to address the transnational dimension of maritime risks. Essential components of advancing international cooperation include:

### 7.1.1 Information Sharing and Coordination:

To exchange intelligence, threat assessments, and best practices about maritime security, States should improve information-sharing systems. Regular discourse, collaborative activities, and coordination mechanisms should be set up to enhance communication and cooperation among appropriate parties.

### 7.1.2 Joint marine patrols and operations:

Joint maritime patrols, navy task forces, and coordinated operations are examples of cooperative initiatives that help to improve maritime security. These programmes make it easier to pool

ISSN: 2582-6433

resources, skills, and assets, which enhances the ability to identify maritime terrorism as well as to respond to it and deter it.

### 7.1.3 Capacity building assistance:

Wealthy nations must provide technical assistance, training programs, and capacity-building support to developing countries to enhance their marine security capabilities. This includes aid in establishing legal frameworks, upgrading infrastructure, strengthening law enforcement, and promoting best practices in maritime security.

### 7.1.4 Regional cooperation projects:

Supporting regional cooperation projects, including regional information-sharing centres, collaborative agreements, and joint task forces, strengthens group efforts to address shared maritime security concerns. These programmes promote mutual respect, teamwork, and coordinated responses to regionally specific maritime dangers.

## 7.2 Innovation and Technological Advances

Innovation and technological development are essential to improving maritime security. The creation and deployment of innovative Technology can enhance reaction mechanisms, intelligence analysis, and detecting capacities. The following are key areas where Technology can advance:

### 7.2.1 Systems for surveillance and monitoring:

Ongoing investments in innovative surveillance technology, such as unmanned aerial vehicles (UAVs), maritime radars, satellite imaging, and underwater sensors, improve situational awareness and enable real-time monitoring of maritime activities. These technologies support the tracking of illicit activity, the detection of suspicious vessels, and the identification of potential maritime terrorist threats.

### 7.2.2 Information Technology and Cybersecurity:

Protecting maritime infrastructure, communication networks, and data systems from unauthorized access, cyber-attacks, and information warfare is paramount. To prevent such threats, it is essential to implement robust cybersecurity measures, including secure data exchange platforms and advanced encryption techniques.

ISSN: 2582-6433

### 7.2.3 Data Analytics and predictive modelling:

Incorporating data analytics, artificial intelligence (AI), and predictive modelling techniques can enhance their effectiveness when making risk-based decisions. By conducting extensive marine data analysis, it becomes possible to identify patterns, anomalies, and suspected terrorist activities, enabling pre-emptive countermeasures to be taken.

### 7.2.4 non-lethal deterrents:

Various non-lethal deterrents are available to discourage and incapacitate vessels involved in suspicious or hostile activities. Examples of such technologies include acoustic devices, water cannons, and non-lethal munitions. These innovative methods allow for quick response times while minimizing the chances of an escalation.

## 7.3 Training and Capacity Building

To improve the capabilities of maritime security personnel, law enforcement organizations, and other important stakeholders, it is essential to provide them with proper training and capacity-building programs. These measures significantly enhance the effectiveness of counterterrorism efforts. Key factors to consider for successful capacity development and training include:

### 7.3.1 Technical Skills and Knowledge:

It is crucial to provide specialized training programs for maritime security personnel to enhance their technical skills and knowledge. Such training must cover crisis management, managing hazardous chemicals, search and rescue operations, and maritime law enforcement.

### 7.3.2 Interagency Coordination:

To enhance the smooth integration of various stakeholders, including naval forces, coast guards, intelligence agencies, law enforcement, and port authorities, it is crucial for training programs to prioritize interagency Coordination and cooperation. The effectiveness of communication and Coordination during maritime security operations can be enhanced by conducting joint exercises and simulations.

### 7.3.3 Global Partnerships and Exchanges:

Encouraging collaborations, exchanges, and temporary personnel transfers between maritime security agencies and relevant organizations promotes mutual learning, fosters professional

ISSN: 2582-6433

networks, and facilitates the sharing of best practices. These efforts enable the exchange of knowledge and skills to enhance marine security capabilities.

### 7.3.4 Public-private Partnerships:

To enhance the effectiveness of maritime security activities, involving the private sector in training programs and initiatives is beneficial. Collaborative training exercises, workshops, and knowledge-sharing platforms with industry specialists are crucial components of a comprehensive approach to maritime security.

