IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 February 2026, accepted 3 March 2026, date of publication 12 March 2026, date of current version 17 March 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3673557

RESEARCH ARTICLE

A Proactive Defense: An Open-Source Intelligence (OSINT) Framework for Maritime Cybersecurity

AHMED NAGI NASR[1], AYBARS ORUÇ[1], RICARDO LUGO[1], INGA ZAITSEVA-PÄRNASTE[2], AND PENTTI KUJALA[1]

[1]Estonian Maritime Academy, Tallinn University of Technology, 11712 Tallinn, Estonia
[2]Kuressaare College, Tallinn University of Technology, 93811 Kuressaare, Estonia

Corresponding author: Ahmed Nagi Nasr (ahmed.nasr@taltech.ee)

This work was supported in part by the DIGIMARIS Project under Grant CB0600317, in part by the European Union under the Interreg Central Baltic Programme 2021-2027, in part by the CyberSecPro Project under Grant 101083594, in part by the European Union's Digital Europe Programme; and the MariCybERA Project under Grant 952360, and in part by the European Union's Horizon 2020 Research and Innovation Programme.

ABSTRACT The accelerating digital transformation of the maritime industry, driven by the widespread adoption of Internet of Things (IoT) devices, integrated vessel systems, and automated port operations, has significantly expanded its cyber-attack surface, rendering it increasingly vulnerable to sophisticated threats. This study investigates the application of Open-Source Intelligence (OSINT) as a proactive, scalable, and cost-effective methodology for enhancing maritime cybersecurity. We present a specialized maritime OSINT framework comprising a systematic five-phase workflow (Identification, Collection, Processing, Analysis and Dissemination) tailored to the sector's unique operational and threat landscape. The framework is supported by a comprehensive taxonomy of maritime cyber threats and a curated toolkit of over 100 OSINT resources, spanning vessel tracking, corporate intelligence, digital reconnaissance, and analytical platforms. Through applied case studies, we demonstrate how this approach can identify critical vulnerabilities such as exposed operational technology, weak software supply chain links, and human-factor risks derived from publicly accessible data. Our findings confirm that maritime OSINT provides an indispensable intelligence layer, enabling stakeholders to transition from reactive security postures to proactive risk management through early threat detection, informed vulnerability assessment, and enhanced situational awareness, while adhering to the proposed ethical and legal guidelines for responsible intelligence collection.

INDEX TERMS Cyber threat intelligence, maritime cybersecurity, maritime operations, maritime OSINT, open-source intelligence, OSINT, threat prevention.

I. INTRODUCTION

The maritime industry is undergoing rapid and extensive digitalization across all aspects of the domain. Although this technological integration promises enhanced productivity and streamlined operations, it simultaneously expands the attack surface. With over 80% of international trade relying on maritime transportation [1], it is crucial to secure and protect the different aspects of the sector from cybersecurity challenges. Cyberattacks on the maritime industry have increased by a staggering 900% in recent years [2]. It is sensible to implement additional security layers [3].

This digital transformation includes automation in ports, integration of IoT devices on vessels, and establishment of interconnected logistics systems. Unfortunately, a single vessel often presents a complex security environment, simultaneously operating cutting-edge technologies alongside very old legacy systems, further complicating compliance with evolving regulations such as the Network and Information Systems (NIS)-2 Directive (EU 2022/2555) [4], which mandates stringent cybersecurity risk management for maritime operators and the International Maritime Organization (IMO—the UN agency responsible for regulating shipping) resolution MSC.428(98) [5], requiring cyber risks to be addressed under the International Safety Management (ISM) Code (an international standard for the safe management and operation of ships) [6]. Maritime

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

organizations are high-value targets for various threat actors. Current security practices are often reactive, stressing the need for proactive intelligence capabilities, such as Open-Source Intelligence (OSINT), to anticipate and mitigate threats [7], [8].

OSINT can be weaponized by malicious actors to plan and execute targeted attacks against maritime assets by exploiting the very data intended for safety and transparency. By systematically analyzing OSINT sources, adversaries can identify high-value targets through unexplained loitering patterns and route anomalies, which may signal vessels carrying sensitive cargo or operating under duress.

For example, the Automatic Identification System (AIS) is a standard tracking system used globally to monitor vessel positions, routes, and identities in real time, which can be utilized to detect deliberate gaps in transmission or inconsistencies that indicate spoofing. Attackers can pinpoint vessels attempting to conceal their movements, making them vulnerable to interception, piracy, or cyber-physical attacks. Additionally, by mapping broader traffic patterns within strategic chokepoints or politically sensitive areas, malicious actors can identify optimal times and locations for ambushes, smuggling operations, or coordinated cyber intrusions, turning publicly available maritime data into a tactical blueprint for disruption and exploitation.

The primary objective of this study is to leverage this specialized framework to empower maritime stakeholders with a proactive, cost-effective capability for early threat detection, vulnerability identification, and enhanced situational awareness, thereby enabling a shift from reactive security postures to preventive risk management. Beyond the framework itself, this study makes two additional contributions:

First, it introduces a structured analytical approach that transforms raw OSINT findings into actionable intelligence through vulnerability categorization, severity ranking, and mapping to established frameworks such as MITRE ATT&CK [9].

Second, it provides practical guidance for organizational adoption through a tiered integration model that enables maritime stakeholders of all sizes to operationalize OSINT within the existing governance structures and regulatory compliance frameworks.

The study follows a structured methodological framework organized into five key phases: identification, where strategic objectives are defined; collection, where data are systematically gathered from public sources; processing, where data are cleaned and normalized; analysis, where processed data are examined to extract intelligence; and dissemination, where findings are synthesized into actionable reports. Throughout this workflow, a variety of OSINT tools are utilized, each aligned with the goals of the corresponding phase. These tools were identified through a dedicated research process to assemble a practical toolkit tailored for the maritime domain. This research is primarily methodological and framework-oriented in nature. Rather than presenting quantitative experimental results, it offers a structured, repeatable process for maritime OSINT collection and analysis, validated through a qualitative case study.

This study investigates the potential of OSINT to enhance maritime cybersecurity, with a primary focus on preventive measures. The novelty of this study lies in the development of a comprehensive and actionable OSINT framework specifically tailored to the maritime cybersecurity context, a contribution that fills a significant gap in the existing literature. While prior research has acknowledged the value of OSINT, this study provides a holistic, step-by-step methodology for its implementation, complete with a taxonomy of maritime cyber threats and a systematic process for collecting and analyzing data from diverse public sources such as AIS, Shodan, and crew social media.

The remainder of this paper is organized as follows. Section II establishes the necessary background by detailing OSINT principles, the maritime cybersecurity landscape, key threat actors, and prevalent attack vectors. Section III reviews the related work and positions our contribution within the existing scholarly discourse. Section IV presents the core of our research: a detailed maritime OSINT methodology, including a five-phase intelligence workflow, a discussion of the research process behind the compilation of a categorized toolkit, and a critical examination of ethical and legal considerations. Section V details the resulting taxonomy of maritime OSINT tools. Section VI demonstrates the practical application of the proposed framework through a case study, validating its utility in identifying real-world vulnerabilities. Section VII discusses the findings, emphasizing organizational integration, process development, and human factors in maritime cybersecurity. Finally, Section VIII concludes the paper by summarizing the key contributions and outlining directions for future research.

II. BACKGROUND

This background section begins by establishing the fundamental role of OSINT and demonstrating how the vast, publicly accessible digital footprint of the industry can be weaponized by threat actors. It then delves into the specific methodologies of passive and active OSINT, highlighting the emerging threat of AI-enhanced attacks that automate profiling and phishing. This section subsequently maps the complex maritime cybersecurity landscape, emphasizing the convergence of Information Technology (IT) and Operational Technology (OT) as a key vulnerability. Finally, it categorizes diverse threat actors and analyzes the primary attack vectors they exploit, from network intrusions and satellite communication compromises to social engineering and supply chain attacks. Together, these elements frame a sector under mounting pressure, where increasing digitalization is met with sophisticated and multifaceted cyber threats.

A. OPEN-SOURCE INTELLIGENCE (OSINT)

Open-Source Intelligence (OSINT) is the practice of gathering and analyzing information that is freely and legally accessible to the public for purposes such as threat assessment and

cybersecurity. OSINT plays a vital role in staying informed and responding effectively using deductions derived from aggregated data [10], [11].

From pictures to videos to other forms of digital media, people are increasingly sharing personal information online, and the same applies to the maritime domain. With proper tools and social engineering skills, malicious actors can gain access to sensitive information, such as passwords, or even extort someone [11].

For example, we can obtain a lot of information related to the maritime sector from public records and websites such as MarineTraffic [12]. Namely, we can find the vessel's IMO number, Maritime Mobile Service Identity (MMSI) numbers, dimensions, owner, current location, and even its departure and destination ports. For some vessels, information about past crew members may also be accessible. All this information can be obtained by knowing the name of the vessel. Over time, bad actors can build a dossier with sufficient crucial information, then plan and launch various attacks, ranging from physical assaults (e.g., piracy and smuggling) to sophisticated cyber intrusions that exploit vulnerabilities in the vessel's systems [13].

An excessive amount of sensitive information is shared intentionally or unintentionally. Some threat actors can build extensive and detailed profiles about vessels or other sensitive maritime infrastructure by collecting and processing freely available information.

B. PASSIVE OSINT AND ACTIVE OSINT IN MARITIME

Passive OSINT involves collecting and analyzing publicly available information without directly interacting with the target systems or individuals. In the maritime context, this includes gathering data from official registries, vessel tracking platforms such as MarineTraffic, regulatory publications, crew social media profiles, and industry news sources. Maritime organizations routinely generate a significant digital footprint across these open sources, which can be harvested to build comprehensive threat intelligence profiles without alerting the target of the threat. For instance, researchers can analyze AIS data, port records, and satellite imagery to detect suspicious activities, such as AIS blackouts or sanction-evading vessel movements, while remaining undetected by potential adversaries [14]. Passive collection enables maritime security teams to identify vulnerabilities using tools such as Shodan without intrusive scanning, thereby supporting proactive threat hunting and situational awareness. As discussed in Section IV-C, practitioners must navigate data protection regulations, such as the GDPR, by ensuring purpose limitation and data minimization.

Active OSINT involves deliberate interaction with target systems or individuals to elicit information from them. In maritime cybersecurity, this may include probing publicly accessible network services, querying exposed APIs, conducting targeted social engineering, or using penetration-testing tools to validate vulnerabilities identified through passive means. Simulating attack scenarios, such as phishing campaigns, using scraped crew data or testing weak credentials on shipboard Wi-Fi terminals help organizations assess their resilience to real-world attacks by mimicking adversary behaviors to uncover security gaps that passive collection alone might miss [15]. However, active OSINT incurs higher legal and operational risks, as it may involve accessing systems without explicit authorization or interacting with personnel under a pretext. Therefore, strict ethical guidelines, proportionality, and clear operational boundaries are essential. For example, penetration testing teams collaborating with OSINT units must ensure that their activities are scoped, authorized, and designed to enhance security—not to disrupt operations or violate privacy. When properly integrated into maritime security workflows, active OSINT provides actionable threat validation, strengthens defensive simulations, and helps organizations transition from reactive to proactive cyber defense.

Recent findings highlight how Artificial Intelligence (AI) has significantly increased the efficiency and effectiveness of cyberattacks. Heiding et al. [16] demonstrated that AI-powered phishing tools can automatically gather information from public sources, build detailed vulnerability profiles, and generate personalized phishing emails with a 54% success rate, which is 350% more effective than traditional ''spray-and-pray'' phishing attempts. When applied to the maritime context, this means that attackers could rapidly collect data on vessel crew members from professional networks, leaked credentials, or shipping company websites and launch convincing phishing attacks masquerading as legitimate port authority messages or safety information.

Moreover, AI now enables large-scale automated personality profiling of targets, making phishing attempts more persuasive. Buraya et al. [17] showed that personality attributes can be inferred by fusing data from multiple social media platforms, providing a 360° behavioral profile of an individual. Similarly, Liu et al. [18] found that even subtle cues, such as social media profile picture choices, can reliably predict the Big Five personality traits. By combining these methods, attackers can infer whether a maritime officer is highly agreeable, extroverted, or conscientious, and tailor phishing content to exploit these psychological tendencies. This aligns with the findings of Eftimie et al. [19], who demonstrated that spear-phishing emails designed to manipulate traits such as high agreeableness or extraversion substantially increase the likelihood of victims clicking on malicious links or disclosing sensitive information.

