TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 19
Number 4
December 2025
DOI: 10.12716/1001.19.04.11

Maritime Security Operations Center (M-SOC): Systematic Literature Review, Research Gaps and Future Areas to Investigate

A.N. Nasr, R. Vaarandi, I. Zaitseva-Pärnaste & P. Kujala
Tallinn University of Technology, Tallinn, Estonia

ABSTRACT: The maritime industry is undergoing rapid digital transformation, integrating advanced technologies to enhance operational efficiency and connectivity. However, this shift introduces significant cybersecurity vulnerabilities, as increasing reliance on digital systems for navigation, communication, and control exposes vessels to cyber threats. Despite growing awareness, the industry lacks unified cybersecurity frameworks, leading to fragmented defenses that attackers can exploit to compromise critical systems such as navigation and control functions. The Maritime Security Operations Centers (M-SOCs) Framework aims to provide a consolidated approach to threat monitoring, detection, and response. However, research on adapting traditional Security Operations Centers (SOCs) to the unique maritime environment remains limited.
This paper addresses this gap by conducting a systematic literature review (SLR) using the SALSA (Search, Appraisal, Synthesis, and Analysis) framework to examine the current state of M-SOCs. By analyzing existing research, we identify key trends, challenges, and opportunities in maritime cybersecurity operations. Our findings highlight the need for tailored SOC models that account for the maritime sector's distinct operational, technological, and personnel constraints. This review contributes to the growing body of knowledge on maritime cybersecurity, offering insights to guide future M-SOC development and implementation. Ultimately, this work supports efforts to strengthen cyber resilience in the maritime domain against evolving threats and increasing attack surface.

1 INTRODUCTION

With cutting-edge technologies quickly incorporated into vessel operations, the maritime industry is seeing a rapid digital transformation. These developments increase connectedness and efficiency, but they also present new cybersecurity threats. Ships are more susceptible to cyberattacks as they depend more and more on digital systems for control, communication, and navigation. The sector currently lacks integrated solutions that provide a comprehensive picture of a vessel's cybersecurity state, despite growing awareness. The defenses in place now are frequently fragmented and focus on specific systems separately. Attackers can use the security flaws created by this disjointed strategy to get access to vital systems or obstruct navigation.

Efforts to enhance cyber resilience in the maritime sector are underway. and the industry is investigating integrated solutions that consider the complexity of contemporary maritime operations to increase cyber resilience. The Maritime Security Operations Center (M-SOC), which aims to offer unified monitoring, threat detection, and response across all onboard systems, is one new approach. There is little research on how to tailor conventional Security Operations Centers (SOCs) for the maritime environment, despite

the M-SOC framework's potential. People, procedures, and technology are the three main components of SOCs, and each must be customized to meet the requirements of maritime operations.

This review article seeks to address this gap by examining the current state of the art in Maritime Security Operations Centers. Using the SALSA (Search, Appraisal, Synthesis, and Analysis) method, we have reviewed a comprehensive body of literature to identify key trends, challenges, and opportunities in the field. By synthesizing existing research, this paper aims to provide a meaningful overview of the current landscape and offer insights that can guide future efforts to develop and implement M-SOCs. Our findings will contribute to the growing body of knowledge on maritime cybersecurity, providing a foundation for researchers and practitioners to build upon as they work to safeguard the maritime domain against emerging cyber threats.

2 BACKGROUND

With the increased cyber integration into the maritime systems, it is needed to tend to the cybersecurity aspect of all the newly introduced concerns and increasing attack surface. However, when planning cybersecurity measures, we need to keep in mind the unique nature of the maritime industry and how complex and vast it is. With majority of the world trade relying on maritime transportation It is crucial to have secure operations. and a similar level of cyber protection as other sensitive infrastructures. [1], [2]

Unlike land-based industries, maritime operations face some very particular hurdles. For starters, connectivity at sea is intermittent and bandwidth-limited, making real-time defense and remote support a logistical nightmare. Many vessels also rely on legacy systems that weren't designed with cybersecurity in mind, and there's a wide disparity in digital maturity across different types of ships and fleets. Add to that the fact that many crews have limited IT training, and you're left with a sector uniquely vulnerable to cyber disruption. [3], [4]

Safeguarding the maritime domain from cyberattacks is a crucial task that will proactively mitigate devastating incidents, with the maritime industry handling nearly 90% of world trade. It increasingly depends on complicated, interconnected global cyber architectures, integrating Information Technology (IT) and Operational Technology (OT) systems to support its various and complex operations and processes. [5], [6]

The digital transformation occurred in the maritime industry in recent years, bringing automation, IoT integration, and interconnected control systems into everyday operations. But with innovation comes exposure, and the maritime world is now suffering from a cyber threat landscape that's as complex as it is urgent. [7]

Cyberattacks on maritime infrastructure are very dangerous and destructive since the maritime domain is interconnected with practically all other domains. The 2017 NotPetya ransomware attack that crippled Maersk operations and racked up an estimated $300 million in damages was a turning point. But that was just the beginning. From GPS spoofing to AIS manipulation and attacks on integrated bridge systems, the list of digital threats has only grown longer and more sophisticated. [8], [9]

A landmark moment came in 2021, when the International Maritime Organization (IMO) required ship operators to embed cybersecurity into their safety management systems. This mandate has helped spur industry-wide movement toward more structured cyber risk management, and M-SOCs are central to this shift. Still, regulation often lags innovation, and there's ongoing debate about whether current policies can keep pace with evolving threats. [10]

Increasingly, maritime operations are critical infrastructure on par with energy, finance, and telecommunications. The EU's NIS2 directive states that the maritime sector is critical, underscoring just how vital secure and resilient maritime systems are to national and international stability. In this context, the push for M-SOC development isn't just the best practice; it's a strategic imperative. [11], [12]

The Maritime Security Operations Center is a customized version of SOC, which is a centralized framework combining personnel, processes, technologies, and governance to monitor, detect, analyze, and respond to cybersecurity threats in real-time, protecting an organization's systems, networks, and data. [6], [13]

The core concept of M-SOC is to establish a centralized hub to collect data from vessels, providing continuous monitoring of the digital systems. However, that is not the only function that an M-SOC can do; upon collecting the data from the various systems onboard the vessel, the inland cybersecurity team analyzes and responds to potential threats in real-time (see Figure 1). By integrating skilled personnel, streamlined processes, advanced technologies, and robust governance and compliance protocols, M-SOCs ensure rapid identification and mitigation of potential attacks. This holistic approach aims to prevent damage before it occurs, or in case of an incident occurring, it will provide mitigating strategies. Additionally, M-SOCs facilitate continuous monitoring, incident response, and threat intelligence analysis to strengthen organizational resilience against evolving cybersecurity risks. [14]

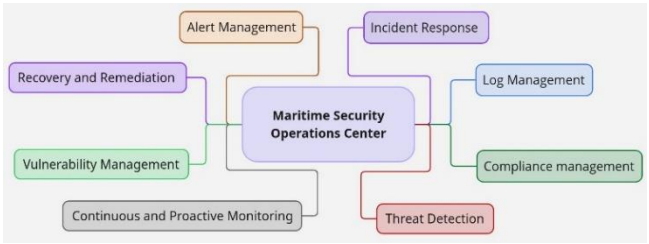

Figure 1. M-SOC Functions, adapted from [15], [16]

Looking into SOC, we found that literature suffers from significant fragmentation and a lack of unifying frameworks. While researchers largely concur with the required capabilities of a SOC, a universally accepted definition remains elusive. Existing academic work tends to concentrate on specific aspects of SOC functionality, neglecting a more comprehensive, architectural perspective. Only a small number of

studies have attempted to establish such holistic frameworks. [14], [17], [18]

The fragmented nature of literature poses significant challenges for researchers adapting solutions to the maritime domain, where dynamic and often siloed systems introduce additional complexity. These disconnected IT and OT systems demand innovative approaches to ensure cohesive solutions. Furthermore, effective communication between vessels and inland hubs remains a critical issue to secure data exchange in real-time. Addressing these challenges necessitates the development of integrated, scalable systems that bridge system divides, enhance interoperability, and ensure reliable connectivity across the maritime ecosystem, ultimately strengthening the resilience of maritime cyber architectures. [5]

This paper aims to examine the state-of-the-art in current research on M-SOCs, identifying critical gaps that require attention. It seeks to propose novel contributions to develop practical, effective M-SOC solutions that organizations and companies in the maritime industry can implement to enhance cybersecurity. By analyzing existing literature, technologies, and frameworks, the study will highlight deficiencies in integrating IT and OT systems, addressing challenges in real-time threat detection, response, and resilience. The goal is to provide actionable recommendations for stakeholders to deploy robust M-SOCs, ensuring the protection of complex, interconnected maritime cyber architectures.

