TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Júlia Anna Grosschmid 233933IVCM

Assessing the Economic Impact of Cyberattacks in the Maritime Sector: A Taxonomy-Driven Case Study and Data Analysis

Master's thesis

Supervisor: Sanja Bauk
Professor

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Júlia Anna Grosschmid 233933IVCM

Küberrünnakute majandusliku mõju hindamine merendussektoris: taksonoomial põhinev juhtumiuuring ja andmeanalüüs

Magistritöö

Juhendaja: Sanja Bauk
Professor

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Júlia Anna Grosschmid

18.05.2025

Abstract

The maritime sector's digitalisation has notably increased its cyber risk exposure, endangering critical infrastructure with severe operational and economic repercussions. Yet, the macroeconomic effects of maritime cyber incidents are largely unmeasured due to obstacles such as a lack of data, inconsistent classification of incidents, and constrained financial disclosures. This thesis explores methods to systematically quantify these impacts, introducing a structured approach that organises incident data for improved comparability and strategic evaluation. Utilising this framework in conjunction with selected case studies, the research reveals that, although thorough macroeconomic measurement is challenging, structured event-based assessments provide vital insights into systemic vulnerabilities, gaps in resilience, and opportunities for strategic responses. The thesis concludes with practical suggestions for enhancing data transparency, standardising reporting processes, and encouraging collaboration across sectors, thereby establishing maritime cybersecurity as a crucial element of economic resilience and national security.

Key words: Maritime cybersecurity, cyberattack impact, economic impact assessment, incident taxonomy

This thesis is written in English and is 158 pages long, including 9 chapters, 39 figures and 16 tables.

Annotatsioon

Küberrünnakute majandusliku mõju hindamine merendussektoris: taksonoomial põhinev juhtumiuuring ja andmeanalüüs

Merendussektori digiteerimine on oluliselt suurendanud selle haavatavust küberohtude suhtes, asetades kriitilise taristu ohtu ja põhjustades tõsiseid operatiivseid ning majanduslikke tagajärgi. Siiski on merendussektoris aset leidvate küberintsidentide makromajanduslikku mõju suures osas keeruline hinnata, eelkõige andmete puudumise, intsidentide ebaühtlase klassifitseerimise ning piiratud finantsinfo tõttu. Käesolev magistritöö käsitleb võimalusi nende mõjude süstemaatiliseks kvantifitseerimiseks, esitades struktureeritud lähenemisviisi, mis korrastab küberintsidentide andmestikku parema võrreldavuse ja strateegilise hindamise eesmärgil. Rakendades seda raamistikku koos valitud juhtumiuuringutega, selgub, et kuigi põhjalik makromajanduslik mõõtmine on keeruline, pakuvad struktureeritud sündmuspõhised analüüsid väärtuslikku teavet süsteemsete haavatavuste, vastupanuvõime puudujääkide ning strateegilise reageerimise võimaluste kohta. Töö lõpeb praktiliste ettepanekutega andmete läbipaistvuse suurendamiseks, aruandlusprotsesside ühtlustamiseks ning sektoritevahelise koostöö tugevdamiseks, rõhutades merenduse küberjulgeoleku olulisust majandusliku vastupanuvõime ja riikliku julgeoleku keskse komponendina.

Märksõnad: merenduse küberjulgeolek, küberrünnaku mõju, majandusmõju hindamine, intsidentide taksonoomia

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 158 leheküljel, 9 peatükki, 39 joonist, 16 tabelit.