In a realistic maritime attack scenario, an AI-driven adversary could scrape OSINT sources to map a vessel's exposed digital assets, identify crew members' online profiles, and infer their personality traits from the posted content and images. The AI system can then craft hyper-personalized phishing emails appearing to come from trusted logistics partners or fleet management services, designed to exploit the specific cognitive biases of individual targets. The automation of OSINT trawling and psychological

profiling drastically reduces the time and expertise required for sophisticated attacks, increasing both their scale and success rate. These findings highlight the critical importance of integrating human-factor defenses alongside traditional technical measures in maritime cybersecurity strategies [16], [17], [18], [19].

C. MARITIME CYBERSECURITY LANDSCAPE

Cyberattacks targeting the maritime sector are a reality that must be acknowledged and protected against. The increasing number of attacks is a result of the rapid integration of advanced technologies into various aspects of this domain. Ships are becoming more digitally interconnected, and as a result, their growing digital footprint presents opportunities for cyber adversaries to exploit them [20].

Recent research in maritime cybersecurity [21], [22], [23] has revealed an increasing sophistication in threats and their potential for serious disruption. One of the key findings is the unique nature of maritime cybersecurity, particularly how the convergence of Information Technology (IT) and Operational Technology (OT) introduces entirely new attack surfaces.

Researchers have identified five primary domains of vulnerability within the maritime sector: vessel navigation systems, cargo management, port operations, shipping company networks, and broader supply chain communication. Among these, vessel systems stand out as particularly exposed, largely due to their heavy reliance on Global Navigation Satellite Systems (GNSS), which are susceptible to jamming and spoofing attacks [21], [24], [25].

For example, AIS can be disrupted or deliberately turned off, leading to what is known as ''AIS blackouts''. Such gaps obscure a vessel's activities, raising concerns, especially in politically sensitive areas or during suspicious operations [26].

D. THREAT ACTORS

The cyber threat landscape in maritime environments is evolving and becoming increasingly complex. Various threat actors with different motivations and skill levels attempt to circumvent security defenses. Therefore, it is logical to identify and understand their tactics and techniques to adapt and protect our systems effectively. Based on a retrospective analysis of past maritime cyber incidents and intelligence, we can categorize threat actors into the following:

State-sponsored actors typically target maritime assets with strategic, economic, or military relevance. These actors launch attacks for a multitude of reasons, such as intelligence collection of maritime infrastructure, operational disruption, or strategic leverage. Their operations often employ sophisticated techniques, such as zero-day exploits, advanced persistent threats (APTs), and long-term infiltration campaigns to evade detection and maximize their impact [27], [28].

Cybercriminal organizations and individuals target maritime operations for financial gain through ransomware, business email compromise, and cargo theft facilitation. The high value nature of maritime assets and their critical role in global trade make this sector a prime target for exploitation. Ransomware groups have specifically attacked shipping companies and port operators [27].

Hacktivists target maritime organizations for ideological reasons. These actors, often environmental or labor rights activists, turn maritime systems into battlegrounds for their causes. Unlike financially motivated cybercriminals, hacktivists attack primarily to grab as much attention as possible to gain press and media coverage [29]. Attacks on Maritime IT systems, such as website defacement, distributed denial-of-service (DDoS) campaigns, or data breaches leading to leaked sensitive information, have publicity and reputational damage, especially with social media involved, increasing the attack impact on shipping companies, port authorities, or maritime regulatory bodies [30], [31].

Finally, insider threats from current or former employees with access to operational maritime systems or sensitive data pose a significant risk to maritime organizations [32]. Due to the extensive knowledge of internal systems, operational processes, and security controls that these actors gain during their employment, the impact of damage can be severe or even catastrophic [33]. Insiders may act with malicious intent due to personal grievances, coercion, or financial incentives, intentionally compromising networks or leaking sensitive data [34], [35].

E. ATTACK VECTORS

Cyberattacks threaten maritime operations through diverse attack vectors, each leveraging unique aspects of maritime systems, processes, and human elements. To build strong defenses and guide security investments, it is crucial to understand these vectors. Analysis of past maritime cyber incidents emphasizes several common and successfully exploited attack methods against maritime targets [22].

Network-based attacks target interconnected systems within the maritime sector, including corporate networks, ship communication platforms, and port management infrastructure, many of which rely on outdated legacy systems with known vulnerabilities. These attacks commonly exploit weaknesses such as outdated software, weak user authentication, and misconfigured network settings. A real-world example is the 2023 cyberattack on Det Norske Veritas (DNV)'s ShipManager software, a widely used fleet management system. The breach, which affected over 1,000 vessels, disrupted operations and forced DNV to isolate its servers, highlighting the risks posed by aging infrastructure in critical maritime IT systems [36], [37].

Vessel operations relying on Very Small Aperture Terminals (VSAT) and other satellite systems are susceptible to cyberattacks because of inherent vulnerabilities in satellite communication [38], particularly when integrated with outdated legacy systems that lack modern security patches. Research indicates that common maritime satellite equipment often exhibits weaknesses, such as weak encryption, persistence of default credentials, and exploitable firmware flaws [39]. These risks were demonstrated in the 2022

cyberattack on Iranian oil tankers, where hackers exploited satellite communication systems to disrupt navigation and spoof GPS data, causing operational chaos and forcing vessels onto unintended routes. This incident underscores how legacy maritime technologies can become critical liabilities when left unsecured [35].

Social engineering preys on maritime personnel through tactics like phishing, pretexting, and business email compromise (BEC) [40]. These attacks bypass technical defenses by exploiting human factors, often leveraging specialized industry knowledge to craft believable scams. APTs sophisticated, long-term cyberattacks typically backed by nation-states or organized crime frequently employ such methods to infiltrate maritime targets. A prime example is the multi-year spear phishing campaign uncovered by EclecticIQ, where attackers impersonated shipping companies and sent weaponized Excel and Word documents that are embedded with malware. The attackers employed several exploits in order to execute the shellcode. The APT group exfiltrated sensitive data via Simple Mail Transfer Protocol (SMTP), demonstrating how social engineering enables persistent access for financial gain or espionage [40], [41].

Supply chain compromises exploit the intricate web of vendors, service providers, and contractors that support maritime operations [42]. Attackers infiltrate primary targets by compromising trusted third parties to hijack legitimate channels for unauthorized access. The catastrophic 2017 NotPetya attack on Maersk, triggered by a compromised Ukrainian accounting software vendor, exemplifies this risk: the malware crippled 49,000 workstations and 7,000 servers, paralyzing ports globally for weeks. The incident caused $300M in losses, underscoring how supply chain breaches can devastate business continuity, disrupt cargo operations, contractual obligations, and just-in-time logistics [42], [43], [44], [45].

Operational technology exploitation targets industrial control systems governing ship propulsion, navigation, and port cargo handling. The 2020 cyberattack on Iran's Shahid Rajaee port exemplifies this: attackers disrupted gate controls and traffic systems, causing days of cargo backlog and reputational damage. Similarly, in 2023 the port of Rotterdam suffered a distributed denial of service (DDoS) attack—a cyberattack that disrupts services by overwhelming them with excessive traffic—attributed to pro-Russian hackers. Such incidents reveal how IT-OT convergence creates novel risks like malware jumping from corporate networks to critical OT infrastructure [46], [47], [48].

III. RELATED WORK

There are only a few studies that explore the intersection of maritime operations and OSINT, and each adopts a distinct methodology and focus. While existing research demonstrates the potential of OSINT for improving maritime situational awareness, cybersecurity, and operational integrity, these works often differ in scope—ranging from privacy and ethical considerations to simulation-based training and real-world case studies.

Tanabe et al. [49] situate OSINT within the broader intelligence cycle, arguing that while it is formally a collection discipline, its effective execution inherently involves processing and analysis techniques. The authors present a comparative study of established OSINT cycles from entities like Bellingcat (an investigative journalism collective specializing in open-source analysis) and the Berkeley Protocol (United Nations-endorsed guidelines for digital open-source investigations) and propose a unified method that integrates OSINT techniques—such as those for text, technical, and social media analysis—into a workflow that can be combined with other intelligence disciplines (HUMINT, SIGINT, etc.) for all-source analysis. This work is highly relevant as it provides a formal, process-oriented perspective on OSINT, which complements the application-specific frameworks discussed elsewhere and reinforces the need for a structured, technique-driven methodology to be adopted within the maritime domain.

Rajamäki et al. [50] examine the intersection of OSINT and Big Data Analytics (BDA) in maritime surveillance, focusing particularly on privacy challenges within the Maritime Integrated Surveillance Awareness (MARISA) project. The study highlights how OSINT and BDA are vital for maritime security operations—enabling data fusion from multiple open sources like AIS signals, social media, and global news datasets—but also raise serious ethical and legal concerns regarding personal data protection. Emphasizing the principles of Privacy by Design (PbD) and compliance with General Data Protection Regulation (GDPR), Rajamäki argues that privacy must be embedded into surveillance systems from the start to maintain public trust and prevent misuse of sensitive data. The paper concludes that while OSINT-driven maritime awareness systems enhance security and operational efficiency, they must balance intelligence value with individual rights and algorithmic accountability to ensure responsible and transparent data use.

Lovell and Heering [51] present Exercise Neptune, a simulator-based maritime cybersecurity training program developed at Tallinn University of Technology to enhance seafarers' awareness and response to cyber threats. Using navigational bridge simulators, the exercise replicates real-world maritime environments and incorporates OSINT techniques to simulate cyberattacks on ship systems such as Electronic Chart Display and Information Systems (ECDIS), AIS, and Global Maritime Distress and Safety Systems (GMDSS). Participants successfully exploited vulnerabilities and uncovered sensitive data, including North Atlantic Treaty Organization (NATO) ship credentials and operational details shared via social media and public platforms. The study highlights the critical role of human behavior and digital footprints in maritime cybersecurity, demonstrating how small, individual data leaks can collectively expose operational weaknesses. The authors conclude that effective cybersecurity training must move beyond technical awareness to foster a culture of shared responsibility, integrating cyber hygiene into everyday maritime operations

and simulator-based drills that reflect realistic threat scenarios.

Sage [52] explores the use of OSINT as a practical tool for maintaining situational awareness and operational continuity when electronic tracking systems like the Automatic Identification System (AIS) fail or are intentionally manipulated. The authors emphasize that AIS disruptions, whether caused by cyberattacks, legal restrictions, or deliberate spoofing, can have serious consequences for maritime safety, global trade, and geopolitical stability. Through a detailed case study tracking sanctioned Russian oil exports, the paper demonstrates how freely available OSINT tools—including satellite imagery, webcam feeds, Social Media Intelligence (SOCMINT), and company and sanctions databases—can be used to identify vessels, verify shipping activities, and uncover links between seemingly legitimate maritime actors and sanctioned entities. The findings reveal that OSINT not only compensates for AIS blind spots but also provides contextual intelligence about the people, companies, and behaviors driving vessel operations. Ultimately, the study positions maritime OSINT as a cost-effective, ethical, and adaptable intelligence method that enhances sanctions compliance, maritime transparency, and operational security in an increasingly complex and digitally interconnected maritime landscape.

Kanellopoulos [53] addresses the growing cyber threats facing the maritime sector—including ransomware, navigation system tampering, and cargo data theft—and emphasizes the necessity of a proactive Cyber Counterintelligence (CCI) strategy to safeguard shipping operations. The study outlines key CCI measures such as continuous monitoring, threat intelligence collection, vulnerability assessments, and employee training, while also underscoring the importance of collaboration and information sharing among industry stakeholders. Although the paper does not focus explicitly on OSINT, its emphasis on proactive intelligence gathering and cross-sector collaboration aligns closely with the goals of maritime OSINT frameworks, thereby reinforcing the value of open-source methods in enhancing situational awareness and cyber resilience within the shipping industry.

Building on these foundations, the current study aims to address a significant gap in existing literature by proposing a comprehensive, structured, and directly applicable OSINT framework tailored specifically to maritime cybersecurity. While previous works have explored discrete aspects of the intersection, such as privacy ethics, training simulations, or targeted case studies, there remains a need for an integrated methodology that bridges strategic principles with hands-on, operational execution. Existing research often isolates specific challenges or tools without offering a holistic workflow that maritime security practitioners can systematically adopt. This paper seeks to unify these fragmented insights into a cohesive framework that not only details the necessary steps, tools, and techniques but also embeds them within the practical realities and constraints of maritime operations. Importantly, this includes providing a curated and categorized toolkit of over 100 OSINT resources, which includes vessel tracking, corporate intelligence, digital reconnaissance, geospatial analysis, and threat assessment, specifically selected for their relevance to the maritime domain.

IV. METHODOLOGY

The methodology presented in this section is designed as a practical framework for maritime OSINT practitioners. It is not intended as an experimental design requiring quantitative validation, but rather as a structured, qualitative approach to intelligence gathering that can be adapted and refined based on operational context.