3 METHODOLOGY

A Systematic Literature Review (SLR) is a structured and methodical approach to gathering, critically assessing, synthesizing, and presenting findings from a wide range of research studies focused on a specific research question or topic. By utilizing this approach, the study will provide a comprehensive and unbiased analysis of existing literature, enabling researchers to identify patterns, gaps, and insights relevant to their area of study. [[19]

The Search, Appraisal, Synthesis, and Analysis (SALSA) framework serves as a structured methodology for defining the search protocols that a Systematic Literature Review (SLR) should adhere to. This approach ensures methodological rigor, systematic execution, comprehensiveness, and reproducibility, thereby enhancing the reliability and validity of the review process and mitigation of risks associated with publication bias [20].

The SALSA framework can be broken down into several phases; the search phase focuses on compiling an initial collection of relevant publications. The appraisal phase involves evaluating these publications to eliminate those that are irrelevant or do not meet the criteria. Finally, the synthesis and analysis phases extract meaningful data from the selected studies, enabling researchers to draw conclusions and produce a cohesive final report. When the process is carried out correctly and with few errors, the study can yield reliable results and conclusions that could guide researchers and decision-makers (see Figure 2). [21]

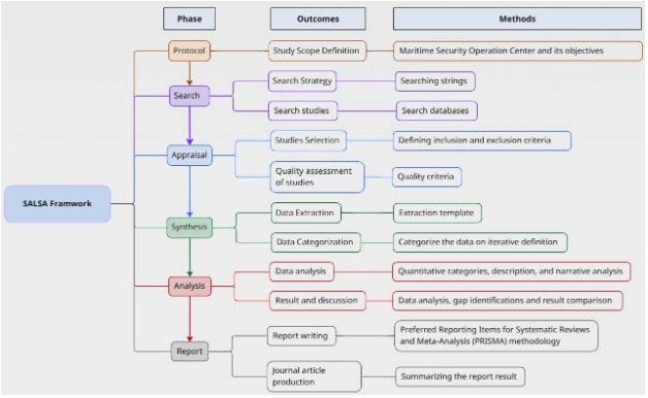

Figure 2. SALSA Framework. [22]

In this study we are following the SALSA framework, which was applied by Grant et al. [23] and García-Holgado et al. [21] and tailored version for IT by Carrera-Rivera et al. [24] and Mengist et al. [22]. To ensure a comprehensive approach, these versions incorporate the search protocol phase, derived from the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, along with a dedicated report phase, which resulted in the six-phase framework, PSALSAR (see Table 1), that we will be using in this study.

Table 1. PSALSAR framework

Phase	Outcomes	Methods
Protocol	Study Scope Definition	Maritime Security Operation Center and its objectives
Search	Search strategy	Searching strings
	Search studies	Search databases
Appraisal	Studies Selection	Defining inclusion and exclusion criteria
	Quality assessment of studies	Quality criteria
Synthesis	Data Extraction	Extraction template
	Data Categorization	Categorize the data on iterative definition
Analysis	Data analysis	Quantitative categories, description, and narrative analysis
	Results and discussion	Data analysis, gap identifications and result comparison
	Conclusion	Presenting conclusion and recommendation
Report	Report writing	Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) methodology
	Journal article production	Summarizing the report result

3.1 *Protocol – SLR methodology step 1*

At this stage, the scope of the study is carefully defined and refined, enabling the formulation of focused and meaningful research questions while establishing clear research boundaries. However, we need to create a research protocol to ensure that the study is reproducible and transparent. Determining the scope is essential to identify the proper research methods. [25]

The PICOC framework (Population, Intervention, Comparison, Outcome, Context) helps structure research questions and identify key search terms for Systematic Literature Reviews (SLRs), as defined in Table 2. Originally used in medical and social sciences, it has been adapted for computer science research to

help build terminology that can be used for building proper search queries in the selected databases. For example, the keyword “Center” can be replaced by “Centre”. [24]

Table 2. PICOC Framework to determine the research scope

Concept	Definition	SLR Application
Population	The research is addressing Maritime Security Operations center or its implementation	Scientific research that discusses SOC implementation in maritime and M-SOC’s people, processes and Technology
Intervention	Existing techniques used to address the problem	Discussing the existing techniques or frameworks used in M-SOC domain in order to identify the gaps that need further research.
Comparison	Methods to compare and evaluate the effectiveness of interventions used to address or assess M-SOC aspects against each other	Difference between the different methods applied to build the research about M-SOC or its aspects like people, processes and Technology.
Outcome(s)	Approaches to evaluate the knowledge base and find gaps in selected publications on M-SOC	Existing state of the art on M-SOC Mentioned gaps: limitations when it comes to lack of studies in a certain aspect in M-SOC
Context	The particular settings or areas of the population which are more common.	Trends in M-SOC research, existing knowledge, the challenges and gaps in M-SOC

Based on the PICOC framework and after refinement, the research questions are as follows:

1. What is the current state-of-the-art in M-SOCs research?
2. What methodological approaches are being used to study M-SOCs?
3. Which aspects of M-SOCs have received the most and least research attention?
4. What are the primary challenges and gaps in M-SOC implementation and research?
5. What are the emerging trends and future directions for M-SOC development?

The questions are the key components of the study that provide a precise and clear understanding of the study's objectives and guide the direction of the investigation. The questions will be answered by following the SALSA approach in the result section of the study.

3.2 *Search – SLR methodology step 2*

This phase involved identifying relevant sources of information through a structured search strategy and delivery process. The search strategy was designed to pinpoint appropriate databases and formulate precise search strings to retrieve documents that are pertinent to the research topic. This systematic approach ensures the collection of high-quality and relevant literature for analysis. [[25]

While conducting our research, we came to realize that while numerous papers can be linked to M-SOC operations, many do not explicitly mention M-SOC. This is understandable, as an M-SOC represents an amalgamation of various methods and practices integrated into a holistic framework designed to operate in a dynamic and complex domain. However, since this analysis's exclusive focus is on M-SOCs, only papers directly addressing M-SOCs will be utilized.

While designing the search terms’ structure, we decided to include publications that only had the exact terms in the table below in the title, abstract, or keywords. One more thing that we encountered is that if we search for each word separately (“Maritime” AND “Security” AND “Operations” AND “Center” or similar compilations), we will get misleading results. Hence the search strings mentioned in Table 3.

Table 3. Search String and Databases. [20]

Database	Searching term		No of articles	Date of acquisition
Google Scholar	Main searching terms-using document title, abstract and keywords search option	"Security operations center" AND "maritime"	12	02-02-2025
		"Security operations centre" AND "maritime"	5	02-02-2025
		"Maritime Security operations center"	3	02-02-2025
		"Maritime Security operations centre"	3	02-02-2025
	Secondary searching terms	"SOC" AND "maritime"	4	21-02-2025
		"MSOC"	0	21-02-2025
		"M-SOC"	0	21-02-2025
		"Cyber security operations center" AND "maritime"	2	06-03-2025
		"Cyber security operations centre" AND "maritime"	3	06-03-2025
Scopus	Main searching terms-using document title, abstract and keywords search option	"Security operations center" AND "maritime"	6	02-02-2025
		"Security operations centre" AND "maritime"	6	02-02-2025
		"Maritime Security operations center"	4	02-02-2025
		"Maritime Security operations centre"	4	02-03-2025
	Secondary searching terms	"SOC" AND "maritime"	4	21-02-2025
		"MSOC"	0	21-02-2025
		"M-SOC"	3	06-03-2025
		"Cyber security operations center" AND "maritime"	0	06-03-2025
		"Cyber security operations centre" AND "maritime"	0	06-03-2025

ScienceDirect	Main searching terms-using document title, abstract and keywords search option	"Security operations center" AND "maritime"	1	02-02-2025
		"Security operations centre" AND "maritime"	1	02-02-2025
		"Maritime Security operations center"	1	21-02-2025
		"Maritime Security operations centre"	1	06-03-2025
	Secondary searching terms	"SOC" AND "maritime"	1	06-03-2025
		"MSOC"	0	06-03-2025
		"M-SOC"	1	06-03-2025
		"Cyber security operations center" AND "maritime"	0	06-03-2025
		"Cyber security operations centre" AND "maritime"	0	06-03-2025

The search was conducted across Scopus, ScienceDirect, and Google Scholar. This combination was chosen for its high level of comprehensiveness, particularly with Google Scholar's broad coverage and the advanced search capabilities of ScienceDirect and Scopus, which helped in finding relevant articles. [26], [27]

The main and secondary search strings were mentioned in Table 3. It can be more apparent that the body of research is quite limited, even after the addition of other terms, which did not yield many additional results. Therefore, the inclusion and exclusion criteria served to exclude duplicate papers or non-peer-reviewed papers.