List of abbreviations and terms

ADMIRAL	*Advanced Maritime Cybersecurity Attack Database* – a structured dataset on maritime cyber incidents (used in academic and industry research)
ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information* – France's national cybersecurity authority
AIS	Automatic Identification System – a maritime communication system for tracking vessel identity and location
BIMCO	Baltic and International Maritime Council – a leading international shipping association
C4ADS	Center for Advanced Defense Studies – U.S.-based non-profit conducting open-source intelligence on global security threats
CMA CGM	Compagnie Maritime d'Affrètement – Compagnie Générale Maritime – one of the world's largest container shipping companies
CNIL	*Commission Nationale de l'Informatique et des Libertés* – French data protection authority responsible for enforcing GDPR
CERT	Computer Emergency Response Team
CEO	Chief Executive Officer
CPS	Cyber-Physical System – systems that integrate physical processes with digital control and communication technologies
CPPI	World Bank's Container Port Performance Index
Cyber	relating to, or involving computers or computer networks (such as the Internet) (Oxford dictionary)
Cyberattack	An act or action initiated in or through cyberspace to cause harmful effects. (NATO term)
Cybersecurity	The application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation. (NATO term)
Cyberspace	The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are

	separated or independent, which process, store or transmit data. (NATO term)
EEZ	Exclusive Economic Zone
ENISA	European Union Agency for Cybersecurity – the EU body responsible for network and information security
EU	European Union
GDP	Gross Domestic Product - the standard measure of the value added created through the production of goods and services in a country during a certain period.
GMTS	Global Maritime Transportation System: the integrated system of ships, ports, and services enabling international maritime trade
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HSI	Homeland Security Investigations – a division of the U.S. Department of Homeland Security responsible for transnational crime, including cybercrime
ICS	Industrial Control Systems
IMO	International Maritime Organization: specialised UN agency responsible for maritime safety and environmental regulation
IoT	Internet of Things – interconnected devices capable of collecting and exchanging data
ISM	International Safety Management Code – an IMO-mandated framework for ensuring safe ship operation and pollution prevention
ISS	Incident Severity Score: a metric used to assess the severity of a cyber incident, introduced in this research
IT	Information Technology
Maritime	The term referring to anything related to the ocean, sea, and rivers. Maritime includes the ships, ports, companies, and individuals that are involved in the industry (Oxford dictionary)
MCAD	Maritime Cyber Attack Database: The open-source dataset of documented cyberattacks affecting the maritime sector, managed by Maritime IT Security Research Group at NHL Stenden University of Applied Sciences
NCA	Number of Cyber Attacks: a metric indicating the volume of recorded cyber incidents
NIS/NIS2	Network and Information Systems (Directive): EU legislation establishing a baseline for cybersecurity across member states

NIST	National Institute of Standards and Technology: a U.S. agency providing cybersecurity standards and guidelines
NSA	National Security Agency: U.S. intelligence agency responsible for national cybersecurity and signals intelligence
OECD	Organisation for Economic Co-operation and Development
OT	Operational Technology: hardware and software systems that monitor and control physical devices and industrial processes
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
PPT	People, Process, Technology: a framework for organisational and cybersecurity analysis
RDP	Remote Desktop Protocol: a protocol enabling remote access to Windows-based systems
RF	Radio Frequency
SCADA	Supervisory Control and Data Acquisition: systems for controlling and monitoring industrial processes
SOC	Security Operations Centre – a dedicated unit responsible for monitoring, detecting, and responding to cyber threats
TEU	Twenty-Foot Equivalent Unit: a standard measure of containerised cargo capacity
USB	Universal Serial Bus
VDR	Voyage Data Recorder: maritime equivalent of a black box, recording ship data for investigation
VMS	Vessel Monitoring System
VSAT	Very Small Aperture Terminal: satellite communication system used on ships

Table of contents

List of Figures

List of Tables

Dedication

To my family, who stood by me with love, patience, and humour, and even more patience when times turned out to be far from easy.

To the mentors, teachers, and colleagues who challenged me, inspired me, and helped shape both this work and the person behind it.

And to you, the reader, thank you for engaging with this effort. I hope it informs, provokes thought, and perhaps contributes, in some way, to a safer maritime future.

Acknowledgement

I would like to express my sincere gratitude to my supervisor, Professor Sanja Bauk, for guiding me with insightful patience and constructive feedback, and for our valuable discussions and support throughout this research project.