This section begins by detailing the research process undertaken to identify and catalog relevant OSINT tools. Given the scarcity of academic literature focusing specifically on maritime OSINT tooling, this compilation was derived from practitioner blogs, industry reports, cybersecurity forums, and the application of generic OSINT tools to maritime use cases. Following this, the core of the methodology is presented: a tailored maritime OSINT workflow that adapts the fundamental intelligence cycle to the unique challenges and data streams of the maritime environment. Finally, the section concludes with a critical examination of the ethical and legal considerations that must govern all maritime OSINT activities, ensuring operations are responsible, compliant, and focused on legitimate security objectives.

A. OSINT TOOLS RESEARCH PROCESS

The catalog of tools presented in this research was assembled from a range of public sources to address a gap in literature. While academic journals, industry reports, and cybersecurity publications provided critical context on maritime security and OSINT methodologies, they seldom offer detailed lists of operational tools. To build a practical toolkit, the research expanded into the broader OSINT and cybersecurity communities.

This involved reviewing practitioner blogs, security conference materials, and technical forums where tools are actively discussed and evaluated. The primary focus was on identifying general-purpose OSINT, geospatial, and network security tools that could be effectively applied to maritime targets—such as using search engines like Shodan [54] to locate exposed shipboard systems, or platforms like MarineTraffic [12] to analyze vessel movements. Tools were assessed based on their relevance to core maritime data streams like AIS, satellite imagery, vessel registries, and corporate records.

This approach ensures the resulting compilation is not merely theoretical but reflects tools used in practice. The list serves as a functional, applied resource tailored to the unique intelligence requirements of the maritime domain.

B. MARITIME OSINT WORKFLOW

OSINT workflow is structured around the core phases of intelligence (see Figure 1) [55], which provides a systematic framework for conducting maritime OSINT investigations.

The process begins with ***Identification*** phase, where the intelligence requirements and the target's specific information environment are defined. This is followed by the ***Collection*** phase, involving the methodical gathering of data from the diverse array of maritime-specific sources previously outlined. The raw data then undergoes ***Processing*** phase to be cleaned, normalized, and structured into a usable format. Subsequently, the ***Analysis*** phase transforms this processed information into actionable intelligence by identifying patterns, relationships, and threats. Finally, ***Dissemination*** phase where the findings are disseminated to relevant stakeholders in a format that supports decision-making and security operations. The following sections will examine each of these phases in detail, with a focus on their unique application and challenges within the maritime domain [56].

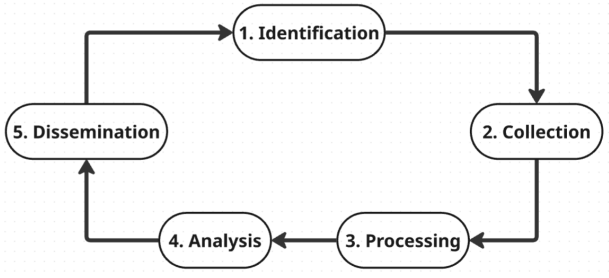

FIGURE 1. Cyber investigation phases flowchart [55].

This methodology is inherently iterative, requiring periodic execution and continuous refinement to ensure the compilation of a comprehensive and up-to-date dossier on the target.

1) PHASE ONE: IDENTIFICATION

The identification phase is the critical first step in any maritime OSINT investigation. Here, analysts move from a general objective to a specific plan by systematically mapping and evaluating the information landscape relevant to their target, such as a specific vessel or port. This involves surveying available data streams—including AIS trackers, satellite imagery, official registries, port records, and cybersecurity databases—to determine which sources are most credible, accessible, and relevant. The goal is to build a tailored collection strategy that will efficiently yield insights into the target's operations, affiliations, or digital exposure.

Within maritime security and cybersecurity, this phase is foundational for proactive defense. By identifying the right sources upfront—such as technical scans for exposed network devices or compliance records—analysts can accurately model a target's attack surface and operational patterns. This enables the prioritization of monitoring efforts and supports the design of defensive measures based on a clear understanding of the target's real-world information footprint, ensuring all subsequent analysis is focused and actionable.

2) PHASE TWO: COLLECTION

The collection phase is the operational execution of the OSINT workflow, where data is systematically gathered from the sources identified during the planning stage. In the maritime context, this involves harvesting raw, publicly available data from a diverse array of streams. Analysts concurrently collect terrestrial and satellite AIS positions, vessel registration details from international and flag-state databases, port call records, satellite imagery, and relevant maritime compliance filings. This stage emphasizes breadth and methodical capture, ensuring a comprehensive dataset for subsequent analysis.

For maritime cybersecurity, the collection scope extends to technical and adversarial sources. Investigators actively gather data from network scanning tools like Shodan or Censys to identify exposed shipboard or port Industrial Control Systems (ICS), harvest indicators of compromise from threat intelligence feeds, and monitor relevant forums, social media, and dark web channels for discussions on maritime-specific vulnerabilities or threat actor activity. This multi-source aggregation, combining operational, administrative, and technical data, creates the essential evidence base for identifying anomalies, profiling potential threats, and uncovering digital exposure points within the maritime domain.

3) PHASE THREE: PROCESSING

The processing phase transforms the raw data gathered during collection into a structured, reliable dataset ready for analysis. In maritime OSINT, this involves the critical tasks of cleaning, normalizing, and validating disparate data streams. AIS feeds, port records, satellite imagery metadata, and technical scan results are decoded, sorted, and integrated. Duplicate entries are removed; time stamps are synchronized to a common standard, and corrupted or anomalous records—such as impossible vessel speeds or locations—are flagged for review. This process converts a vast volume of unstructured information into a coherent, accurate foundation.

This stage is particularly vital for maritime cybersecurity applications, where data integrity directly impacts threat assessment. Processing includes verifying the authenticity of technical data, such as correlating Shodan scan results with known network architectures, and translating forum or threat feed information into actionable indicators of compromise (IoCs). By structuring the data into a searchable and correlated format—often within a dedicated analysis platform or database—the phase ensures that subsequent analytical efforts are focused on verified, relevant information, enabling precise pattern recognition and vulnerability identification.

4) PHASE FOUR: ANALYSIS

The analysis phase represents the transition from structured data to actionable intelligence. Using the cleansed dataset from the processing stage, maritime OSINT investigators employ analytical techniques to identify patterns, relationships, and anomalies. This involves correlating disparate data points—such as mapping a vessel's AIS track against its port call records and ownership history—to reconstruct timelines, establish behavioral baselines, and detect deviations like loitering in sensitive areas or spoofed positional data.

The core objective is to synthesize information from technical scans, regulatory filings, and open-source reports to develop a coherent narrative about the target's operations, affiliations, or security posture.

Within the domain of maritime cybersecurity, analysis focuses explicitly on threat and vulnerability assessment. Analysts examine processed data to identify digital exposure points, such as unprotected network services on shipboard systems, and correlate these findings with threat intelligence on active exploitation campaigns. By connecting technical vulnerabilities with contextual data, analysts can prioritize risks and predict potential attack vectors, for example, a vessel's itinerary or the software versions disclosed in a procurement notice. This phase demands rigorous cross-verification from multiple sources to ensure accuracy, as the insights generated directly inform critical decisions regarding threat mitigation, defensive resource allocation, and overall maritime security resilience.

5) PHASE FIVE: DISSEMINATION

Dissemination is the final stage of the intelligence cycle, and it is essential to maritime OSINT, particularly for proactive cyber defense. Sharing insights with maritime authorities, vessel operators, port security, and regulators ensures that key stakeholders understand emerging threats and the digital exposure of ships, ports, and navigation systems.

This process also builds practical awareness of data privacy, AIS vulnerabilities, and risks from unsecured onboard networks. Equipped with this knowledge, crews and operators can handle sensitive data more carefully, reducing the likelihood of targeted incidents. Proactively, it enables investigators to better detect communication anomalies, identify compromised systems, and evaluate threats like spoofed MMSI profiles or Global Positioning System (GPS) manipulation.

Furthermore, effective dissemination ensures that open-source intelligence, such as vessel-tracking data and port-network metadata, is used to anticipate attacks rather than merely respond. When integrated early in the OSINT process, shared findings help shape strategic defenses, guiding resource allocation and monitoring tools to stay ahead of potential adversaries.

C. ETHICAL AND LEGAL CONSIDERATIONS

This section examines the essential ethical and legal boundaries that govern responsible OSINT activities within the maritime domain. It navigates the delicate balance between acquiring actionable security intelligence and upholding fundamental rights and legal obligations. The discussion begins with privacy considerations, emphasizing principles like data minimization and purpose limitation to prevent overreach. It then explores the complex legal frameworks, including data protection regulations and cybersecurity information-sharing protocols, that practitioners must operate within. Finally, it establishes core ethical guidelines for conducting OSINT, arguing that legitimacy, proportionality, and transparency are not merely compliance checkboxes but the foundation of credible and responsible maritime threat intelligence.

1) PRIVACY CONSIDERATIONS

When conducting maritime OSINT operations, privacy is critical to responsible intelligence work. Handling personal and corporate data comes with serious ethical and operational responsibilities, and it starts with a clear commitment to data minimization. In other words, only collect what is truly necessary. The focus should remain on security-relevant information, not on sweeping up personal details about crew members, passengers, or company staff that have no bearing on the threat landscape [57].

Purpose limitation is equally important. OSINT activities should be guided by clearly defined objectives specifically tied to maritime security. It's essential to avoid missions creeping into unrelated areas like employee surveillance or corporate espionage. Alongside that, well-thought-out data retention policies are key. Information should be held only as long as it is needed, with timelines based on how sensitive or operationally useful the data is. That balance between security and privacy helps maintain trust while keeping the intelligence function sharp and focused.

2) LEGAL FRAMEWORKS

Maritime OSINT does not operate in a vacuum; it is shaped by several legal frameworks that often span multiple jurisdictions. One of the biggest legal challenges comes from data protection laws. Regulations like GDPR lay out strict rules for how personal data must be handled during OSINT activities. That means everything from how information is collected and analyzed to how long it is stored and with whom it is shared, needs to follow clearly defined legal standards [58].

In addition to privacy laws, there are also legal frameworks governing how security intelligence is shared between private maritime organizations and government entities. Many jurisdictions now have formal processes for cybersecurity information exchange, often backed by liability protections and strict procedural guidelines. The European Union Agency for Cybersecurity (ENISA) Guidelines for Subject Matter Experts (SMEs) [59] on the security of personal data processing provide critical direction for maritime OSINT practitioners handling sensitive information. These guidelines emphasize that risk-based measures such as data minimization, encryption of datasets, and strict access controls are key considerations when processing crew details, port worker records, or vessel ownership data obtained from open sources. For OSINT practitioners, understanding and working within these legal boundaries is foundational to both compliance and operational credibility [60].

3) ETHICAL GUIDELINES

Ethics in maritime OSINT go well beyond following a legal checklist; they are responsible for disciplined conduct. First off, intelligence efforts must have a legitimate purpose,

focusing squarely on safeguarding vessels, crew, cargo, and critical systems. It is not about acquiring a competitive edge or pursuing goals unrelated to security [61].

Then there's proportionality, which is all about balance. The level of data collection and analysis should match the actual security risk; no over-the-top snooping when less intrusive methods can do the job. Finally, transparency matters. While some operational details will naturally stay under wraps, maritime organizations should strive to be open with relevant stakeholders about their intelligence activities. This builds trust and keeps everyone aligned on the mission.

V. MARITIME OSINT TOOLS

This section presents a comprehensive OSINT investigative toolkit for maritime security, structured into a modular framework of interconnected investigative domains. It begins by establishing the foundational capability of vessel and port facility tracking, which provides the critical geospatial and temporal baseline for all subsequent analysis. From this starting point, the research expands into deeper layers of intelligence: administrative and regulatory research to uncover corporate ownership and compliance; personnel profiling to assess social engineering risks; geospatial and environmental analysis to understand the operational context; and digital infrastructure reconnaissance to map cyber vulnerabilities. Finally, it details the analytical and threat assessment tools that synthesize these disparate data streams into actionable intelligence, enabling the identification of hidden relationships, assessment of vulnerabilities, and evaluation of complex threats. Together, these six categories form a complete workflow for transforming raw, publicly available data into a strategic understanding of maritime entities, activities, and risks.

A. VESSEL AND PORTS FACILITY TRACKING

The ability to monitor vessel movements and maritime traffic constitutes a foundational capability within maritime OSINT. This category provides the essential data layer for establishing the target's operational baseline, including its real-time location, historical routes, speed, and port call patterns. The primary data source for this analysis is AIS, which can be described as a publicly broadcast signal designed for collision avoidance and maritime domain awareness [62]. By aggregating and visualizing this data, investigators can reconstruct a vessel's past activities, identify deviations from expected behavior, such as:

- Unexplained loitering,
- Route anomalies,
- Gaps in transmission that may indicate spoofing,
- Map broader patterns of traffic within strategic chokepoints or sensitive areas.