3.3 *Appraisal – SLR methodology step 3*

The appraisal phase involved evaluating selected articles against the review's objectives. This included screening the literature to identify relevant papers using predefined inclusion and exclusion criteria. Only papers meeting the inclusion criteria were selected for in-depth investigation and content assessment, as detailed in Table 4.

Table 4. Inclusion and Exclusion criteria.

Criteria	Decision
The search strings found in keywords, title. Abstract section of the paper	Inclusion
Papers that are written in English language	Inclusion
Papers that are published in peer-reviewed Journals/Conferences	Inclusion
Papers that at least discussed a single aspect of M-SOC	Inclusion
Duplicated papers from the search phase	Exclusion
Inaccessible papers	Exclusion
Not primary or original research papers	Exclusion
Papers published before 2010	Exclusion

Using our designed search string, we initially found 65 articles across Google Scholar (32), Scopus (27), and ScienceDirect (6), encountering only one inaccessible paper. After removing duplicated papers and inaccessible papers, 9 articles remained that satisfied our criteria.

Table 5 summarizes key research papers relevant to Maritime Security Operations Centers (M-SOCs), spanning from 2016 to 2024.

Table 5. M-SOC Studies

No,	Paper Title	Publish Year	Publication Type	Country	Access	Status
1	Toward a better future through maritime security. [28]	2016	Book Chapter	Italy	Closed Access	Requested a copy but no answer, Excluded
2	Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre. [29]	2019	Conference	France	Open access	Available, Included
3	A Concept for Establishing a Security Operations and Training Centre at the Bulgarian Naval Academy. [30]	2020	Journal	Bulgaria	Open access	Available, Included
4	Training the Maritime Security Operations Centre Teams. [31]	2022	Conference	Italy	Open access	Available, Included
5	Sector-Specific Training - A Federated Maritime Scenario. [32]	2022	Conference	Belgium	Open access	Available, Included
6	Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment. [33]	2022	Conference	Norway	Open access	Available, Included
7	Improving Cybersecurity Capabilities at Nikola Vaptsarov Naval Academy by Building and Developing a Security Operations and Training Center. [34]	2023	Conference	Bulgaria	Open access	Available, Included
8	Bridging the Gap: Enhancing Maritime Vessel Cyber Resilience through Security Operation Centers. [6]	2024	Journal	Norway	Open access	Available, Included
9	Exploring Historical Maritime Cyber-Attacks and Introducing Maritime Security	2024	Conference	Estonia	Closed Access	Available, Included

	Operations Center as a Solution to Mitigate Them. [13]					
10	Enabling cyber resilient shipping through maritime security operation center adoption: A human factors perspective. [5]	2024	Journal	Norway	Open access	Available, Included

3.4 *Synthesis – SLR methodology step 4*

The synthesis phase focused on systematically extracting and classifying relevant data from the nine selected papers to generate meaningful insights and conclusions. Key variables of interest, as outlined in Table 6, were identified and documented in a dedicated extraction log to facilitate structured processing. The data collected was then organized into thematic categories and prepared for analysis.

Table 6. Extraction Criteria [[22]

No.	Criteria	Categorization (If Applicable)
1	Year of publication	Between 2016 to 2024.
2	Country of Origin	Norway, Bulgaria, etc.
3	Research objectives	Framework proposal or implementation, Increasing or raising awareness about maritime cybersecurity, etc.
4	Methodology used	Empirical, systems-oriented, etc.
5	Key findings	Connectivity constraints, Human resource limitations, technical complexity, etc.
6	M-SOC components/features described	Offshore/onboard the ship, Onshore center, etc.
7	Challenges identified	Personnel process or Technological challenges, Lack of available standardization, etc.
8	Solutions proposed	Specialized training, technical solutions, procedural solutions, etc.
9	Future research directions suggested	Human-System Integration, Integration with Broader Maritime Systems, etc.
10	Stakeholders involved	Ship Crew/Owners, Policy makers, Maritime cybersecurity professionals, etc.
11	Implementation context	training and education, technical architecture and implementation, human factors and operational challenges, and threat analysis and historical context.

3.5 *Analysis – SLR methodology step 5*

In this phase, we investigate the synthesized data that we compiled from the previous phase based on the extraction parameters detailed in Table 6. By the end of the analysis phase, all research questions will be answered. In this phase, we also formulate a comprehensive idea about the publications to build pathways for future research and, finally, conclude the study of the selected papers.

Since there were limited numbers of publications, the selected papers were investigated in depth, which enabled the authors with the implementation of the SALSA framework to conduct qualitative analysis and produce reliable findings and conclusions.

Voyant Tools, a web-based analysis platform, was used to calculate keyword frequencies across all selected articles. VOSviewer is also used to visualize bibliometric networks and text mining. Additionally, Publish or Perish, an open-source tool, retrieved and analyzed article citations. [35], [36], [37], [38]

3.6 *Report – SLR methodology step 6*

In the report phase, the result of the analysis is presented in addition to recording the methodology. Fernández del Amo et al. [25] state that this phase consists of two crucial steps:

1. Procedure Description: Tables 1 through 6 provide a clear explanation of the research process, including the methods followed. Which helps other researchers replicate the study and reduce the bias.
2. Results Dissemination: Publicly sharing the study findings, usually through a journal article.

The last phase in SLR is publishing a journal article, which guarantees that the research findings are available for both scholarly and practical application. [22], [25]

4 RESULT

The result section consisted of an overview that discussed with a close look at where we currently stand in M-SOC research and implementation, presenting the field's state of the art. Moving to discuss emerging strategies, persistent challenges, and the evolving role of M-SOCs in safeguarding maritime operations at the intersection of physical security and cyber resilience.

This systematic literature review aims to address five research questions (see Section 3.1). The following sections will provide answers to these questions. Sections 4.2 and 4.3, form the state-of-the-art in the domain (RQ1). Section 4.4 evaluates the methodological approaches used in the reviewed papers (RQ2). Section 4.5 focuses on the publications distribution to understand the research attention (RQ3).

Section 5 outlines the main challenges and research gaps (RQ4), including issues related to standardization and misalignment between regulations and real-world needs. Section 7 addresses emerging trends and future directions (RQ5), pointing to adaptive system architectures and human-centered design.

After the review, we found out that the M-SOC studies can be categorized into four categories: training and education, technical architecture and implementation, human factors and operational challenges, and threat analysis and historical context. The review also addresses the scale of implementation and the purpose of the studies.

4.1 *The Geographical and Temporal Distribution of Research Efforts*

Geographic representation reflects a diverse distribution but is confined within Europe, including contributions from France, Italy, Bulgaria, Belgium, Norway, and Estonia. Most papers are openly accessible, facilitating broad dissemination and

engagement, though a couple remain behind closed access. The citations vary widely, with some foundational works from earlier years gathering significant attention, while recent publications reflect emerging focus areas such as training, human factors, and cyber resilience. Notably, several studies concentrate on practical implementations and training facilities, particularly from Bulgarian and Italian institutions, while others emphasize technical innovation and historical threat analysis.

The maritime industry has experienced a significant digital transformation in recent years, creating new vulnerabilities and expanding the attack surface for cyber threats. The final list of articles analyzed in this review consists of 9 publications, covering the period from 2016 to 2024, with relatively steady growth in studies through time. As shown in Table 6, all studies were conducted in Europe, reflecting a strong regional bias in M-SOC research. While authors can sometimes collaborate across countries, in all 9 publications, the authors were from the same country.