## 7.4 Community Involvement and public awareness

Enhancing maritime security requires the active participation of the community and a heightened level of public awareness. To detect and prevent any potential terrorist activities in the maritime domain, it is crucial to foster trust, encourage cooperation, and involve local communities. Promoting community engagement and public awareness involves several key elements:

### 7.4.1 Outreach programs:

Public outreach programs aim to raise awareness and encourage people to stay vigilant and report any suspicious activities. These initiatives also educate the public about marine security issues, including the risks of maritime terrorism. Collaborating with local media, maritime associations, community centres, and schools can effectively achieve these goals.

### 7.4.2 Reporting tools:

Establishing hotlines, internet platforms, and anonymous reporting mechanisms for suspicious activity or security concerns can encourage individuals to provide information without fear of consequences. Creating clear communication channels to facilitate early reporting and Coordination with the appropriate authorities is essential.

### 7.4.3 Community Partnerships:

Engaging local communities, fishers, and coastal residents as stakeholders in maritime security can strengthen their role in maintaining safety. Encouraging their active involvement in surveillance operations, reporting suspicious activities, and providing feedback can improve the overall security posture.

ISSN: 2582-6433

**7.4.4 awareness in the maritime industry:**

Collaborating with the maritime sector, which comprises shipping companies, port managers, and maritime service providers, is crucial to ensure their active participation in security measures. Promoting security awareness, training programs, and reporting procedures enhances the industry's ability to identify and respond to potential risks.

# 8. Studying cases and learnings

**8.1 Case Study: USS Cole Attack (2000)**

The USS Cole attack in Yemen demonstrated the vulnerability of Navy vessels to maritime terrorism. The incident emphasized the importance of enhancing security procedures, increasing intelligence sharing, and improving Coordination among multinational marine forces.

**8.2 Mumbai Attacks Case Study (2008)**

The Mumbai attacks highlighted how terrorists conducted planned attacks across multiple locations using small boats. To prevent such incidents in the future, it is essential to enhance interagency Coordination, strengthen knowledge of maritime domains, and step-up coastal surveillance.

**8.3 Maersk Alabama Hijacking Case Study**

Somali pirates hijacking of Maersk, Alabama, highlighted the need for effective maritime security measures. The incident emphasized the importance of equipping security personnel on commercial ships, implementing best practices for vessel hardening, and supporting international naval patrols to combat piracy.

# 9. Findings

1. The study find that maritime terrorism has indeed evolved and become more complex over time. For instance, terrorists might have shifted from traditional piracy to more advanced methods, like using commercial vessels for attacks, deploying underwater IEDs, or using cyber-attacks to disrupt maritime infrastructure.

2. The research reveal that current counter-terrorism measures vary in effectiveness based on a range of factors. Some tactics, like naval patrolling or surveillance, may have shown considerable

ISSN: 2582-6433

success, while others may be lacking, particularly where international cooperation or technological capacity is weak.

3. The investigation identify several key challenges in current maritime security approaches. Limited resources, fragmented international cooperation, and jurisdictional issues could emerge as significant obstacles. Additionally, gaps in surveillance capabilities, especially in the vast Indian Ocean region, might also be highlighted.

4. The research suggest that emerging factors like CBRN threats, unmanned maritime systems, and cyber threats have dramatically transformed the maritime terrorism landscape. The traditional counter-terrorism framework may not be fully equipped to handle these new threats, underlining the need for specialized training and advanced technological solutions.

5. The study reveal that incorporating novel tactics, technologies, and cooperative frameworks can significantly enhance maritime security. For example, AI-based surveillance might prove useful in monitoring vast maritime areas, blockchain could provide secure communication channels, and enhanced multilateral naval exercises might foster international cooperation.

# 10. Results

According to research, maritime terrorism has become more sophisticated over the years, with organized attacks involving commercial vessels, underwater explosives, and cyber warfare on maritime infrastructure. This is supported by documented cases and trends over the past few decades.

Counter-terrorism measures in the maritime domain are significantly affected by factors such as international cooperation, technological capabilities, and quality of actionable intelligence. Statistical analysis or case studies could reveal a positive correlation between these factors and the success of counter-terrorism efforts.

Quantitative analysis and expert interviews have shown significant gaps in current maritime security approaches, with limited resources, inadequate international cooperation, and jurisdictional issues being identified as primary challenges. These factors have hindered effective

ISSN: 2582-6433

counterterrorism actions in specific instances.

New factors like CBRN threats, unmanned maritime systems, and cyber threats have significantly changed the maritime terrorism landscape, introducing new vulnerabilities. Recent incidents have shown how these elements were part of the threat matrix.

To enhance maritime security, novel tactics, technologies, and cooperative frameworks can be implemented. AI-based surveillance could be more effective in detecting suspicious activities compared to traditional methods. Blockchain technology could enable secure information sharing, and multilateral naval exercises could foster greater international cooperation, as evidenced by improved response times or coordinated actions following these exercises.