Practical application of this methodology is enabled by a diverse ecosystem of specialized platforms and resources (see Appendix Table 1). This continuous tracking forms the critical temporal and geospatial framework upon which subsequent layers of technical, visual, and contextual intelligence are overlaid, serving as the indispensable first step in developing a comprehensive understanding of any maritime entity or activity.

B. ADMINISTRATIVE AND REGULATORY MARITIME INTELLIGENCE

The strategic value of corporate and official registry intelligence lies in its ability to explore the legal and administrative corners of the maritime domain. While vessel tracking reveals where a ship is, these resources answer the critical questions of who controls it, how it is managed, and its operational standing. By mapping corporate hierarchies, verifying ownership through official documents, and assessing financial and regulatory compliance, investigators can transform a vessel identifier into a comprehensive OSINT profile. This layer of intelligence is indispensable for exposing complex ownership structures used for sanctions' evasion, identifying companies with poor safety records indicative of higher operational risk, and linking maritime assets to broader financial networks, thereby providing the essential context that turns observed movement into actionable strategic insight.

These types of tools (see Appendix Table 2) are most powerful when their data is correlated and analyzed in combination, revealing insights that isolated data points cannot provide. For example, using OpenCorporates to uncover a complex ownership web linked to a vessel found on Worldships.com, and then investigating the financial risk of that parent company via Lloyd's List Intelligence, creates a complete threat assessment.

C. CREW AND OFFICE PERSONNEL

While platforms designed for crew recruitment and maritime networking serve a legitimate commercial purpose, they also represent a significant vector for information leakage. A proactive security assessment must acknowledge that these resources are routinely exploited by malicious actors to harvest personnel data, including crew identities, certifications, employment histories, and vessel associations. This harvested intelligence can facilitate sophisticated social engineering, targeted phishing campaigns, or the mapping of operational patterns, thereby directly threatening maritime security and operational integrity. Consequently, a core component of personnel security involves continuously auditing/monitoring these platforms (see Appendix Table 3) to identify and mitigate the exposure of sensitive information that could be leveraged for adversarial purposes.

1) GEOSPATIAL, ENVIRONMENTAL, AND INFRASTRUCTURE INTELLIGENCE

Geospatial, environmental, and infrastructure intelligence provides the foundational physical and contextual layer for maritime OSINT. This category of tools (see Appendix Table 4) moves analysis beyond the vessel's track to understand the operational environment. It enables investigators to analyze navigational routes using nautical charts

(OpenSeaMap), conduct detailed visual reconnaissance of ports and coastal infrastructure (Google Earth, Soar Atlas), and incorporate real-time weather and oceanographic data (Windy) to explain vessel behavior or assess voyage feasibility. Critically, it also maps critical subsea assets like telecommunications cables, allowing for the assessment of vulnerabilities where maritime activity intersects with global infrastructure. By fusing this geospatial and environmental data with movement and corporate intelligence, a complete, multi-dimensional picture of maritime operations and risks emerges.

D. DIGITAL INFRASTRUCTURE, SOCIAL RECONNAISSANCE AND CYBER-THREAT INTELLIGENCE

Once an initial foothold on a vessel's technological systems is established through network scanning (Shodan, Censys), an investigator can deploy a suite of IT-oriented OSINT approaches to deepen the intelligence picture. This includes using tools like Sherlock and Hunter.io to collect data on crew and personnel, building profiles from names and email addresses discovered in domain records (ViewDNS.info, Crt.sh). These identifiers can then be leveraged to "dive deeper," checking for credential exposures on Have I Been Pwned or cross-referencing with social media activity. Concurrently, vulnerability databases (CVE.org) and threat intelligence platforms (AlienVault OTX) contextualize technical findings, while dark web searches (Ahmia) and conflict data (ACLED) provide insight into the adversarial and operational environment.

The digital OSINT tools and techniques (see Appendix Table 5) represent a curated selection for maritime applications rather than an exhaustive catalogue. While a vast body of literature details OSINT methodologies for generic cybersecurity and IT environments, the focus here is explicitly on their adaptation and relevance to the unique attack surface and intelligence requirements of the maritime sector. Consequently, emphasis is placed on tools that excel at probing maritime-specific technologies (e.g., exposed shipboard ICS), correlating personnel data with physical operations, and contextualizing findings within the global shipping ecosystem.

E. ANALYTICAL AND THREAT ASSESSMENT TOOLS

The final analytical phase employs specialized tools (see Appendix Table 6) to transform raw maritime data into actionable intelligence. Link analysis platforms like Maltego are critical for visualizing the complex relationships between vessels, corporate owners, and ports, revealing hidden ownership structures. Concurrently, vulnerability scanners (Nmap, OpenVAS) probe the digital attack surface of shipboard and port systems, while threat intelligence resources (ONI Worldwide Threat Reports or GPS Interference Map) provide essential context on regional piracy, conflict, and navigation warfare risks. Frameworks such as the OSINT Framework guide investigators to relevant sources, and technical utilities like the Equasis CLI enable bulk data processing. This integrated analytical layer synthesizes technical, corporate, and geospatial findings to produce comprehensive risk assessments and support decisive maritime security actions.

VI. IMPLEMENTATION OF MARITIME OSINT TO PORT OF TULUM

Building on prior research [63] and [64], which has extensively explored IoT-based and broader cyberattacks targeting maritime systems, our research introduces an OSINT-driven dimension to this domain. While previous efforts focused primarily on technical vulnerabilities and network-level threats, we expand the threat landscape by incorporating publicly available intelligence. For example, using data gathered from Shodan to craft targeted phishing campaigns aimed at compromising credentials for onboard Wi-Fi terminals.

By combining traditional cyber reconnaissance with OSINT techniques, such as identifying exposed services or login portals, we reveal additional attack vectors that could be exploited without triggering system in-place alerts. This fusion not only broadens the adversarial perspective but also emphasizes the importance of considering both technical and human-layer vulnerabilities in maritime cybersecurity assessments.

Such an approach enables comprehensive utilization of the diverse range of data available through OSINT. This information can be strategically applied to support preventive measures, including threat hunting, vulnerability assessments, and the development of early warning systems.

Staying ahead of the curve and closely examining the digital footprint of both the organization and its personnel, it becomes possible to identify potential security exposures before they can be exploited. Platforms intended for crew networking, vessel tracking, or industry transparency are routinely exploited by malicious actors to harvest personnel data, map operational patterns, and identify targets for social engineering or cyberattacks. Therefore, a proactive defense must include auditing these resources from an adversarial perspective to identify and mitigate information leakage.

A. CASE STUDY: PROACTIVE OSINT ASSESSMENT OF THE PORT OF TULUM, EREWHON

Note that the case study presented in this section is based on a fictional port (the Port of Tulum) to avoid real-world targeting and ensure ethical compliance; it is designed to illustrate the practical application of the framework rather than to report on an actual security assessment

This case study applies the maritime OSINT framework outlined in Section IV-B to conduct a proactive security assessment of the Port of Tulum, a fictional but representative mid-sized port in Erewhon. The objective is not to disrupt operations, but to demonstrate how publicly accessible information can be systematically gathered, analyzed, and used to identify potential vulnerabilities in physical, digital, and human security layers.

Port Overview (Based on Provided Data):

- Country: Erewhon
- Port Authority: Port of Tulum Authority
- Location: Seiduna 987-55, Tulum
- Contact: info@porttulum.com | http://www.porttulum.com

Coordinates: Latitude 99.45°N, Longitude 80.05°E (Note: fictional coordinates for exercise)

1) PHASE ONE: IDENTIFICATION

The purpose of this phase is to define the specific intelligence requirement and scope of the assessment, establishing the key focal points that will guide the subsequent investigation.

The intelligence requirement, which is defined as: ''Map the digital and administrative footprint of Tulum Port to identify potential vulnerabilities exploitable by a threat actor.''

Key focal points included:

- Publicly accessible IT/OT systems.
- Personnel information (management, IT staff, security).
- Operational schedules and vessel traffic.
- Physical layout and key infrastructure.

2) PHASE TWO: COLLECTION

This phase involves systematically gathering relevant raw data from diverse public sources, including vessel tracking, corporate records, digital infrastructure scans, and geospatial imagery, to build a comprehensive information baseline.

Data was gathered from multiple open sources:

Maritime Traffic & Scheduling (MarineTraffic [12]/ VesselFinder [65]):

- Live AIS data showed regular cargo and container ship traffic.
- Historical data revealed patterns: peak activity on weekdays, frequent calls from regional feeder vessels.
- Example AIS screenshot showing vessel M/V Erewhonian Pride docked at Berth 3, with publicly visible cargo manifest metadata.

Administrative & Corporate Intelligence:

- Website Analysis (porttulum.com): The ''Management'' page listed names and titles:
  - Director: E... V...
  - IT Manager: M... T...
  - Harbor Master: Captain I... V...
- Email Pattern Discovery: Standard format identified: first.last@porttulum.com.
- LinkedIn & Professional Networks: Profiles found for targeted personnel, revealing career history, certifications, and professional connections.

Digital Infrastructure Reconnaissance (Shodan [54]/ Censys [66]):

- Search query: org:''Port of Tulum Authority'' and net:''192.0.2.0/24'' (hypothetical range).
- Findings:
  - Multiple exposed Industrial Control System (ICS) devices (SCADA interfaces) with web login panels.
  - An unprotected network-attached storage (NAS) device with a port documents folder indexed.
  - Several IPs running ''MikroTik RouterOS'' with default credentials or outdated firmware.
  - An exposed Remote Desktop Protocol (RDP) service on a server labeled ''Tulum-Port-Mgmt''.

Geospatial & Infrastructure Intelligence:

- Google Maps [67] / OpenStreetMap [68]: High-resolution imagery showed the layout of gates, cranes, admin buildings, and perimeter fencing.
- Submarine Cable Map: A major fiber-optic cable landed near the port's data center location.

3) PHASE THREE: PROCESSING

The purpose here is to organize, filter, and structure the collected raw data into a usable format, such as databases and inventories, to prepare it for effective analysis.

- Data was organized into structured tables:
  - Personnel Database: Names, roles, emails, social links.
  - Asset Inventory: IPs, open ports, services, vulnerabilities.
  - Operational Timeline: Vessel arrivals/departures, shift changes.
- Raw Shodan data was filtered to highlight critical exposures: RDP, default logins and unpatched services.

4) PHASE FOUR: ANALYSIS

In this phase, the processed data was systematically analyzed and evaluated to transform raw findings into actionable intelligence. To move beyond a descriptive account and provide a structured assessment, we categorized the identified vulnerabilities, ranked their potential severity, and mapped them to the MITRE ATT&CK framework [9], a globally recognized knowledge base of adversary tactics and techniques.

Categorization and Severity Ranking of Findings

The intelligence gathered was grouped into four thematic categories reflecting different layers of the port's attack surface: Digital Infrastructure, Human/Personnel, Operational, and Physical. Each finding was then assessed for its potential severity, considering both the ease of exploitation and the potential impact on port operations (see Appendix Table 7).

Synthesis of Risk Scenarios

Cross-referencing the data within this structured framework revealed several high-probability, high-impact attack scenarios that an adversary could develop using this OSINT:

Scenario 1: Targeted Ransomware Attack (Digital + Human): An attacker could use the identified email format (first.last@porttulum.com) and the LinkedIn profiles of the IT Manager and other staff to craft a highly believable spear-phishing email. If successful, this could provide a foothold in the corporate network, from which they could pivot to the exposed RDP service or unpatched network devices. This access could then be used to deploy ransomware, potentially disrupting terminal operating systems and causing significant

operational delays, as seen in historical incidents like the NotPetya [45].

Scenario 2: Operational Disruption via ICS Manipulation (Digital): The discovery of exposed ICS interfaces presents a direct and critical threat. An adversary could attempt to gain access to these systems using default credentials (common in OT environments) or by exploiting known vulnerabilities. Successful access could allow them to manipulate cargo handling equipment, cranes, or gate systems, causing physical damage and prolonged operational standstill, reminiscent of the cyberattack on Iran's Shahid Rajaee port [48].

Scenario 3: Credential Harvesting and Network Pivot (Human + Digital): Using the identified personnel data, an attacker could set up credential harvesting pages mimicking the port's VPN or email login portals. Compromised credentials for a high-level user, such as the Harbor Master or a system administrator, could then be used to directly access internal systems via the exposed RDP service, bypassing perimeter defenses.

This structured analysis demonstrates that OSINT is not merely a data-gathering exercise but a powerful analytical capability. By categorizing, ranking, and mapping findings to established threat frameworks, we can move from simple observation to the prediction of specific, credible attack paths. This allows security teams to prioritize remediation efforts on the most critical risks rather than reacting to every piece of exposed data equally.