I also wish to thank Dr Rain Ottis for encouraging me in my first steps toward embarking on this master's journey. My gratitude extends to all the faculty and staff of the School of Information Technologies at Tallinn University of Technology, whose encouragement and assistance have been instrumental in helping me complete this thesis.

I am deeply grateful to my family and my husband for their unwavering support, and belief in me throughout this journey. Their encouragement gave me the strength to keep going, even during the most challenging times.

Introduction

The maritime industry, responsible for roughly 80% of global trade by volume, faces escalating cyber threats that jeopardise economic stability and supply chain integrity [1]. While technological advancements, digitalisation, internet connectivity, and automation have brought efficiency gains, they have also introduced significant cybersecurity challenges. Recent studies reveal a 200% increase in average cyberattack costs to $550,000 per incident, with ransom demands exceeding $3.2 million [2]. Systematic vulnerabilities stem from ageing infrastructure, inadequate cybersecurity investment, and the digitalisation of navigation and port systems. While resilience frameworks like the International Maritime Organisation's (IMO) guidelines and system dynamics models are emerging, research indicates stagnating preparedness levels and projected declines in cyber resilience [3].

This critical infrastructure faces escalating cyber threats with profound economic ramifications. Recent study reveals that maritime cyberattacks cost the industry between $7.5 billion and $12 billion annually [4]. On a very broad scale, these figures include single incidents such as the 2017 NotPetya attack that has caused $300 million in direct losses for Maersk [5]. These attacks disrupt port operations, compromise navigation systems, and expose sensitive cargo data, creating cascading effects across global supply chains. Their economic impact extends beyond immediate financial losses, including trade flow distortions, insurance market destabilisation, and long-term competitiveness erosion in maritime-dependent nations.

This thesis aims to synthesise open-source findings on maritime cyberattacks to assess their global economic impact. The study examines the most vulnerable areas of maritime operations and evaluates mitigation strategies to enhance cybersecurity resilience. Ultimately, the findings contribute to a broader understanding of how cyberattacks in the maritime sector influence global economic stability and what measures can be taken to mitigate their risks effectively.

1.1 Problem Statement

Cyberattacks transcend geopolitical boundaries and negatively impact nearly everyone, regardless of nation, political views, or economic position. They pose a growing threat to global industries, with economic consequences extending far beyond their immediate victims. The maritime sector, as the facilitator of global trade, connector of industries, is particularly vulnerable due to its increasing digitalisation, outdated legacy systems, and regulatory gaps in cybersecurity enforcement. Despite its critical role in the global economy, maritime cybersecurity remains an underexamined area in economic impact assessments. While global estimates exist for the costs of cyberattacks, there is no comprehensive assessment of their specific impact on the maritime economies. Studies have shown that cyberattacks slow Gross Domestic Product (GDP) growth [6], [7], yet the extent to which maritime cyber incidents contribute to this effect remains unclear. Given that the maritime sector central role, cyberattacks targeting it may have a disproportionately high economic impact compared to attacks on other industries.

Accurately quantifying this impact, however, is challenging due to severe data limitations. Publicly available sources capture only a fraction of all incidents, as many go unreported due to confidentiality concerns, reputational risks, and regulatory inconsistencies. While cybersecurity firms, CERTs, insurers, and government agencies, collect more extensive data, much of it remains inaccessible. In some cases, valuable insights can only be drawn from alternative sources, such as dark web marketplaces where adversaries disclose stolen data and ransom negotiations. An observation was made during the course of this research, when attempts to verify specific cyber incidents revealed that public evidence had been either removed or withheld, with confirmation found solely in threat actor communications.