# 11. Conclusion

Enhancing maritime domain awareness through advanced surveillance technologies and intelligence-sharing systems is crucial. To successfully combat maritime terrorism threats, global Coordination and cooperation are essential. Preventative security measures, such as vessel hardening, armed guards, and industry standards adherence, are vital in ensuring maritime security. Investments in cybersecurity measures are necessary to safeguard critical port infrastructure and prevent cyber threats. Training and capacity development for maritime security personnel and law enforcement organizations are necessary to stay ahead of evolving threats. Case studies and lessons learned demonstrate the importance of an adaptive and multifaceted strategy that includes operational, technological, and cooperative measures to enhance maritime security and minimize the risks of terrorist activities in the maritime domain.

To combat the grave threat of maritime terrorism, a comprehensive strategy is necessary to strengthen maritime security. This requires effective countermeasures such as enhancing international cooperation, utilizing technical advancements, investing in capacity building and training, and promoting public awareness and community involvement. Although some current tactics have shown some effectiveness, gaps and challenges still need to be addressed. The importance of multidimensional approaches, risk assessments, public-private partnerships, and ongoing adaptation is highlighted by successful situations. By implementing these measures, states and other parties can improve maritime security, reduce risks, and ensure international maritime trade's safe and secure flow.

ISSN: 2582-6433

# 10. References

[1] Amy Sing Wong; Spyridon Vrettos; Michelle L Taylor; "An Assessment of People Living by Coral Reefs Over Space and Time", GLOBAL CHANGE BIOLOGY, 2022.

[2] S. Khan; Fasih Ahmed; M. Mubeen; "A Text-Mining Research Based on LDA Topic Modelling: A Corpus-Based Analysis of Pakistan's UN Assembly Speeches (1970-2018)", INT. J. HUMANIT. ARTS COMPUT., 2022. (IF: 3)

[3] U L H P Perera; H C S Subasinghe; Amila Sandaruwan Ratnayake; W A D B Weerasingha; T D U Wijewardhana; "Maritime Pollution in The Indian Ocean After the MV X-Press Pearl Accident", MARINE POLLUTION BULLETIN, 2022.

[4] Xiaojing Du; James M Russell; Zhengyu Liu; Bette L Otto-Bliesner; Delia W Oppo; Mahyar Mohtadi; Chenyu Zhu; Valier V Galy; Enno Schefuß; Yan Yan; Yair Rosenthal; Nathalie Dubois; Jennifer Arbuszewski; Yu Gao; "North Atlantic Cooling Triggered a Zonal Mode Over the Indian Ocean During Heinrich Stadial 1", SCIENCE ADVANCES, 2023.

[5] Alka Yadav; Sourish Das; K Shuvo Bakar; Anirban Chakraborti; "Understanding the Complex Dynamics of Climate Change in South-west Australia Using Machine Learning", ARXIV-PHYSICS.DATA-AN, 2023.

[6] Tosin Ige; Abosede Kolade; Olukunle Kolade; "Enhancing Border Security and Countering Terrorism Through Computer Vision: A Field of Artificial Intelligence", ARXIV-CS.CV, 2023.

[7] M. Zacharias; L. Gerber; K. Hyrenbach; "Review of The Southern Ocean Sanctuary: Marine Protected Areas in The Context of The International Whaling Commission Sanctuary Programme", J. CETACEAN RES. MANAGE., 2023. (IF: 3)

[8] A. Susandi; A. F. Pratama; A. Wijaya; "An Overview of Extreme Storm Trends in Java Island Using Storm Severity Index (SSI)", IOP CONFERENCE SERIES: EARTH AND ENVIRONMENTAL SCIENCE, 2023.

[9] Jillian A Hudgins; Emma J Hudgins; Stephanie Köhnk; Enas Mohamed Riyad; Martin R Stelfox; "A Brighter Future? Stable and Growing Sea Turtle Populations in The Republic of Maldives," PLOS ONE, 2023.

[10] E P D N Thilakarathne; W N D S Jayarathna; S W R Sewwandi; S C Jayamanne; N P P Liyanage; "Tropical Coral Reefs in Sri Lanka Are Threatened Due to The Fluctuation of Seasonal and Interannual Sea Surface Temperature", ENVIRONMENTAL MONITORING AND ASSESSMENT, 2023.