5) PHASE FIVE: DISSEMINATION

The final purpose is to communicate the analytical findings and tailored recommendations in a clear, actionable report to the relevant stakeholders, enabling informed decision-making and security improvements.

A classified threat report was drafted for port management, summarizing:

- Critical Risks: Unsecured ICS devices, exposed management interfaces.
- Medium Risks: Employee information leakage, predictable credentials.
- Recommendations:
  - Segment OT networks from the public internet.
  - Enforce multi-factor authentication on all external services.
  - Conduct cybersecurity awareness training for staff.
  - Regularly audit digital footprints using OSINT tools.

VII. DISCUSSION

This discussion section interprets the practical findings of the maritime OSINT framework, translating methodology into actionable security strategy. It begins by addressing the often-overlooked human factor, demonstrating how OSINT reveals personnel-related vulnerabilities that form the backbone of social engineering attacks. The section then outlines the essential pillars for organizational implementation, detailing the necessary integration structures, standardized processes, and continuous training required to operationalize intelligence. Furthermore, it reflects on the implications drawn from the Port of Tulum case study, highlighting the framework's value in enabling proactive, cost-effective risk management. Finally, it concludes with a critical examination of the framework's inherent limitations.

A. HUMAN FACTOR: THE MISSING PIECE

By systematically collecting and analyzing publicly available data such as exposed ports, service banners, login interfaces, and even crew information, analysts can uncover vulnerabilities without engaging in intrusive activities. Tools like Shodan allow researchers to monitor maritime digital footprints in real time, revealing unsecured services or outdated firmware on vessel-based systems. When paired with social engineering insights, such as email addresses, domain structures, or crew habits found online, this intelligence becomes a foundation for constructing realistic attack simulations and assessing resilience against potential phishing campaigns or password reuse attacks.

More importantly, integrating OSINT into existing threat hunting workflows enables early detection of anomalies and suspicious behavior patterns. For instance, if a vessel satellite terminal appears in Shodan with default credentials or is associated with known vulnerable software, this can trigger a risk flag long before an exploit is attempted. Likewise, when OSINT feeds are combined with internal logs or vulnerability scanners, security teams gain a more complete picture of their exposure, allowing them to prioritize patching, improve network segmentation, and harden systems against both opportunistic and targeted attacks.

B. ORGANIZATIONAL INTEGRATION

Effective implementation requires seamless integration of OSINT practices into existing maritime security operations. A clear definition of roles and responsibilities is essential, spanning from OSINT collection specialists to analysts and end users of the collected intelligence. Depending on the organization's size and available resources, these roles may be filled with dedicated personnel or incorporated into the duties of existing security teams. Penetration testing or pentesting teams should collaborate closely with OSINT units, using open-source findings to simulate targeted attacks. For example, phishing campaigns based on scraped crew profiles or spoofed AIS data [69].

Integrating OSINT into security operations ensures that intelligence insights translate directly into actionable security measures. This involves establishing clear workflows that link intelligence findings to security controls, incident response protocols, and informed risk management decisions [70].

Resource allocation for OSINT integration should align with the organization's size, threat landscape, and overall security maturity. While smaller maritime organizations can

TABLE 1. Vessel and port facility platforms.

No.	Platform Name	Link	Primary Use in Maritime OSINT
1	MarineTraffic	marinetraffic.com	Used to visualize global shipping traffic, monitor specific vessels in near real-time, analyze port activity, and access ship particulars and photos.
2	VesselFinder	vesselfinder.com	
3	Myshiptracking	myshiptracking.com	
4	Shipfinder	shipfinder.co	
5	VesselTracker	vesseltracker.com	
6	ShippingExplorer	shippingexplorer.net	
7	HiFleet	hifleet.com	Analyzes fleet compositions, trade patterns, and vessel technical specifications for market intelligence.
8	AIS Hub	aishub.net	Serves as a valuable source for raw, community-sourced AIS data, useful for accessing feeds in regions with limited commercial coverage.
9	PocketMariner	pocketmariner.com	Utilized for mobile, on-the-go vessel tracking and navigation reference, particularly useful for field observations.
10	CruisingEarth	cruisingearth.com	Used to obtain visual, real-time confirmation of a vessel's presence in port via live webcam feeds, supplementing AIS data.
11	NoForeignLand	noforeignland.com/map/	Leveraged to gather crowd-sourced intelligence from the cruising community on vessel locations, anchorages, and local conditions.
12	Cruise Mapper	cruisemapper.com	Specifically used to track cruise ship itineraries, monitor fleet movements, and access schedules and deck plans for this vessel class.
13	Superyachts.com	superyachts.com	Used to investigate the luxury yacht market, identify ownership (via sale/charter listings), and track specific high-value assets.
14	TankerTrackers	tankertrackers.com/report/sanctioned	Used to identify and monitor vessels that are officially sanctioned or engaging in clandestine activities like ship-to-ship transfers.
15	Planet Insights	insights.planet.com	Used to task and analyze high-frequency satellite imagery to monitor port infrastructure, shipbuilding activity, or track vessels over time.
16	Copernicus Browser	browser.dataspace.copernicus.eu	Used to freely access and download high-resolution Sentinel satellite radar (SAR) and optical imagery for wide-area maritime surveillance.
17	Bellingcat SAR Ship Detection Tool	ollielballinger.users.earthengine.app/view/ship-detection-tool	Specifically used to programmatically search vast archives of SAR satellite data to locate and identify vessels in any weather, day or night.
18	Shipspotting.com	www.shipspotting.com	Used to find photographic evidence of a vessel's appearance, modifications, past names (livery), and historical locations.
19	SkylineWebcams	skylinewebcams.com/en/live-cams-category/seaport-cams.html	Used for live visual verification of vessel presence, activity, and conditions at major ports worldwide.
20	Worldcam	worldcam.eu	Used to discover and access a broad network of public webcams that may offer views of ports, waterways, or coastal areas of interest.

adopt basic OSINT practices with minimal investment, larger entities may benefit from building comprehensive intelligence functions supported by dedicated staff and specialized analytical tools [71].

C. PROCESS DEVELOPMENT

Having well-defined processes in place is key to ensuring consistency and methodological discipline across maritime OSINT efforts. Structured workflows—starting from the initial information needed all the way to the final OSINT-based product—help turn scattered data into insightful information. When adapted to the maritime context, the intelligence cycle typically includes defining requirements, planning the collection, gathering relevant information, processing and analyzing it, testing the collected data via penetration testing to validate findings (e.g., stress-testing identified vulnerabilities like exposed ship systems or weak credentials), and refining intelligence priorities before delivering actionable insights to support real decision-making in compliance with IMO Guidelines on Maritime Cyber Risk Management [72].

To keep intelligence efforts aligned with real-world security needs, requirements management becomes essential. This includes regular reviews, prioritization frameworks, and feedback loops to assess whether the intelligence being produced is meeting operational goals. On top of that, quality control plays a critical role. Applying analytical standards and involving independent reviews all help ensure that the final intelligence products are accurate, unbiased, and genuinely useful to those making security decisions.

D. TRAINING AND AWARENESS

Running effective maritime OSINT operations isn't just about having the right tools; it takes people with the right skills and domain knowledge, a requirement reinforced by both NIS-2 Directive Article 21, which mandates cybersecurity training for critical sectors, including maritime transport [73], and IMO's ISM Code, which emphasizes crew competency in risk management [6]. Different roles demand different expertise. While all team members need a solid grasp of intelligence fundamentals, those working in maritime environments also need a strong understanding of operational realities at sea, how ships move, how port systems work, and what normal looks like in that domain [74].

TABLE 2. Administrative and regulatory maritime intelligence platforms.

No.	Platform Name	Link	Primary Use in Maritime OSINT
1	ILO/IMO Joint Database on Abandonment of Seafarers	wwwex.ilo.org/dyn/r/abandonment/seafarers/home	Investigates vessel or company history of labor violations and seafarer welfare issues as risk indicators.
2	Equasis.org	equasis.org/EquasisWeb/public/HomePage	Accesses ship safety inspections, detention records, and company performance for operational risk assessment.
3	International Telecommunication Union's Maritime Mobile Access and Retrieval System (ITU MARS)	itu.int/mmsapp/shipstation/list	Identifies and verifies vessel maritime mobile service identity (MMSI) numbers to support radio communications tracking and AIS authentication.
4	Global Integrated Shipping Information System (GISIS)	webaccounts.imo.org/Common/WebLogin.aspx?App=GISISPublic	Researches official IMO documentation including company details, pollution incidents, and vessel certificates.
5	HELCOM	maps.helcom.fi/website/mapservice	Used to monitor environmental and maritime safety data, incident reports, and shipping activities specifically within the Baltic Sea region.
6	International Commercial Chamber (ICC) Commercial Crime Services (CCS)	icc-ccs.org/map	Used to research piracy and armed robbery incident reports, as well as check vessels against the ICC's database for involvement in maritime fraud.
7	PortTechnology.org	porttechnology.org	Gathers intelligence on port security systems, terminal operations, and cybersecurity technologies.
8	Marine Cadastre (U.S.)	hub.marinecadastre.gov/pages/vesseltraffic	Visualizes jurisdictional boundaries, offshore infrastructure, and vessel routes in U.S. waters.
9	Sea-Distances.org	sea-distances.org	Calculates port-to-port distances and durations to validate vessel itineraries and identify travel anomalies.
10	National Geospatial-Intelligence Agency (NGA)	msi.nga.mil/Publications/SDEnroute	Provides authoritative navigational intelligence, coastal descriptions, and maritime safety notices for regional activity assessment.
11	OpenCorporates	opencorporates.com	Maps corporate hierarchies, identifies beneficial owners, and traces vessel ownership across jurisdictions.
12	Lloyd's List Intelligence	lloydslistintelligence.com	Conducts commercial due diligence and assesses financial and geopolitical risk for shipping companies and vessels.
13	Black Book Online	blackbookonline.info/Maritime-Public-Records.aspx	Provides consolidated access to official maritime records for vessel documentation and ownership verification.
14	World-ships.com	world-ships.com	Provides central lookup for vessel identification details and integrates ownership data with real-time AIS positions.
15	BoatInfoWorld.com	boatinfoworld.com	Researches recreational and small commercial vessels not found in major maritime databases.
16	Marine Link	marinelink.com	Monitors industry news, company announcements, and maritime technology trends.
17	Maritime Database	maritime-database.com	Compiles shipping company profiles, identifies key personnel, and analyzes fleet compositions.
18	Regs4ships	regs4ships.com	Searches international maritime regulations to verify vessel and company compliance posture.

But it does not stop at the initial training. Continuous learning is essential to keep pace with evolving threats, technologies, and shifting geopolitical dynamics. That means regular training refresher, threat briefings, and chances for professional growth. Additionally, organizational awareness efforts help people outside the security team, like crew members or port operators, understand how intelligence fits into the bigger picture. When they see how their day-to-day observations contribute to broader threat awareness, the whole system becomes more responsive and resilient.

E. ETHICAL AND OPERATIONAL NOTES

All information was obtained from publicly accessible sources only. No systems were accessed without authorization. The exercise adhered to the ethical guidelines in Section IV-C, with purpose limitation and data minimization strictly observed. The fictional "Port of Tulum" was used to avoid real-world targeting.

F. IMPLICATIONS FOR MARITIME SECURITY

The case study of the Port of Tulum validates several key principles of the proposed framework. First, it demonstrates that OSINT provides a low-cost, high-value layer of threat intelligence that is accessible to ports and maritime organizations of all sizes, enabling proactive risk assessment without significant capital investment. Additionally, the assessment underscores that human factors remain the weakest link in maritime cybersecurity; personnel data—including names, roles, and professional associations—is frequently and unintentionally exposed via corporate websites, professional networking platforms, and third-party data breaches.

This exposure reinforces the necessity for proactive and continuous monitoring of an organization's own digital footprint. The intelligence gathered during this exercise was sourced entirely from publicly accessible information, underscoring a fundamental truth: what is visible to security researchers is equally visible to adversaries. Therefore,

TABLE 3. Crew and office personnel platforms.

No.	Platform Name	Link	Primary Use in Maritime OSINT
1	Crewlinker	crewlinker.com	Analyzes crewing needs and hiring patterns to assess company operational tempo and expansion.
2	Crewbay	crewbay.com	Researches personnel and activities in the private and recreational sailing sector.
3	Crewseekers	crewseekers.net	Gathers intelligence on the global yachting community and vessel or skipper movements.
4	Findacrew	findacrew.com	Identifies connections between vessels, skippers, and crew within the global boating network.
5	Sfsailing.com	sfsailing.com/sailing/index.cfm/crewlist/crew_main	Monitors local San Francisco sailing forum for crew positions and recreational sailing activity.
6	Sailorshub.in	sailorshub.in	Finds seafarer profiles, monitors industry discussions, and gathers career and certification details.
7	OceanCrew.org	oceancrew.org	Analyzes job postings to identify active shipping companies and potential fleet expansions.
8	CoBoaters	coboaters.com	Maps personal connections and activity patterns in the private recreational boating community.
9	NGO Shipbreaking Platform	shipbreakingplatform.org	Investigates end-of-life vessels, shipbreaking practices, and environmental or labor violations.