Due to the limited number of studies that were conducted and how scattered they are across multiple aspects of M-SOCS, the current state of the art does not provide a comprehensive view. However, there has been an uptick in publications over the last decade, with most of the papers published after 2020. The increased publication number might be due to the implementation of the International Maritime Organization (IMO) Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems, which was adopted in June 2017 and came into effect in January 2021, driving increased attention to maritime cybersecurity. [10]

4.2 *Current State of Maritime Cybersecurity*

As M-SOCs continue to evolve, their development increasingly reflects both lessons learned from traditional SOCs and the distinct demands of the maritime environment. While SOC principles form the foundation of M-SOC operations, the maritime context introduces unique variables. These challenges demand a tailored approach to training, human-system interaction, and technical infrastructure. Recent research and implementation efforts demonstrate a growing emphasis on adapting SOC methodologies to fit the complexities of maritime operations, resulting in an emerging body of knowledge that spans education, organizational dynamics, and innovative technical solutions. The following sections explore these key dimensions of the current state of the art of M-SOCs.

As M-SOCs continue to mature, training and education remain a primary focus, reflecting the early-stage development of maritime-specific cybersecurity capabilities. Institutions like the Bulgarian Naval Academy have established dedicated facilities that blend operational security functions with hands-on training. Modern programs rely heavily on simulation-based learning, where participants engage in red team versus blue team exercises to mimic real-world maritime cyber threats. These simulations are increasingly supported by server virtualization technologies, enabling safe and flexible training environments without impacting live systems. In advanced setups, federated scenarios simulate interactions between vessels, ports, and other maritime stakeholders, preparing trainees for the complexities of coordinated cyber responses. Complementing these efforts, emerging competency frameworks—some adapted from the NIST NICE model—are helping define the specific skills and knowledge required for M-SOC personnel. [30], [34]

The effectiveness of M-SOCs depends heavily on human elements, which continue to pose both challenges and opportunities. Low levels of cyber awareness among vessel crews persist, with studies indicating that many seafarers remain unclear on their roles during cyber incidents. On the analyst side, issues such as alert fatigue, workload pressure, and burnout mirror those found in traditional Security Operations Centers, contributing to high turnover and operational strain. Communication between shore-based analysts and onboard crews is another critical concern, often complicated by differences in cyber literacy. Analysts also need in-depth maritime domain knowledge to contextualize alerts effectively, including familiarity with navigation systems, vessel operations, and regulatory frameworks. Additionally, integrating M-SOCs within maritime organizational structures remains complex, requiring clear coordination between shipboard personnel, technical teams, and security staff. [39], [40]

On the technical front, M-SOCs are evolving rapidly, incorporating intelligent decision support systems that use AI and machine learning to interpret large volumes of maritime data and detect anomalies. These systems are tailored to operate within the bandwidth limitations typical of maritime environments, using compression and prioritization techniques to ensure critical information is transmitted efficiently. To mitigate the risks of network integration, many M-SOCs use isolated monitoring systems that collect traffic data without introducing new vulnerabilities. Furthermore, detection capabilities are becoming more specialized, with signatures designed specifically for maritime systems such as AIS, ECDIS, and integrated navigation platforms. As vessel autonomy advances, M-SOCs are increasingly interfacing with Remote Operations Centers, opening new possibilities for unified security management, though this also introduces additional layers of complexity and potential attack surfaces. [13]

4.3 *Categorization of Maritime Security Operations Center Articles by Theme*

The systematic review of M-SOC literature reveals distinct thematic clusters that reflect the multidisciplinary nature of this domain (see Figure 5). The analyzed articles can be categorized into four primary research themes: Training and Education (40%), Technical Architecture and Implementation (20%), Human Factors and Operational Challenges (30%), and Threat Analysis and Historical Context (10%).

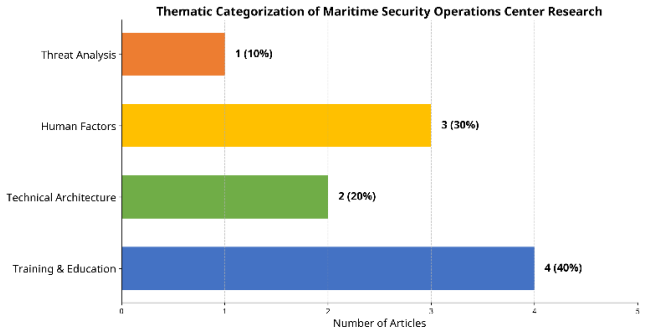

Figure 5. Thematic Categorization

4.3.1 *Training and Education Approaches*

The evolution of M-SOCs has brought renewed attention to the development of specialized training and educational programs tailored to the unique challenges of maritime cybersecurity. Unlike general cybersecurity education, training for M-SOC personnel must account for the highly specific operational contexts of ships, ports, and maritime infrastructure. The reviewed literature consistently underscores the need for immersive, domain-specific learning environments where both technical and soft skills are cultivated in parallel. [31]

Several key contributions illustrate the growing sophistication of this training landscape. Raimondi et al. [31] made a three-fold contribution to the field. It is also worth mentioning that the training environment utilized was based on the M-SOC architecture provided by Jacq et al. [29]

First, the authors developed a comprehensive profile definition for maritime SOC operators by leveraging the NICE (National Initiative for Cybersecurity Education) framework. The paper details three skill groups for SOC operators: Configuring (related to security monitoring tools), Monitoring (analyzing and interpreting data from systems), and Investigating (conducting deep analysis of incidents). For each skill group, they identify associated task groups that operators must perform. The qualifying expertise section outlines six maritime-specific knowledge areas that SOC operators must acquire: Sensors, Integrated Navigation Systems (INS), National Marine Electronics Association (NMEA) protocol, Satellite connections, Regulations, and soft skills for interacting with ship crews who often lack cybersecurity expertise.

The second contribution is the development of a virtual training scenario that simulates a vessel's Integrated Navigation System and monitoring infrastructure. This testbed includes both a remote site (the ship under monitoring) and a shore-side center hosting the M-SOC. The security infrastructure includes Suricata [41] for intrusion detection system (IDS) functionality and Splunk [42] as the shipboard security information and event management (SIEM). The shore-side center includes the main SIEM, Moodle [43], and a Monitoring host for evaluation (using Prometheus [44] and Grafana [45]).

The third contribution is a detailed training exercise focusing on specific skills for Tier 1 operators. The exercise simulates an attack that injects false heading values into the INS network, requiring trainees to configure the SIEM to detect the attack, document their approach, and identify anomalous values. The authors provide specific queries in Splunk Search Processing Language that trainees might use to detect the attack and classify anomalous data. They also present a comprehensive evaluation methodology that considers report quality, correct classification of anomalous packets, and detection time.

La Vallée et al. [32] extend this conversation by addressing the need for sector-specific cybersecurity training in the maritime domain through the implementation of federated cyber ranges that allow different providers to combine assets for more specialized training environments. The authors describe a federated maritime scenario training delivered as part of the ECHO Federated Autumn School 2021, which simulated a passenger ship's network infrastructure including service, navigation, and passenger networks connected through firewalls. The scenario was implemented through a federation of two separate cyber ranges connected via VPN, demonstrating the successful implementation of a federated cyber range for maritime-specific training that addresses both technical federation challenges and pedagogical aspects of defensive training.

Meanwhile, Nikolov et al. [30], [34] provide a more hands-on perspective through two studies focused on the Bulgarian Naval Academy. These papers present the concept, design, and organizational steps for building and developing a Security Operations and Training Center at the Nikola Vaptsarov Naval Academy in Bulgaria. The author proposes a dual-purpose facility functioning as both a training center and an SOC for the academy's computer network, noting that this integration is innovative as most existing centers provide only training environments. The paper details requirements for the Security Operations and Training Centre (SOTC)'s structural components, categorizing key resources into hardware (physical resources), software (intellectual resources), and staff (human resources), with emphasis on cyber range platforms for simulating cyber incidents and attacks.

Taken together, these studies converge on a core insight: building effective M-SOC teams requires more than technical instruction; it demands experiential learning that reflects the realities of maritime operations. Whether through simulation-based exercises, federated training scenarios, or purpose-built facilities like the SOTC, the direction of current research clearly points toward holistic, practice-driven education as the foundation for maritime cyber resilience.