[11]Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I., & Ortiz, D. S. (2006). Maritime Terrorism: Risk and Liability. Retrieved 6 14, 2023, from

ISSN: 2582-6433

https://rand.org/pubs/monographs/mg520.html

[12]Knyazeva, N. A., & Korobeev, A. I. (2015). Maritime Terrorism and Piracy: The Threat to Maritime Security. Mediterranean Journal of social sciences, 6, 226. Retrieved 6 14, 2023, from https://mcser.org/journal/index.php/mjss/article/download/8224/7888

[13]Malcolm, J. A. (2011). The securitisation of the United Kingdom's maritime infrastructure during the 'war on terror'. Retrieved 6 14, 2023, from [14]http://wrap.warwick.ac.uk/45468/1/wrap_thesis_malcolm_2011.pdf

Otto, L. (2015). Maritime Crime in Nigeria and Waters Beyond Analysing the Period 2009 to 2013. Africa insight, 45(1), 15-29. Retrieved 6 14, 2023, from https://ajol.info/index.php/ai/article/view/131913

[15]Parashar, S. (2007). Maritime Counter-Terrorism: A Pan-Asian Perspective. Retrieved 6 14, 2023, from https://amazon.com/maritime-counter-terrorism-perspective-swati-parashar-ebook/dp/b00913csrk

[16]Huang, D., & Hua, Y.. (2022, February 8). Economic Cost Model of Options to Global Sulphur Cap considering Speed Differentiation. https://scite.ai/reports/10.1155/2022/137272

[17] Musa, M. A., & Zulkifli, N.. (2022, February 10). The US-Malaysia Maritime Security Cooperation and Implication Towards Malaysia's National Security. https://scite.ai/reports/10.47405/mjssh.v7i2.1306

[17] Maritime Terrorism | SpringerLink. (n.d). https://link.springer.com/chapter/10.1007/978-3-030-34630-0_9

[18] Onwuegbuchunam, D. E., Okeke, K. N., Aponjolosun, M. O., & Igboanusi, C.. (2021, January 1). Impacts of Terrorism and Piracy on Maritime Activities: An Exploratory Study. International Journal of Transportation Engineering and Technology, 7(4), 104. https://doi.org/10.11648/j.ijtet.20210704.13

[19] Imran Khan; Muhammad Imran; Hamid Iqbal; "Geo-Political Checkmate in The Indian Ocean Region: 21st Century Maritime Silk Road, Energy Security and Indo-US Nexus", 2019.

[20] Sanjaya Baru; "Indian Ocean Perspectives: From Sea Power to Ocean Prosperity", STRATEGIC ANALYSIS, 2019.

[21] Robert McCabe; "Improving Maritime Security Sector Capacity to Counter Terrorism: Lessons from International Capacity Building Projects in The Western Indian Ocean", 2020.

[22] Lei Zhou; Raghu Murtugudde; "Oceanic Impacts on MJOs Detouring Near The Maritime Continent", JOURNAL OF CLIMATE, 2020. (IF: 3)

[23] Abdallah M. El-Nofely; Rehna Gul; "The East African Indian Ocean and The Security Challenges", JOURNAL OF LAW, POLICY AND GLOBALIZATION, 2020.

ISSN: 2582-6433

[24] P. K. B. Isuru Premarathna; "Maritime Security Challenges in The Indian Ocean: Special Reference to Sri Lanka", 2021.

[25] Adi Bandono; Avando Bastari; Okol Sri Suharyo; "The Education Perspective of Indonesia Maritime Geopolitics In The Indian Ocean", 2021.

[26] Adam W. Schneider; Emily C. Gill; Balaji Rajagopalan; Guillermo Algaze; "A Trade-Friendly Environment?: Newly Reconstructed Indian Summer Monsoon Wind Stress Curl Data for The Third Millennium BCE and Their Potential Implications Concerning The Development of Early Bronze Age Trans-Arabian Sea Maritime Trade", JOURNAL OF MARITIME ARCHAEOLOGY, 2021.

[27] Zaeem Hassan Mehmood; Ramla Khan; "Assessing Indian Ocean Economics: Perspective from Pakistan", ANDALAS JOURNAL OF INTERNATIONAL STUDIES (AJIS), 2021.

[28] R S Aswani; Shambhu Sajith; Mohammad Younus Bhat; "Is Geopolitics A Threat for Offshore Wind Energy? A Case of Indian Ocean Region", ENVIRONMENTAL SCIENCE AND POLLUTION RESEARCH INTERNATIONAL, 2021. (IF: 3)

# 11. Disclosure of conflict of interest

The authors have no conflict of interest.

# 12. Acknowledgements

The authors are thankful to the School of Integrated Coastal and Maritime Security Studies, Rashtriya Raksha University, Gandhinagar, Gujarat, India.