TABLE 4. Geospatial, environmental & infrastructure intelligence platforms.

No.	Platform Name	Link	Primary Use in Maritime OSINT
1	OpenSeaMap	openseamap.org	Accesses community-updated nautical charts for route analysis and area familiarization.
2	OpenStreetMap	openstreetmap.org	Provides geographic base layer to verify coastal infrastructure and port context.
3	Google Maps.	google.com/maps	Conducts visual reconnaissance of port facilities and coastal installations.
4	Google Earth	earth.google.com	
5	Soar Atlas	soaratlas.com/discover	Accesses commercial satellite and aerial imagery for monitoring vessel activity and infrastructure.
6	Windy	windy.com	Integrates weather and ocean data to analyze voyage feasibility and environmental impacts.
7	Submarine Cable Map	subtelforum.com/submarine-cable-map	Identifies undersea cable infrastructure and assesses risks from maritime activity.

the integration of structured OSINT practices into routine security audits and compliance checks is essential. By identifying and remediating these exposures before they can be weaponized, maritime stakeholders can shift from a reactive security posture to a preventive one, effectively preempting attacks and strengthening overall cyber resilience.

G. OSINT INTEGRATION INTO MARITIME CYBERSECURITY GOVERNANCE AND OPERATIONAL PROCESSES

This section provides practical guidance for organizations of varying maturities to adopt the proposed framework, linking it to regulatory compliance and established security workflows.

1) GOVERNANCE AND REGULATORY ALIGNMENT

Integrating OSINT begins at the governance level, where it should be framed as a tool for fulfilling existing regulatory obligations.

- IMO Resolution MSC.428(98) [5] and the ISM Code [6]: The ISM Code requires companies to identify and assess risks to shipboard safety management systems. OSINT provides a direct, externally focused method for this identification. For example, the IT team performs a quarterly Shodan scan of vessel IP ranges. Finding an unsecured remote access point that must be documented and mitigated under the ISM framework.
- NIS-2 Directive [73]: For ports and maritime operators falling under NIS-2, Article 21 mandates specific cybersecurity measures, including supply chain security, incident handling, and basic cyber hygiene. OSINT directly supports these mandates. The framework's ability to profile third-party vendors and monitor for leaked credentials provides a cost-effective method for assessing the cyber hygiene of the broader supply chain, a key requirement of the directive.
- Data Protection (GDPR): As outlined in Section IV-C, all OSINT activities must be governed by strict ethical and legal guidelines. By adhering to principles of data minimization and purpose limitation, maritime organizations can conduct personnel-focused OSINT in a manner that remains compliant with GDPR and similar privacy regulations.

TABLE 5. Digital infrastructure, social reconnaissance and cyber-threat intelligence platforms.

No.	Platform Name	Link	Primary Use in Maritime OSINT
1	Shodan	shodan.io	Actively scan for and identify exposed maritime Industrial Control Systems (ICS), onboard satellite terminals, and port network devices accessible from the internet.
2	Censys	search.censys.io	
3	ZoomEye	zoomeye.ai	
4	Netlas.io	netlas.io	
5	FOFA	en.fofa.info	
6	Criminal IP	criminalip.io	
7	Sherlock	github.com/sherlock-project/sherlock	Discover crew and employee social media profiles, professional emails, and historical company web pages to build target profiles and map organizational structures.
8	Hunter.io	hunter.io/domain-search	
9	Recruit'em	recruitin.net	
10	Meta Platforms, Wayback Machine	web.archive.org	
11	WhatsMyName Web	whatsmyname.app	
12	Searchsystems.net	publicrecords.searchsystems.net	
13	ViewDNS.info	viewdns.info	Enumerate subdomains, map a shipping company's digital footprint, discover associated services, and gather contact information from public sources.
14	Crt.sh	crt.sh	
15	DNSdumpster	dnsdumpster.com	
16	TheHarvester	github.com/laramies/theHarvester	
17	IPinfo.io	ipinfo.io	
18	IP Geolocation API	ip2location.io	
19	Phonebook.cz	phonebook.cz	
20	TinEye	tineye.com	Analyze photos from ship tours, port visits, or crew social media to verify locations, extract timestamps, and identify camera sources or detect forgeries.
21	EXIF.tools	exif.tools	
22	Forensically	29a.ch/photo-forensics/#forensic-magnifier	
23	Exifdata.com	exifdata.com	
24	Have I Been Pwned	haveibeenpwned.com	Check if crew or corporate emails have been exposed to data breaches (providing password intelligence) and research known software vulnerabilities in maritime systems.
25	CVE.org	cve.org	
26	National Vulnerability Database	nvd.nist.gov	
27	Armed Conflict Location & Event Data Project (ACLED)	acleddata.com	Contextualize maritime incidents, port disruptions, or vessel deviations within local or regional conflict dynamics and security events.
28	Ahmia	ahmia.fi	Search for mentions of specific vessels, companies, or crew within indexed dark web forums, which may reveal planned attacks, leaked data, or illicit services.
29	DuckDuckGo on Tor	duckduckgo.com	
30	Haystak	torry.io/learn/haystak	
31	OnionLand	onionland.io	

2) OPERATIONALIZING OSINT: A TIERED INTEGRATION MODEL

The operational integration of OSINT should be scaled to an organization's size, resources, and risk profile.

Tier 1: The Basic "Digital Footprint Audit" Model (Small Operators):

For smaller shipping agents, port service providers, or shipowners with limited IT staff, a lightweight approach is

TABLE 6. Analytical and threat assessment tools platforms.

No.	Platform Name	Link	Primary Use in Maritime OSINT
1	Maltego	maltego.com	Provides link analysis capabilities to map relationships between vessels, corporate entities, port calls, and digital infrastructure for identifying ownership structures.
2	Gephi	gephi.org	Enables large-scale network analysis and visualization of relationships within shipping consortia, fleet operations, and communication patterns.
3	Octopus.do	octopus.do/sitemap/generator	Creates visual sitemaps and knowledge graphs to document investigation structure and link targets to data sources.
4	Nmap	nmap.org	Scans public IP ranges of vessels or ports to identify open ports, running services, and operating systems.
5	Nikto	github.com/sullo/nikto	Scans maritime web servers for known security misconfigurations and vulnerabilities.
6	OpenVAS	openvas.org/	Scans maritime web servers for known security misconfigurations and vulnerabilities.
7	Metasploit	metasploit.com	Validates vulnerabilities in authorized engagements to assess risk and potential impact.
	Searchsploit	exploit-db.com/searchsploit	
8	Lynis	cisofy.com/lynis	Performing security audits on Unix/Linux-based shipboard systems or shore-side servers to identify hardening issues and compliance gaps.
9	Pulsedive	pulsedive.com	Enriches technical indicators with threat intelligence to assess association with malicious activity.
10	ONI Worldwide Threat to Shipping	oni.navy.mil/ONI-Reports/Shipping-Threat-Reports/Worldwide-Threat-to-Shipping/	Researching historical and current regional threats (piracy, conflict, terrorism) to assess the voyage risk for specific vessels or shipping lanes.
11	GPS/GNSS Interference Map	gpsjam.org	Correlating vessel AIS anomalies or navigation failures with geographically mapped incidents of GPS jamming and spoofing to attribute disruptions.
12	OSINT Framework	osintframework.com	Serving as a centralized, curated directory to quickly discover and access the most relevant OSINT data sources and tools for a maritime investigation.
13	OSINT Map by CybDetective	cybdetective.com/osintmap	Using a visual, mind-map-style interface to navigate and select specialized OSINT tools and techniques for different phases of a maritime inquiry.
14	Synapsint	synapsint.com	Aggregates searches across social media and public data platforms for maritime companies, vessels, or personnel.
15	Google Dataset Search	datasetsearch.research.google.com	Discovering specialized, publicly available datasets relevant to maritime research, such as port statistics, environmental data, or vessel emission databases.
16	Equasis CLI (Command Line)	github.com/rhinonix/equasis-cli	Queries the Equasis database programmatically to retrieve vessel inspection, detention, and ownership history in bulk.
17	GPSwise	gpswise.aero/map	Web-based map tool specifically designed for tracking and visualizing instances of GPS jamming and spoofing worldwide.

most feasible. This involves designating a single responsible person to conduct a semi-annual "digital footprint audit." This individual would use a simplified checklist derived from the framework, including:

- Searching for the company's vessels on public AIS trackers.
- Performing a basic domain and email pattern review.
- Checking company email domains against Have I Been Pwned [75].
- Conducting a simple Shodan search for the company's public IPs.

The findings are then compiled into a simple report for management, highlighting any critical exposures.

Tier 2: Integrated MSOC/Watchkeeper Model (Mid-Sized Companies):

Organizations with a Maritime Security Operations Center (MSOC) [23], [76] or a dedicated IT security team should integrate OSINT into their daily monitoring workflows. This involves:

- Continuous Monitoring: Using tools like Shodan Monitor to receive alerts when new company assets are exposed online.
- Threat Intelligence Feeds: Subscribing to open-source threat intelligence feeds and correlating indicators with internal logs.
- Standard Operating Procedures (SOPs): Developing SOPs for OSINT collection. For example, an SOP titled "Vessel Pre-Charter OSINT Check" could require analysts to run a standard set of queries on a vessel's IMO number, owner, and management company before a charter is finalized.

Tier 3: Dedicated Threat Intelligence Function (Large Ports and Major Operators):

Large port authorities or global shipping lines should consider a dedicated threat intelligence team. This team would not only conduct the activities in Tier 2 but also engage in proactive threat hunting, dark web monitoring (using tools like Ahmia [77]), and geopolitical risk analysis. They would produce regular intelligence briefs for the C-suite and board,

TABLE 7. Structured analysis of OSINT findings for the port of Tulum.

Category	Finding / Vulnerability	Description	Potential Severity	MITRE ATT&CK Mapping (Tactic: Technique)
Digital Infrastructure	Exposed ICS/SCADA Interfaces	Multiple industrial control system login panels were found directly accessible from the public internet via Shodan.	CRITICAL	Initial Access (T1190): Exploit Public-Facing Application
	Unpatched Network Devices (MikroTik Routers)	Several IPs running "MikroTik RouterOS" were identified with outdated firmware, potentially vulnerable to known exploits.	HIGH	Initial Access (T1190): Exploit Public-Facing Application
	Exposed RDP Service	An RDP service on a server labeled "Tulum-Port-Mgmt" was openly accessible, presenting a direct target for brute-force attacks.	HIGH	Initial Access (T1133): External Remote Services
	Unprotected NAS Device	A network-attached storage device with a publicly accessible folder containing port documents was discovered.	HIGH	Collection (T1119): Automated Collection; Exfiltration (T1048): Exfiltration Over Alternative Protocol
Human / Personnel	Human / Personnel	Names, titles, and email address formats for key personnel (IT Manager, Harbor Master) were publicly available on the port's website.	MEDIUM	Reconnaissance (T1591): Gather Victim Org Information; Initial Access (T1566): Phishing
	Geotagged Social Media Posts	Employee social media posts (found via Sherlock) occasionally contained geotagged photos near restricted areas.	LOW	Reconnaissance (T1593): Search Open Websites/Domains; Physical Access (Tactical Goal)
Operational	Public Vessel Schedules	Detailed vessel arrival/departure schedules were visible on tracking platforms, revealing peak operational periods and just-in-time logistics dependencies.	MEDIUM	Reconnaissance (T1591): Gather Victim Org Information; Impact (T1499): Endpoint Denial of Service (by timing an attack)
Physical	Visual Identification of Infrastructure	High-resolution satellite imagery clearly showed the layout of gates, cranes, admin buildings, and perimeter fencing.	LOW	Reconnaissance (T1597): Search Closed Sources; Physical Access (Tactical Goal)

directly informing strategic risk management decisions, such as altering shipping routes based on OSINT-derived insights into regional instability.

By adopting this tiered approach and linking OSINT activities directly to governance, compliance, and operational workflows, maritime organizations can transition from viewing OSINT as an abstract academic concept to a practical, value-driving component of their proactive cyber defense strategy.