4.3.2 *Architectural and Technical Implementations*

As M-SOCs mature, the technical architecture behind these systems has become a central focus in current research. The literature reflects a growing need for solutions that not only ensure robust cybersecurity but are also adapted to the unique operational and environmental constraints of the maritime domain, constraints like intermittent connectivity, geographically dispersed assets, and highly heterogeneous onboard systems. [12], [46]

Jacq et al. [29] provide one of the most comprehensive explorations of M-SOC architecture, detailing the design and experimental validation of a maritime-specific cybersecurity operations center. Their work goes beyond conceptual models to specify how such a center can be technically configured, integrating a range of detection, analysis, and response tools designed for remote, bandwidth-limited environments. Through practical experimentation, the study illustrates how architectural flexibility and system interoperability are essential for maintaining situational awareness across both shore-based and vessel-based infrastructures.

The paper presents a comprehensive architecture for maritime cyber-monitoring, consisting of six functional blocks for remote sites: Network Connection Safety (ensuring harmlessness on supervised systems), Network Probe Isolation (isolating each sensor), Local Preprocessor (synchronizing and normalizing data), Local Engine (storing events locally), Ship Shore Manager (managing data transmission to shore), and Cyber Situational Awareness Console (providing an overview of the onboard cyber situation).

On the shore side, the paper outlines a four-block architecture that supports the maritime cyber-monitoring system. It begins with the Ship Shore Manager (SSM), which establishes a dedicated communication channel to ensure that onboard data is transmitted to shore systems in an orderly, timely manner and within bandwidth constraints. Next, the Central Processor (CP) acts as the main aggregation point where logs, metadata, and alerts from remote vessels are filtered, normalized, and prepared for SOC analysis. The Data Store (DS) provides secure, indexed storage, typically using big data technologies to enable efficient querying and long-term retention. Lastly, the Bandwidth Manager (BM) monitors and configures bandwidth usage across remote sites, ensuring reliable connectivity and performance across the maritime network.

4.3.3 *Human Factors and Operational Considerations*

While technical innovation is vital, the real-world effectiveness of M-SOCs often hinges on something less tangible but equally critical: people. The human and organizational layers that underpin these centers—ranging from crew behavior to interdepartmental coordination—can either fortify or fracture the broader cybersecurity posture at sea.

Nganga et al. [5], [6], in two interconnected studies, emphasize that cyber resilience in shipping is deeply tied to human factors. Their research highlights a persistent gap in cyber awareness among seafarers, where a notable portion of crew members remain uncertain about their roles during a cyber incident. This gap is compounded by communication barriers between shipboard crews and shore-based M-SOC analysts—barriers that are often cultural, technical, and procedural. In high-pressure scenarios, the ability to exchange clear, context-sensitive information is crucial, and the lack of standardized communication protocols remains a key vulnerability.

Nganga et al. [5] examined the human factors that influence the adaptive response capabilities of M-SOCs in addressing vessel cyber threats. Through interviews with participants from M-SOC organizations, the authors identified several core challenges, with cyber awareness emerging as a significant domain-specific issue. The results showed that low cyber awareness among vessel owners led to insufficient investment in operational technology monitoring, while low awareness among crew members created communication challenges during incident management, with one in four seafarers not knowing what actions were required during a cyber incident.

While Nganga et al. [6] explored the enabling factors and challenges that M-SOCs face in facilitating timely detection of cyber events in the maritime domain. The authors identified incident management as the core category, supported by incident analysis, cyber onboarding, operational domain, and incident communication. The findings highlight that connectivity is a key consideration during cyber onboarding, with some M-SOCs unable to establish real-time monitoring due to connectivity challenges, while others had to prioritize monitoring critical systems due to bandwidth limitations.

Looking at another aspect, Nganga et al. [33] explore the operational complexity of responding to maritime cyber threats in a multi-stakeholder environment. Their study underscores the importance of coordinated action, where different actors, from vessel operators to port authorities, must align quickly and effectively. The challenge lies not only in the timeliness of response but also in navigating the competing priorities, jurisdictional boundaries, and varying levels of cybersecurity maturity among stakeholders.

Across these studies, a common thread that emerges is that technical infrastructure alone is not enough. Without well-trained personnel, clearly defined responsibilities, and smooth organizational integration, even the most advanced M-SOC can fall short. Human factors, often underestimated, are increasingly being recognized as central to building cyber-resilient maritime operations. The research signals a growing awareness that operational effectiveness must account for behavior, communication, and collaboration just as much as it does for firewalls and intrusion detection systems.

4.3.4 *Threat Analysis and Historical Context*

Understanding where we've been is often the clearest way to anticipate where we're headed, especially in cybersecurity. Nasr et al. [13] take this to heart by delving into the historical trajectory of maritime cyberattacks, tracing key incidents that have exposed critical vulnerabilities in maritime infrastructure. Their work doesn't just recount past failures; it builds a compelling case for why M-SOCs are not just useful, but essential.

By analyzing real-world incidents from navigation systems tampering to large-scale ransomware attacks, the article identifies recurring attack vectors and systemic weaknesses. These case studies serve as both cautionary tales and learning tools, offering a practical lens through which to model future threats. Rather than approaching M-SOC development as a theoretical exercise, the authors ground it in the realities of how cyber threats have unfolded in maritime contexts.

The study's strength lies in connecting the dots between historical breaches and the structural need for M-SOCs. It argues that without institutional memory and a clear understanding of threat evolution, security strategies risk being reactive rather than resilient. In short, history isn't just background—it's the blueprint. This perspective reinforces the idea that M-SOCs must be informed by patterns of past incidents to better anticipate and mitigate the threats of tomorrow.

4.4 *Methodological Approaches*

The research landscape of M-SOCs is shaped by a diverse mix of methodological approaches (see Figure 6), each offering a different aspect or insight into the evolving field of maritime cybersecurity.

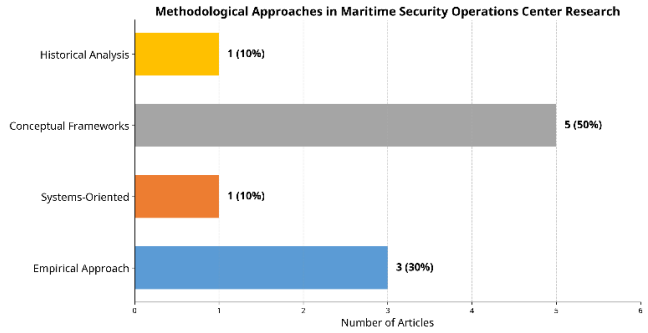

Figure 6. Methodological Approaches

One of the employed approaches is the empirical approach [5], [6], [33], where researchers conduct interviews, surveys, and real-world case studies to assess and explore the human factor and other operational challenges when it comes to M-SOC effectiveness. These efforts provide insight into how cybersecurity converges with the maritime domain on a daily basis.

In parallel, other researchers adopted a systems-oriented perspective [29], focusing on the design and technical implementation of M-SOC architecture. This study looked deeper into infrastructure-level concerns like data flow, bandwidth limitations, and system integration, highlighting the practical realities of deploying cybersecurity solutions in complex and often remote maritime environments.

Complementing this technical focus are contributions that propose conceptual models and frameworks [30], [31], [32], [34], aiming to organize thinking around core issues such as training protocols, risk assessment, and inter-organizational collaboration. These frameworks often act as blueprints for future development, guiding both policy and practice.

Finally, historical analysis plays a smaller yet impactful role in shaping methodological understanding. By examining previous cyber incidents at sea [13], researchers have begun to map patterns and vulnerabilities that inform modern security strategies. While each approach operates within its own academic or operational domain, together they form a multi-faceted research base that reflects the complexity and interdisciplinary nature required to secure maritime systems.

4.5 *Research Focus Distribution*

The current body of literature on M-SOCs reveals a distinctly multidisciplinary orientation, with research efforts spanning training and education, technical implementations, human factors, and threat analysis. Among the reviewed articles, training and education clearly lead the pack, accounting for four of the studies [30], [31], [32], [34]. This focus underscores an urgent need to build foundational expertise and operational readiness, especially given that M-SOCs are still an emerging component in maritime cybersecurity infrastructures.