H. LIMITATIONS

While this research provides a comprehensive framework for applying OSINT to maritime cybersecurity, several limitations must be acknowledged:

The proposed framework and tool taxonomy are based on publicly available sources and simulated case studies. Real-world applicability may vary across different maritime organizations, vessel types, and geopolitical contexts. Furthermore, the framework has been validated primarily through illustrative case studies rather than longitudinal real-world deployments. Further empirical testing is needed to assess its effectiveness in diverse threat scenarios and operational settings.

OSINT relies on publicly accessible data, which may be outdated, incomplete, or intentionally misleading. The dynamic nature of cyber threats and the rapid evolution of digital platforms mean that the tools and sources listed may become obsolete or less effective over time. Additionally, Many OSINT tools require technical proficiency and may not be fully accessible or interpretable by non-specialists. Additionally, the increasing use of encryption, privacy-enhancing technologies, and closed platforms may reduce the visibility of publicly available data.

While ethical guidelines are proposed, the legal landscape governing OSINT remains fragmented. Adherence to regulations such as GDPR may limit the scope and methods of data collection, particularly when dealing with crew and personnel information.

The framework assumes a certain level of organizational maturity, resources, and cybersecurity awareness. Smaller maritime entities may lack the expertise, budget, or institutional support to implement such an OSINT program effectively.

From an adversarial point of view, as OSINT methodologies become more widely adopted, threat actors may adapt their tactics to reduce their digital footprint or deploy counter-OSINT measures, thereby diminishing the effectiveness of some techniques over time.

VIII. CONCLUSION

The rapid and widespread digitalization of the maritime sector, while driving unprecedented operational efficiency and connectivity, has also dramatically expanded its cyber-attack surface. This research underscores the urgent need for proactive cybersecurity strategies in an industry where traditional reactive measures are increasingly inadequate. Through the development and application of a dedicated maritime OSINT framework, this paper demonstrates how publicly available information can be systematically leveraged to identify vulnerabilities, detect early-stage threats, and enhance situational awareness across maritime operations.

Our study makes several key contributions. **First**, we introduce a structured, phase-based OSINT methodology tailored to the maritime context, encompassing identification, collection, processing, analysis, and dissemination. **Second**, we provide a comprehensive taxonomy of maritime cyber threats, actors, and attack vectors, contextualizing OSINT within the sector's unique risk landscape. **Third**, we present a curated and categorized toolkit of over 100 OSINT resources specifically relevant to maritime security. **Fourth**, we embedded this technical discussion within a necessary ethical and legal framework, emphasizing privacy, proportionality, and compliance with regulations such as GDPR and the NIS-2 Directive. **Finally**, we provide practical guidance on integrating the OSINT framework into existing maritime cybersecurity governance structures, offering a tiered adoption model that enables organizations of all sizes to operationalize these techniques in alignment with regulatory requirements and established security workflows.

The case study presented in this paper illustrates how basic, disciplined OSINT techniques can expose significant digital footprints and potential security weaknesses in critical infrastructure without intrusive measures. This reinforces the paper's central thesis: OSINT is not merely an adjunct to maritime cybersecurity but a foundational component of a modern, proactive defense posture. By transforming freely available data into actionable intelligence, maritime stakeholders can shift from a reactive, incident-driven security model to one focused on prevention, early warning, and informed risk management. Furthermore, by categorizing identified vulnerabilities, ranking their severity, and mapping them to established frameworks such as MITRE ATT&CK, the case study demonstrates how raw OSINT findings can be systematically evaluated to construct plausible, multi-vector attack scenarios. This structured analytical approach transforms simple observation into predictive threat intelligence, enabling organizations to prioritize remediation efforts based on concrete risk assessments and anticipate adversary behavior before an incident occurs.

To advance maritime OSINT capabilities, future research should prioritize integration with artificial intelligence and machine learning to automate threat detection, behavioral analysis, and monitoring digital forums. This should be coupled with the development of advanced sensor fusion platforms that combine AIS, satellite imagery, and IoT data into a unified, real-time maritime common operational picture.

A deeper exploration of human-centric OSINT, including social media profiling and simulated social engineering attacks, is needed to address the critical human factor in cybersecurity. Furthermore, the field would benefit significantly from the standardization of threat intelligence sharing formats and the creation of quantitative models to assess the return on investment of OSINT programs. Simultaneously, clearer international legal and ethical frameworks must be established to govern active reconnaissance activities. Finally, investing in advanced training simulators will be essential for building practical, scenario-based expertise across the maritime workforce.

IX. APPENDIX

See Tables 1–7

REFERENCES

[1] United Nations Conference on Trade and Development, "Review of maritime transport 2023," in *Proc. United Nations Conf. Trade Develop.*, Geneva, Switzerland, Sep. 2023, p. 157, doi: 10.18356/9789213584569.

[2] W. Loomis, V. Singh, G. C. Kessler, and X. Bellekens, "Raising the colors: Signaling for cooperation on maritime cybersecurity," *Atlantic Council*, pp. 1–51, Oct. 2021. Accessed: Oct. 15, 2025. [Online]. Available: https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Cyber-Maritime-Final-Report.pdf

[3] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity challenges in the maritime sector," *Network*, vol. 2, no. 1, pp. 123–138, Mar. 2022, doi: 10.3390/network2010009.

[4] European Parliament. *NIS 2 Directive–2022/2555–EN–EUR-Lex*. Accessed: Jul. 30, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[5] International Maritime Organization. *Resolution MSC.428(98)–Maritime Cyber Risk Management in Safety Management Systems*. Accessed: May 30, 2025. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[6] (2018). *International Maritime Organization, ISM Code: International Safety Management Code With Guidelines for Its Implementation*. [Online]. Available: http://dx.doi.org/10.62454/KD117E

[7] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, "Cyber physical systems security for maritime assets," *J. Mar. Sci. Eng.*, vol. 9, no. 12, p. 1384, Dec. 2021, doi: 10.3390/jmse9121384.

[8] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels cybersecurity: Issues, challenges, and the road ahead," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 90–96, Jun. 2020, doi: 10.1109/MCOM.001.1900632.

[9] B. Al-Sada, A. Sadighian, and G. Oligeri, "MITRE ATT&CK: State of the art and way forward," *ACM Comput. Surveys*, vol. 57, no. 1, pp. 1–37, Oct. 2024, doi: 10.1145/3687300.

[10] B. E. Uçar, M. Ecevit, H. Dağ, and R. Creutzburg, "A comprehensive review of open source intelligence in intelligent transportation systems," in *Proc. Int. Conf. Intell. Environments (IE)*, Jun. 2024, pp. 109–116, doi: 10.1109/ie61493.2024.10599907.

[11] J. Pastor-Galindo, P. Nespoli, F. Gomez Marmol, and G. Martinez Perez, "The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends," *IEEE Access*, vol. 8, pp. 10282–10304, 2020, doi: 10.1109/ACCESS.2020.2965257.

[12] *MarineTraffic: Global Ship Tracking Intelligence | AIS Marine Traffic*. Accessed: Jul. 11, 2025. [Online]. Available: https://www.marinetraffic.com/

[13] S. Schauer, Kalogeraki, Eleni- Maria, S. Papastergiou, and C. Douligeris, "Detecting sophisticated attacks in maritime environments using hybrid situational awareness," in *Proc. Int. Conf. Inf. Commun. Technol. Disaster Manage. (ICT-DM)*, Dec. 2019, pp. 1–7, doi: 10.1109/ICT-DM47966.2019.9032900.

[14] R. Heartfield, G. Loukas, and D. Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access*, vol. 4, pp. 6910–6928, 2016, doi: 10.1109/ACCESS.2016.2616285.

[15] T. Babenko, K. Kolesnikova, O. Abramkina, and Y. Vitulyova, "Automated OSINT techniques for digital asset discovery and cyber risk assessment," *Computers*, vol. 14, no. 10, p. 430, Oct. 2025, doi: 10.3390/computers14100430.

[16] F. Heiding, S. Lermen, A. Kao, B. Schneier, and A. Vishwanath, "Evaluating large language Models' capability to launch fully automated spear phishing campaigns: Validated on human subjects," 2024, *arXiv:2412.00586*.

[17] K. Buraya, A. Farseev, A. Filchenkov, and T. S. Chua, "Towards user personality profiling from multiple social networks," in *Proc. AAAI Conf. Artif. Intell.*, vol. 31, no. 1, Feb. 2017, pp. 1–9, doi: 10.1609/AAAI.V31I1.11105.

[18] L. Liu, D. Preoţiuc-Pietro, Z. R. Samani, M. E. Moghaddam, and L. Ungar, "Analyzing Personality through Social Media Profile Picture Choice," in *Proc. Int. AAAI Conf. Web Social Media*, vol. 10, no. 1, pp. 211–220, 2016, doi: 10.1609/ICWSM.V10I1.14738.

[19] S. Eftimie, R. Moinescu, and C. Racuciu, "Spear-phishing susceptibility stemming from personality traits," *IEEE Access*, vol. 10, pp. 73548–73561, 2022, doi: 10.1109/ACCESS.2022.3190009.

[20] F. Martínez, L. E. Sànchez, A. Santos-Olmo, D. G. Rosado, and E. Fernàndez-Medina, "Maritime cybersecurity: Protecting digital seas," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1429–1457, Jan. 2024, doi: 10.1007/s10207-023-00800-0.

[21] M. Li, J. Zhou, S. Chattopadhyay, and M. Goh, "Maritime cybersecurity: A comprehensive review," 2024, *arXiv:2409.11417*.

[22] 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," *Prog. Mar. Sci. Technol.*, vol. 9, pp. 235–245, Nov. 2024, doi: 10.3233/PMST240042.

[23] A. N. Nasr, R. Vaarandi, I. Zaitseva-Pärnaste, and P. Kujala, "Maritime security operations center (M-SOC): Systematic literature review, research gaps and future areas to investigate," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 19, no. 4, pp. 1141–1155, Mar. 2025, doi: 10.12716/1001.19.04.11.

[24] C. Kapalidis, S. Karamperidis, T. Watson, and G. Koligiannis, "A vulnerability centric system of systems analysis on the maritime transportation sector most valuable assets: Recommendations for port facilities and ships," *J. Mar. Sci. Eng.*, vol. 10, no. 10, p. 1486, Oct. 2022, doi: 10.3390/jmse10101486.

[25] M. Mohsendokht, H. Li, C. Kontovas, C.-H. Chang, Z. Qu, and Z. Yang, "Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades," *Ocean Eng.*, vol. 312, Nov. 2024, Art. no. 119078, doi: 10.1016/j.oceaneng.2024.119078.

[26] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of AIS automated identification system," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, Dec. 2014, pp. 436–445, doi: 10.1145/2664243.2664257.

[27] R. Cichocki, "State-sponsored and organized crime threats to maritime transportation systems in the context of the attack on Ukraine," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 17, no. 3, pp. 717–721, Sep. 2023, doi: 10.12716/1001.17.03.24.

[28] C. Bronk and P. deWitte, "Maritime cybersecurity: Meeting threats to Globalization's great conveyor," *Comput. Methods Appl. Sci.*, vol. 56, pp. 241–254, Apr. 2022, doi: 10.1007/978-3-030-91293-2_10.

[29] N. C. N. Hampson, "Hacktivism: A new breed of protest in a networked world," *Boston College Int. Comp. Law Rev.*, vol. 35, no. 2, pp. 511–543, May 2012.

[30] T. Jordan and P. A. Taylor, *Hacktivism and Cyberwars: Rebels With a Cause?*. Evanston, IL, USA: Routledge, 2004, doi: 10.4324/9780203490037.

[31] V. Karagiannopoulos, "A short history of hacktivism: Its past and present and what can we learn from it," in *Rethinking Cybercrime: Critical Debates*. Cham, Switzerland: Palgrave Macmillan, Nov. 2021, pp. 63–86, doi: 10.1007/978-3-030-55841-3_4.

[32] F. L. Greitzer, A. P. Moore, D. M. Cappelli, D. H. Andrews, L. A. Carroll, and T. D. Hull, "Combating the insider cyber threat," *IEEE Secur. Privacy Mag.*, vol. 6, no. 1, pp. 61–64, Jan. 2008, doi: 10.1109/MSP.2008.8.

[33] E. Kowalski et al., *Insider Threat Study: Illicit Cyber Activity in the Government Sector*. Carnegie Mellon University, Software Engineering Institute, Jan. 2008, pp. 1–59.

[34] A. Mittal and U. Garg, "A review for insider threats detection using machine learning," in *Proc. Amer. Inst. Phys. Conf.*, vol. 2555, pp. 020006-1–020006-8, Oct. 2022, doi: 10.1063/5.0108887.