Technical implementation and architectural design come next, with one study dedicated to exploring how cybersecurity systems can be effectively engineered for maritime contexts [29]. This paper reflects the growing recognition that the maritime domain presents unique technical challenges—from bandwidth limitations to the integration of legacy systems—that demand specialized solutions. Meanwhile, three articles examine human and operational dimensions [5], [6], [33], drawing attention to the critical role of personnel, communication, and organizational structure in shaping the success of M-SOC initiatives.

A single article discussed threat analysis and historical context [13], offering essential insight into the evolving nature of cyber threats at sea. Looking at all the articles together, this distribution not only illustrates the field's complexity but also hints at its developmental priorities: before advanced technologies can be fully leveraged, the industry must first cultivate the human capital and organizational awareness necessary to support them.

Using network visualization software VOSviewer for keyword co-occurrence analysis offers a precise method to map the relationships between key topics within a body of research. This technique uncovers clusters of related concepts by examining frequent keywords that appear together, providing a clear visualization of thematic structures as shown in Figure 7. [37], [38]

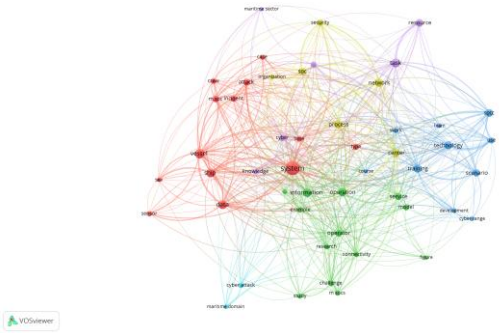

Figure 7. Keyword co-relationship analysis using network visualization in VOSviewer.

Figure 7 shows how keywords and terms from the same body of research are linked. The clusters, distinguished by color, represent thematic groupings such as red group (e.g., ship, vessel, crew) focusing on operational environments, blue group on training, technology, and teams, green group on information, connectivity, and operators, Finally the yellow group on security and M-SOC related processes. The term "system" appears as a central node, linking across

clusters, reinforcing its integrative role in M-SOC research.

Another tool is Voyant, which is an online platform for text reading and analysis with an array of visualization options like Cirrus, as shown in Figure 4. Both tools applied to review literature scope to give us the interplay between core areas to identify prevailing trends and pinpoint underexplored topics for further investigation. [36]

Figure 8. The top frequency words visualization using Cirrus word cloud in Voyant tools

In Figure 8, we observe a word cloud visualizing the most frequent and prominent terms within reviewed literature. Words like cyber, information, maritime, systems, SOC, and security appear most prominently, indicating their central role in the discussion. The visual emphasizes the thematic overlap between cybersecurity and maritime operations, suggesting that much of the research and discussion focuses on how digital security intersects with operational technology, vessel monitoring, and network systems. Terms like training, awareness, and vessel also suggest a strong human factor and operational readiness component within these conversations.

5 RESEARCH GAPS, CHALLENGES AND FUTURE RESEARCH

Based on the analysis of the review results, some significant research gaps and challenges were identified as follows:

Current research on M-SOCs reveals several foundational gaps that impede both their standardization and interoperability. Chief among these is the absence of commonly applied architectural principles or frameworks specifically designed for maritime environments. Although various studies have proposed individual components and conceptual designs, there remains no consensus on a comprehensive reference architecture tailored to M-SOCs. This absence of common frameworks in fragmented implementation efforts, inconsistent monitoring capabilities, and limited interoperability across national and regional centers.

Another notable gap in the literature is the limited availability of practical, real-world examples demonstrating how to implement M-SOC effectively. While conceptual frameworks and theoretical models are increasingly present, very few studies provide implementation scenarios. This lack of applied guidance poses a challenge for stakeholders seeking to develop or enhance their own M-SOCs. The absence of such examples leaves a critical void in supporting informed decision-making and scalable adoption across the sector. SOC literature fills this gap [47], [48], but it still requires further research for the maritime context and unique settings.

In addition, the absence of clearly defined effectiveness metrics and evaluation frameworks for M-SOC performance presents significant challenges in assessing operational outcomes. Without standardized criteria, it is difficult to quantify the impact of M-SOC initiatives or to substantiate the value of investments made in these systems. This lack of evaluative structure also limits the ability to benchmark performance across centers or to identify areas for strategic enhancement and continuous improvement. Equally concerning is the lack of cost-benefit analysis models to evaluate M-SOC investments. Some articles in SOC literature address this issue like [49], [50], [51] where the authors provided various ways to evaluate SOC performance.

Compounding this issue is the limited integration of M-SOCs within existing maritime regulatory frameworks. Regulatory misalignment not only increases the risk of non-compliance but also introduces inefficiencies as organizations attempt to reconcile operational practices with unclear or evolving regulatory demands.

Moreover, the growing shift toward autonomous vessels introduces novel risks, especially in the context of integrating M-SOCs with Remote Operations Centers (ROCs). Despite this, the literature remains sparse on strategies for securing autonomous maritime systems.

Finally, there are considerable gaps in research related to human-system interaction within maritime cybersecurity settings. The distinct operational pressures aboard vessels, such as long shifts, high-stress environments, and inconsistent technical training, affect how maritime personnel interact with M-SOC technologies. These challenges, if not addressed, can undermine the efficacy of real-time threat response.

By examining the gaps and new trends, we've pinpointed several promising directions for future research:

Developing M-SOC architectures that explore more deeply the complex nature of the maritime domain. One important issue would be intermittent connectivity, which is considered a fundamental challenge of maritime cybersecurity. Future research could focus on advanced caching mechanisms, prioritization algorithms for security data transmission, and distributed detection capabilities that function effectively even when disconnected from shore-based systems.

To improve the applicability and impact of M-SOCs, it is essential for the scientific community to

prioritize the development of reliable methodological tools. These tools must be capable of assessing, evaluating, implementing, and quantifying M-SOC effectiveness across various operational contexts.

While developing a standardized framework for M-SOCs is inherently challenging, much like it is for land-based SOCs, there are still viable opportunities to exchange cyber threat intelligence. Standardized tools and information-sharing protocols can facilitate this process. For example, Muhammed Erbas et al. (2025) have proposed adapting the widely used Malware Information Sharing Platform (MISP) for the maritime domain, demonstrating how existing technologies can support cross-organizational threat information exchange, even in the absence of a universal M-SOC architecture.

A critical area for future research involves the development of coherent and adaptive regulatory frameworks for maritime cybersecurity, especially regarding the integration of M-SOCs. Currently, many M-SOCs operate with limited alignment to existing maritime regulations, creating a fragmented landscape where cybersecurity responsibilities are often unclear or inconsistently enforced. This regulatory disconnect not only heightens the risk of non-compliance but also forces maritime organizations to navigate conflicting or ambiguous requirements, resulting in operational inefficiencies and resource strain. Future research should examine how regulatory bodies can better incorporate the role and capabilities of M-SOCs into formal compliance structures, ensuring clarity, consistency, and interoperability across international maritime domains.

Another pressing topic for future research is the cybersecurity integration between M-SOC and Remote Operations Centers (ROCs). As these vessels rely heavily on remote control, sensor networks, and real-time data exchange, they introduce a complex and largely uncharted cybersecurity landscape. The potential attack surfaces multiply, ranging from navigation systems and satellite communications to autonomous decision-making algorithms. There is an urgent need to explore how M-SOCs can be adapted or extended to monitor, secure, and respond to cyber incidents involving remotely operated or autonomous maritime assets. The task includes developing frameworks for secure data sharing, real-time anomaly detection, and coordinated incident response across distributed operational centers.

Human-centered design research for maritime security interfaces could enhance the effectiveness of security operations by making complex security information more accessible to maritime personnel with varying levels of cybersecurity expertise. This research should consider the unique operational contexts of vessels and the diverse backgrounds of maritime personnel.

Building on existing work in training and simulation, future research should develop integrated training and simulation environments that combine realistic maritime operational scenarios with sophisticated cyber-attack simulations. These environments should support both individual skill development and team-based exercises that reflect the collaborative nature of maritime security operations.

Furthermore, while existing case studies provide valuable insights, they often remain limited to site-specific or regionally focused analyses, addressing only selective aspects of M-SOCs. These studies frequently fall short in capturing the complex interactions among human agents, technological systems, and dynamic operational environments. Therefore, scaling these findings beyond localized settings is imperative.

To advance the practical understanding and operational resilience of M-SOCs, there is a pressing need to establish more real-world centers as experimental and demonstration sites. These functioning M-SOCs can serve as live testing grounds for emerging frameworks, technologies, and coordination models, allowing stakeholders to identify operational bottlenecks, unforeseen vulnerabilities, and other challenges that are difficult to capture in theoretical or simulated environments.

6 LIMITATIONS

This review is subject to several limitations that may influence the scope and applicability of its findings. The analysis was restricted to English-language, peer-reviewed publications and select grey literature, which may have excluded relevant studies from non-English-speaking regions and industry sources. As a result, the review may underrepresent regional practices and non-academic insights critical to understanding global M-SOC implementations.

A key methodological limitation is the exclusive focus on studies that explicitly address M-SOCs as primary subjects. Publications centered on related subsystems—such as threat detection, situational awareness, etc.—were excluded unless they directly framed their contributions within the M-SOC context. While this approach ensured thematic coherence, it may have led to the omission of valuable insights relevant to M-SOC functionality.

Lastly, research focused on conceptual and experimental work over empirical case studies restricts the ability to assess the operational effectiveness of M-SOCs. Inconsistencies in definitions and system architectures across the literature further complicated synthesis. Although systematic screening procedures were employed, some level of subjectivity remains in study selection and interpretation. Future research should adopt a broader inclusion strategy, encompassing multilingual sources, empirical evaluations, and studies on integrated M-SOC subsystems to support a more holistic and globally representative understanding.

7 CONCLUSIONS

Despite a growing body of work on Maritime Security Operations Centers (M-SOCs), current research only scratches the surface of what's truly needed for a comprehensive understanding. Many studies have remained within a narrow scope, focused largely on conceptual frameworks or experimental validations without evolving into full-scale, operational insights. As a result, our collective knowledge of M-SOCs

remains fragmented and, in some cases, disproportionately focused on specific elements like training, technical design, or education.

One of the most striking limitations in existing M-SOC research is its narrow geographical scope. Most studies are rooted in European or global maritime contexts, leaving vast maritime regions such as Asia-Pacific, Africa, North America, and South America largely unexplored. This regional bias risks generating a partial understanding of maritime security operations. Localized challenges, such as piracy hotspots, limited infrastructure, or different regulatory environments, remain invisible in the dominant discourse.

Moreover, the thematic focus of these studies tends to lean heavily on training indicators and system architectures. Critical categories such as implementation metrics and the specific challenges posed by small vessels remain vastly underexplored. For a more equitable and realistic perspective, future research must dive into these neglected areas and expand geographically to reflect the true global scope of maritime security operations.

On the other hand, there is a disproportionate focus on technical architecture and training programs. While those aspects are important, they don't necessarily represent the full ecosystem of maritime security operations. Implementation metrics, for instance, are rarely discussed. And considerations for small vessels are pushed to the margins despite their being the most vulnerable.

This imbalance creates a kind of tunnel vision. We end up knowing a lot about how to build or simulate an M-SOC, but very little about how it operates under pressure or how different types of vessels interact with these systems in high-risk zones. If future research doesn't broaden its scope, we'll keep designing solutions that look good on paper but fall short at sea.

Most M-SOC studies treat the system as a machine built, modeled, and evaluated through code and sensors. However, human operators are at the heart of any security operation, yet their roles, behaviors, and challenges are often ignored. Fatigue, training quality, decision-making under stress, and team dynamics are important issues and central to whether an M-SOC succeeds or fails.

Future studies need to dive deeper into the human side of maritime security operations. How do personnel interact with automated systems? How does communication flow across different units and agencies? And what happens when human judgment clashes with algorithmic recommendations? Understanding these dynamics is essential for building systems that actually work in real life.

The emphasis on conceptual and experimental research —around 70% of the reviewed literature— points to a field still in its developmental stages. Only a small fraction of studies ventures into operational assessments. That's a problem. Without empirical research grounded in real-world operations, it's nearly impossible to evaluate the actual effectiveness of M-SOCs or identify the barriers to implementation.

What we need now are more field-based studies. Longitudinal research that tracks M-SOC performance over time. Comparative analyses across regions and operational contexts. Case studies that document both success stories and failures. Only through this kind of empirical grounding can we refine our models and scale successful practices.

Another persistent issue is the lack of standardized frameworks, integration protocols, and evaluation metrics for M-SOCs. Without these, there's no clear roadmap for stakeholders—whether in industry, government, or academia—to follow. This absence not only stalls widespread adoption but also creates fragmented efforts that can't be easily scaled or compared. Future research must tackle the development of adaptable yet standardized architectures and performance benchmarks to guide effective M-SOC deployment across different operational landscapes.

Future research should prioritize developing adaptable, yet standardized, implementation guidelines and evaluation tools. These should be flexible enough to apply across diverse maritime environments but robust enough to offer reliable benchmarks. Think of it as creating a shared language for M-SOC design and evaluation—one that industry, policymakers, and practitioners can all speak.

One of the most critical limitations in M-SOC research is its fragmented nature. Studies often isolate technical systems from organizational realities or treat human operators as afterthoughts in otherwise robust frameworks, which can be seen in standard SOC literature as well. The future of M-SOC research should embrace integrated models that reflect the adaptive, interconnected nature of real-world operations. Think of maritime security not as a static blueprint but as a dynamic ecosystem, one where every change in personnel, protocol, or platform creates ripple effects across the whole system. Research must catch up to this reality.

To truly advance the field, future M-SOC research must expand in scope, deepen in substance, and diversify in context. This means shifting from theoretical modeling to real-world evaluation. Future research should be broader in scope, richer in context, and more diverse in its representation. That means moving past regionally biased studies and focusing on underrepresented maritime zones. It also means valuing human-centered design just as much as technological sophistication.

REFERENCES

[1] G. A. Weaver, B. Feddersen, L. Marla, D. Wei, A. Rose, and M. Van Moer, "Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach," Transp Res Part C Emerg Technol, vol. 137, p. 103423, Apr. 2022, doi: 10.1016/J.TRC.2021.103423.

[2] J. I. Alcaide and R. G. Llave, "Critical infrastructures cybersecurity and the maritime sector," Transportation Research Procedia, vol. 45, pp. 547–554, 2020, doi: 10.1016/J.TRPRO.2020.03.058.

[3] F. Martínez, L. E. Sànchez, A. Santos-Olmo, D. G. Rosado, and E. Fernàndez-Medina, "Maritime cybersecurity: protecting digital seas," Int J Inf Secur, pp. 1–29, Jan. 2024, doi: 10.1007/S10207-023-00800-0/TABLES/6.

[4] A. Zolich et al., "Survey on Communication and Networks for Autonomous Marine Systems," Journal of