[35] Cydome. *Lab Dookhtegan Cyber Attack on Iranian Oil Tankers Disrupts Operations–CYDOME*. Accessed: Jul. 30, 2025. [Online]. Available: https://cydome.io/lab-dookhtegan-cyber-attack-on-iranian-oil-tankers-disrupts-operations/

[36] I. Mraković and R. Vojinović, "Maritime cyber security analysis–how to reduce threats?" *Trans. Maritime Sci.*, vol. 8, no. 1, pp. 132–139, Apr. 2019, doi: 10.7225/toms.v08.n01.013. [Online]. Available: https://www.toms.com.hr/index.php/toms/article/view/250

[37] P. Paganini. *1,000 Ships Impacted By a Ransomware Attack on DNV*. Accessed: Jul. 30, 2025. [Online]. Available: https://securityaffairs.com/140941/cyber-crime/ransomware-attack-maritime-firm-dnv.html

[38] L. Yu, J. Hao, J. Ma, Y. Sun, Y. Zhao, and B. Luo, "A comprehensive analysis of security vulnerabilities and attacks in satellite modems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, vol. 24, Dec. 2024, pp. 3287–3301, doi: 10.1145/3658644.3670390.

[39] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A tale of sea and sky on the security of maritime VSAT communications," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 1384–1400, doi: 10.1109/SP40000.2020.00056.

[40] S. D. Applegate, "Social engineering: Hacking the wetware!" *Inf. Secur. J., Global Perspective*, vol. 18, no. 1, pp. 40–46, Feb. 2009, doi: 10.1080/19393550802623214.

[41] EclecticIQ. *Multi-Year Spearphishing Campaign Targets the Maritime Industry Likely for Financial Gain*. Accessed: Jul. 30, 2025. [Online]. Available: https://blog.eclecticiq.com/multi-year-spearphishing-campaign-targets-the-maritime-industry-likely-for-financial-gain

[42] S. Papastergiou, N. Polemi, and I. Papagiannopoulos, "Business and threat analysis of ports' supply chain services," in *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9190. Cham, Switzerland: Springer, 2015, pp. 642–653, doi: 10.1007/978-3-319-20376-8_57.

[43] A. Cantelli-Forti, M. Colajanni, and S. Russo, "Penetrating the silence: Data exfiltration in maritime and underwater scenarios," in *Proc. IEEE 48th Conf. Local Comput. Netw. (LCN)*, Oct. 2023, pp. 1–6, doi: 10.1109/lcn58197.2023.10223402.

[44] X. Wang, "On the feasibility of detecting software supply chain attacks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2021, pp. 458–463, doi: 10.1109/MILCOM52596.2021.9652901.

[45] S. König, S. Rass, and S. Schauer, "Cyber-attack impact estimation for a port," in *Proc. Hamburg Int. Conf. Logistics (HICL)*, 2019, pp. 164–183, doi: 10.15480/882.2496. [Online]. Available: https://tore.tuhh.de/entities/publication/0258db36-9fea-47d9-a77f-cf566858acdb

[46] Dredgewire. *Port of Rotterdam Cyberattack: Security Breach Uncovered*. Accessed: Feb. 22, 2026. [Online]. Available: https://dredgewire.com/port-of-rotterdam-cyberattack-security-breach-uncovered/

[47] P. Rajaram, M. Goh, and J. Zhou, "Guidelines for cyber risk management in shipboard operational technology systems," *J. Physics: Conf. Ser.*, vol. 2311, no. 1, Jul. 2022, Art. no. 012002, doi: 10.1088/1742-6596/2311/1/012002.

[48] Al Jazeera. (May 2020). *Israel Cyberattack Caused 'total Disarray' At Iran Port: Report*. Accessed: Feb. 18, 2026. [Online]. Available: https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-total-disarray-at-iran-port-report

[49] R. Tanabe, R. de-Oliveira-Albuquerque, D. da-Silva-Filho, D. Alves-da-Silva, and J. J. Costa-Gondim, "OSINT methods in the intelligence cycle," in *Proc. Int. Conf. Comput. Sci., Electron. Ind. Eng. (CSEI)*, in Lecture Notes in Networks and Systems, vol. 678, 2023, pp. 42–54, doi: 10.1007/978-3-031-30592-4_4.

[50] J. Rajamäki, S. Sarlio-Siintola, N. Alapuranen, and M. Nevanperä, "Privacy in open source intelligence and big data analytics: Case 'MARISA' for maritime surveillance," *J. Inf. Warfare*, vol. 19, no. 1, pp. 12–25, 2020.

[51] K. N. Lovell and D. Heering, "Exercise Neptune: Maritime cybersecurity training using the navigational simulators," in *Proc. 5th Interdiscipl. Cyber Res. Conf.* Tallinn: Tallinn University of Technology, Jun. 2019, pp. 34–37.

[52] E. C. Sage, "Shining a light on AIS blackouts with maritime OSINT," *Frontiers Comput. Sci.*, vol. 5, Aug. 2023, Art. no. 1185760, doi: 10.3389/fcomp.2023.1185760.

[53] A.-N. Kanellopoulos, "Enhancing cyber security and counterintelligence in the shipping industry," *Nat. Secur. future*, vol. 25, no. 1, pp. 137–154, Apr. 2024, doi: 10.37458/nstf.25.1.6.

[54] *Shodan Search Engine*. Accessed: Dec. 18, 2025. [Online]. Available: https://www.shodan.io/

[55] D.-Y. Kao, Y.-T. Chao, F. Tsai, and C.-Y. Huang, "Digital evidence analytics applied in cybercrime investigations," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2018, pp. 111–116, doi: 10.1109/AINS.2018.8631403.

[56] A. Yadav, A. Kumar, and V. Singh, "Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security," *Artif. Intell. Rev.*, vol. 56, no. 11, p. 1, Nov. 2023, doi: 10.1007/S10462-023-10454-Y.

[57] T. Riebe, T. Biselli, M.-A. Kaufhold, and C. Reuter, "Privacy concerns and acceptance factors of OSINT for cybersecurity: A representative survey," in *Proc. Privacy Enhancing Technol.*, 2023, pp. 477–493, doi: 10.56553/popets-2023-0028.

[58] I. Böhm and S. Lolagar, "Open source intelligence," *Int. Cybersecurity Law Rev.*, vol. 2, no. 2, pp. 317–337, Dec. 2021, doi: 10.1365/S43439-021-00042-7.

[59] ENISA. *Guidelines for SMEs on the Security of Personal Data Processing*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
[60] J. Rajamäki and J. Simola, "How to apply privacy by design in OSINT and big data analytics?" in *Proc. 18th Eur. Conf. Cyber Warfare Secur. (ECCWS)*, Jul. 2019, p. 364.
[61] J. Rajamäki, S. Sarlio-Siintola, and J. Simola, "Ethics of open source intelligence applied by maritime law enforcement authorities," in *Proc. 17th Eur. Conf. Cyber Warfare Secur. (ECCWS)*, Jun. 2018, pp. 424–431.
[62] A. Goudossis and S. K. Katsikas, "Towards a secure automatic identification system (AIS)," *J. Mar. Sci. Technol.*, vol. 24, no. 2, pp. 410–423, May 2018, doi: 10.1007/s00773-018-0561-3.
[63] A. Amro, "IoT vulnerability scanning: A state of the art," in *Computer Security*, in Lecture Notes in Computer Science, vol. 12501. Cham, Switzerland: Springer, 2020, pp. 84–99, doi: 10.1007/978-3-030-64330-0_6.
[64] A. Amro, "Cyber-physical tracking of IoT devices: A maritime use case," *NIKT*, no. 3, Jan. 2022, Accessed: Jul. 15, 2025. https://www.ntnu.no/ojs/index.php/nikt/article/view/5509
[65] *Ship & Container Tracking—VesselFinder*. Accessed: Dec. 17, 2025. [Online]. Available: https://www.vesselfinder.com/
[66] *Censys Search*. Accessed: Dec. 18, 2025. [Online]. Available: https://search.censys.io/
[67] *Google Maps*. Accessed: Dec. 18, 2025. [Online]. Available: https://www.google.com/maps
[68] *OpenStreetMap*. Accessed: Dec. 18, 2025. [Online]. Available: https://www.openstreetmap.org/
[69] J. Rajamäki and K. Tiitta, "Implementation of OSINT for improving an international finance sector organization's cybersecurity," in *Proc. Int. Conf. Cyber Warfare Secur.*, vol. 19, no. 1, pp. 612–616, Mar. 2024, doi: 10.34190/ICCWS.19.1.1977.
[70] F. Tabatabaei and D. Wells, "OSINT in the context of cyber-security," in *Advanced Sciences and Technologies for Security Applications*. Cham, Switzerland: Springer, 2016, pp. 213–231, doi: 10.1007/978-3-319-47671-1_14.
[71] M. Muckin and S. C. Fitch. (2019). *A Threat-Driven Approach to Cyber Security Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization*. Accessed: Feb. 18, 2026. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-Martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf
[72] L. Marzell, "OSINT as part of the strategic national security landscape," in *Advanced Sciences and Technologies for Security Applications*. Cham, Switzerland: Springer, 2016, pp. 33–55, doi: 10.1007/978-3-319-47671-1_4.
[73] *NIS 2 Directive, Article 21: Cybersecurity Risk-Management Measures*. Accessed: Aug. 1, 2025. [Online]. Available: https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html
[74] R. G. Lugo, A. Juozapavicius, K. Lapin, T. F. Ask, B. J. Knox, and S. Sütterlin, "Human-centric approach to cyber threat identification: The role of cognition, experience, and education in decision-making," *J. Cases Inf. Technol.*, vol. 27, no. 1, pp. 1–13, Jan. 2025, doi: 10.4018/jcit.368220.
[75] *Have I Been Pwned: Check if Your Email Address Has Been Exposed in a Data Breach*. Accessed: Dec. 18, 2025. [Online]. Available: https://haveibeenpwned.com/
[76] A. Oruc, S. Bauk, and J. Zhou, "A national maritime cyber security operations center (M-SOC) concept," *J. Mar. Sci. Eng.*, vol. 14, no. 1, p. 17, Dec. 2025, doi: 10.3390/jmse14010017.
[77] *Ahmia–Search Tor Hidden Services*. Accessed: Dec. 18, 2025. [Online]. Available: https://ahmia.fi/

AHMED NAGI NASR is currently pursuing the Ph.D. degree with Estonian Maritime Academy, TalTech, specializing in the protection of autonomous systems and critical maritime infrastructure. He is a Cybersecurity Researcher. He actively contributes to major EU-funded projects, such as CyberSecPro and DigiMaris, applying offensive security methodologies to enhance the digital resilience of maritime platforms and the IoT environments. His current interests include advanced threat detection, the security of telemetry links for unmanned surface vessels (USVs), and the development of maritime security operations centers (M-SOC).

AYBARS ORUÇ received the Ph.D. degree from the Norwegian University of Science and Technology (NTNU), in 2024. He is currently a Maritime Cybersecurity Expert and a Postdoctoral Researcher with Tallinn University of Technology (TalTech), specializing in the security of critical maritime infrastructure. He possesses a robust technical background, having served as a Marine Engineer on container ships and oil tankers before transitioning into shore-based management as an HSEQ Coordinator. His research interests include the cybersecurity of bridge navigation systems and maritime cyber resilience.

RICARDO LUGO received the Ph.D. degree from Johannes Gutenberg University Mainz, in 2018, with a focus on cognitive performance in cyber defense. He is currently a Senior Research Fellow with Estonian Maritime Academy, TalTech. He is a Distinguished Researcher specializing in the human factors of cybersecurity. He held several academic positions across Norway, including roles at Inland University of Applied Sciences and NTNU. With more than 80 scientific publications, his work bridges psychology and technology by exploring cognitive agility, decision-making, and the use of virtual reality for training.

INGA ZAITSEVA-PÄRNASTE received the Ph.D. degree in civil and environmental engineering from Tallinn University of Technology, in 2013, focusing on baltic sea wave climate. She is an Associate Professor and a Coastal Engineering Expert. Her career uniquely blends high-level industry experience as a hydrographic surveyor for Royal Boskalis Westminster with prestigious academic roles, including a tenure as a Fulbright Visiting Scholar with the NASA Stennis Space Center. Currently, she is a Coordinator with Kuressaare College and the Chief Specialist of Estonian Environment Agency. She has authored more than 30 publications on physical oceanography, offshore wind farm risk assessment, and waterway safety.

PENTTI KUJALA received the Ph.D. degree, in 1994, on ice-induced ship loads. He was a Professor of marine technology with Aalto University, from 2006 to 2022, leading its Marine Technology Group and the Vice Dean. Since 2023, he has been a Professor of waterway safety management with Taltech. He chaired the CEPOLAR Arctic Shipping Center, from 2013 to 2021, and was named the top EU Researcher in waterborne transport, in 2020. He has more than 45 years experience in marine safety. His research focuses on marine safety, risk analysis, and innovative ship structures, with more than 300 publications.