Intelligent and Robotic Systems: Theory and Applications, vol. 95, no. 3–4, pp. 789–813, Sep. 2019, doi: 10.1007/S10846-018-0833-5/METRICS.
[5] A. Nganga, J. Scanlan, M. Lützhöft, and S. Mallam, "Enabling cyber resilient shipping through maritime security operation center adoption: A human factors perspective," Appl Ergon, vol. 119, p. 104312, Sep. 2024, doi: 10.1016/J.APERGO.2024.104312.
[6] A. Nganga, G. Nganya, M. Lützhöft, S. Mallam, and J. Scanlan, "Bridging the Gap: Enhancing Maritime Vessel Cyber Resilience through Security Operation Centers," Sensors 2024, Vol. 24, Page 146, vol. 24, no. 1, p. 146, Dec. 2023, doi: 10.3390/S24010146.
[7] J. Direnzo, D. A. Goward, and F. S. Roberts, "The little-known challenge of maritime cyber security," IISA 2015 - 6th International Conference on Information, Intelligence, Systems and Applications, Jan. 2016, doi: 10.1109/IISA.2015.7388071.
[8] C. Parka, W. Shib, W. Zhangb, C. Kontovas, and C.-H. Changa, "Cybersecurity in the maritime industry: a literature review".
[9] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED." Accessed: Jun. 02, 2025. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[10] "Maritime cyber risk." Accessed: May 30, 2025. [Online]. Available: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
[11] "NIS 2 Directive) (Text with EEA relevance".
[12] C. Bueger and T. Liebetrau, "Critical maritime infrastructure protection: What's the trouble?," Mar Policy, vol. 155, Sep. 2023, doi: 10.1016/J.MARPOL.2023.105772.
[13] A. N. Nasr, R. Leiger, I. Zaitseva-Pärnaste, and P. Kujala, "Exploring Historical Maritime Cyber-Attacks and Introducing Maritime Security Operations Center as a Solution to Mitigate Them," Progress in Marine Science and Technology, vol. 9, pp. 235–245, Nov. 2024, doi: 10.3233/PMST240042.
[14] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," IEEE Access, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.
[15] "What Is a Security Operations Center (SOC)? | IBM." Accessed: Jun. 19, 2025. [Online]. Available: https://www.ibm.com/think/topics/security-operations-center
[16] Y. Baddi, M. A. Almaiah, O. Almomani, and Y. Maleh, "The art of cyber defense: From risk assessment to threat intelligence," The Art of Cyber Defense: From Risk Assessment to Threat Intelligence, pp. 1–310, Nov. 2024, doi: 10.1201/9781032714806.
[17] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A tale of three security operation centers," Proceedings of the ACM Conference on Computer and Communications Security, vol. 2014-November, no. November, pp. 43–50, Nov. 2014, doi: 10.1145/2663887.2663904.
[18] S. Schinagl, K. Schoon, and R. Paans, "A framework for designing a security operations centre (SOC)," Proceedings of the Annual Hawaii International Conference on System Sciences, vol. 2015-March, pp. 2253–2262, Mar. 2015, doi: 10.1109/HICSS.2015.270.
[19] D. Pati and L. N. Lorusso, "How to Write a Systematic Review of the Literature," HERD, vol. 11, no. 1, pp. 15–30, Jan. 2018, doi: 10.1177/1937586717747384.
[20] W. Mengist, T. Soromessa, and G. Legese, "Ecosystem services research in mountainous regions: A systematic literature review on current knowledge and research gaps," Science of The Total Environment, vol. 702, p. 134581, Feb. 2020, doi: 10.1016/J.SCITOTENV.2019.134581.
[21] A. García-Holgado, S. Marcos-Pablos, and F. J. García-Peñalvo, "Guidelines for performing systematic research projects reviews," International Journal of Interactive Multimedia and Artificial Intelligence, vol. 6, no. 2, pp. 136–144, 2020, doi: 10.9781/IJIMAI.2020.05.005.
[22] W. Mengist, T. Soromessa, and G. Legese, "Method for conducting systematic literature review and meta-analysis for environmental science research," MethodsX, vol. 7, p. 100777, Jan. 2020, doi: 10.1016/J.MEX.2019.100777.
[23] M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," Health Info Libr J, vol. 26, no. 2, pp. 91–108, Jun. 2009, doi: 10.1111/J.1471-1842.2009.00848.X.
[24] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research," MethodsX, vol. 9, p. 101895, Jan. 2022, doi: 10.1016/J.MEX.2022.101895.
[25] I. Fernández del Amo, J. A. Erkoyuncu, R. Roy, R. Palmarini, and D. Onoufriou, "A systematic review of Augmented Reality content-related techniques for knowledge transfer in maintenance applications," Comput Ind, vol. 103, pp. 47–71, Dec. 2018, doi: 10.1016/J.COMPIND.2018.08.007.
[26] A. Martín-Martín, E. Orduna-Malea, M. Thelwall, and E. Delgado López-Cózar, "Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories," J Informetr, vol. 12, no. 4, pp. 1160–1177, Nov. 2018, doi: 10.1016/J.JOI.2018.09.002.
[27] E. S. Vieira and J. A. N. F. Gomes, "A comparison of Scopus and Web of science for a typical university," Scientometrics, vol. 81, no. 2, pp. 587–600, Apr. 2009, doi: 10.1007/S11192-009-2178-0/METRICS.
[28] A. Mucedola, "Toward a better future through maritime security," Meeting Security Challenges Through Data Analytics and Decision Support, pp. 133–142, Jan. 2016, doi: 10.3233/978-1-61499-716-0-133.
[29] O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, and J. Simonin, "Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre," 2018 2nd Cyber Security in Networking Conference, CSNet 2018, Jan. 2019, doi: 10.1109/CSNET.2018.8602669.
[30] B. Nikolov, "A Concept for Establishing a Security Operations and Training Centre at the Bulgarian Naval Academy," vol. 46, no. 1, pp. 27–35, 2020, doi: 10.11610/isij.4602.
[31] M. Raimondi, G. Longo, A. Merlo, A. Armando, and E. Russo, "Training the Maritime Security Operations Centre Teams," Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022, pp. 388–393, 2022, doi: 10.1109/CSR54599.2022.9850324.
[32] P. de La Vallée, G. Iosifidis, A. Rossi, M. Dri, and W. Mees, "Sector-Specific Training - A Federated Maritime Scenario," Communications in Computer and Information Science, vol. 1689, pp. 21–35, Jan. 2022, doi: 10.1007/978-3-031-20215-5_3.
[33] A. Nganga, M. Lützhöft, J. Scanlan, and S. Mallam, "Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment," 2022.
[34] B. M. Nikolov, "Improving Cybersecurity Capabilities at Nikola Vaptsarov Naval Academy by Building and Developing a Security Operations and Training Center," Communications in Computer and Information Science, vol. 1790 CCIS, pp. 219–242, 2023, doi: 10.1007/978-3-031-44440-1_30/FIGURES/5.
[35] "Publish or Perish." Accessed: May 22, 2025. [Online]. Available: https://harzing.com/resources/publish-or-perish
[36] "Voyant Tools." Accessed: May 22, 2025. [Online]. Available: https://voyant-tools.org/

[37] "VOSviewer - Visualizing scientific landscapes." Accessed: May 22, 2025. [Online]. Available: https://www.vosviewer.com/
[38] N. J. van Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," Scientometrics, vol. 84, no. 2, pp. 523–538, Jan. 2010, doi: 10.1007/s11192-009-0146-3.
[39] R. Hopcraft, "Developing Maritime Digital Competencies," IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 12–18, Sep. 2021, doi: 10.1109/MCOMSTD.101.2000073.
[40] K. Kanwal, W. Shi, C. Kontovas, Z. Yang, and C. H. Chang, "Maritime cybersecurity: are onboard systems ready?," Maritime Policy and Management, vol. 51, no. 3, pp. 484–502, Apr. 2024, doi: 10.1080/03088839.2022.2124464;CTYPE:STRING:JOURNAL.
[41] "Home - Suricata." Accessed: Jun. 19, 2025. [Online]. Available: https://suricata.io/
[42] "Splunk | The Key to Enterprise Resilience." Accessed: Jun. 19, 2025. [Online]. Available: https://www.splunk.com/
[43] "Home | Moodle.org." Accessed: Jun. 19, 2025. [Online]. Available: https://moodle.org/?lang=en
[44] "Prometheus - Monitoring system & time series database." Accessed: Jun. 19, 2025. [Online]. Available: https://prometheus.io/
[45] "Grafana: The open and composable observability platform | Grafana Labs." Accessed: Jun. 19, 2025. [Online]. Available: https://grafana.com/
[46] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector," Network 2022, Vol. 2, Pages 123-138, vol. 2, no. 1, pp. 123–138, Mar. 2022, doi: 10.3390/NETWORK2010009.
[47] R. Vaarandi and S. Mäses, "How to Build a SOC on a Budget," 2022, doi: 10.1109/CSR54599.2022.9850281.
[48] Joseph. Muniz, Gary. McIntyre, and Nadhem. AlFardan, "Security operations center : building, operating, and maintaining your SOC," 2016.
[49] I. Taqafi, Y. Maleh, and K. Ouazzane, "A MATURITY CAPABILITY FRAMEWORK FOR SECURITY OPERATION CENTER," EDPACS, vol. 67, no. 3, pp. 21–38, 2023, doi: 10.1080/07366981.2023.2159047.
[50] P. Danquah, "Security Operations Center: A Framework for Automated Triage, Containment and Escalation," Journal of Information Security, vol. 11, pp. 225–240, 2020, doi: 10.4236/jis.2020.114015.
[51] M. Rosso, M. Campobasso, G. Gankhuyag, and L. Allodi, "SAIBERSOC: Synthetic Attack Injection to Benchmark and Evaluate the Performance of Security Operation Centers; SAIBERSOC: Synthetic Attack Injection to Benchmark and Evaluate the Performance of Security Operation Centers", doi: 10.1145/3427228.