This thesis addresses this research gap by synthesising available maritime cyberattacks, assessing economic consequences through case studies, and critically examining the challenges of cost estimation. It aims to contribute to a better understanding of maritime cybersecurity risks and their broader economic implications, offering insights for policymakers, industry stakeholders, and researchers. Importantly, while cybersecurity is typically treated as a cost centre within most companies in the maritime sector, this thesis argues that in a domain as interconnected as maritime logistics, such an approach underestimates the externalities. The ripple or cascading effects of underinvestment, as

exemplified by the Transnet attack extend beyond the directly targeted entities, impacting third parties as well as national economies. Through three detailed case studies, this thesis demonstrates that cybersecurity in the maritime sector is not only a matter of financial risk, but also one of systemic resilience and ethical responsibility.

1.2 Research Questions

This thesis is guided by one main research question and four supporting sub-questions. Together, these aim to explore whether the economic consequences of cyberattacks on maritime economies can be meaningfully assessed using currently available data, and to what extent existing incidents offer insight into broader financial and operational impacts.

1.2.1 Main Research Question (MRQ)

Is it possible to calculate the macroeconomic consequences of cyberattacks on the maritime economies, and are documented incidents enough to illustrate the financial and operational impact?

1.2.2 Sub-Questions (RQ)

Economic impact assessment:
RQ1. How do maritime cyberattacks cause economic disruption at the organisational, sectoral, and potentially macroeconomic levels?

Challenges in measuring economic cost:
RQ2. What challenges are there in quantifying the economic impact of maritime cyberattacks due to limitations in data collection and reporting?

Case study analysis of financial and operational impact:
RQ3. Do case studies provide a reliable basis for estimating economic impact, and what do they reveal about the preparedness and resilience of different maritime actors?

Cost of cybersecurity investment versus financial risk:
RQ4. How do cost-benefit considerations influence cybersecurity investment decisions in the maritime sector, and what are the implications of risk-based models in highly interconnected supply chains?

These sub-questions are interdependent and collectively build the foundation for this research. RQ1 and RQ2 establish the problem by examining the nature of economic disruption and the limitations of existing data. In light of the constraints, RQ3 introduces case study analysis as a practical approach to explore the issue in greater depth, and RQ4 connects these insights to broader investment considerations, evaluating how economic risk is managed within the sector and what this implies for future resilience strategies.

1.3 Study Aim and Objectives

This thesis explores whether it is possible to calculate the macroeconomic consequences of cyberattacks on maritime economies. It also assesses whether currently documented and published incidents are sufficient to illustrate the financial and operational impacts caused by such attacks. This research builds on existing macroeconomic findings, such as the Thomas Murray study [6], which demonstrated that cyberattacks can measurably reduce GDP growth and disproportionately affect highly digitalised economies. It also draws on insights from a study on maritime dependency and economic prosperity [8], which highlighted the strong link between maritime trade volumes and national economic performance; drawing connection between access to deep water ports and economic growth. Given the maritime sector's essential role in sustaining international commerce, this thesis hypothesises that cyberattacks on maritime operations may cause more severe macroeconomic consequences than those generally observed across other sectors.

Although the original aim of this thesis was to quantify the macroeconomic costs of maritime cyberattacks, the scarcity of structured, sector-specific data made such calculations unfeasible. In response, the research evolved to focus more heavily on the development of a maritime cyberattack classification framework and the consolidation of incident data to support future economic impact analysis. Nonetheless, the thesis continues to explore the economic dimension through case studies and a critical assessment of modelling limitations, reflecting on the minimal data presented in open access cyberattack records.

1.4 Summary of Methods

This study adopts a mixed-methods approach, combining quantitative dataset structuring with qualitative case study analysis. The research design evolved in response to

significant data limitations, particularly the scarcity of standardised financial information relating to maritime cyber incidents. Rather than applying traditional macroeconomic modelling, which proved unfeasible due to inconsistent disclosure practices and limited reporting, the study focuses on building a foundation for future analysis by improving data clarity and structure.

The first component of the methodology involves the collection, cleaning, and integration of two major open-source datasets into a single structured maritime cyberattack database. A custom classification taxonomy was developed to support multi-dimensional categorisation of incidents, including parameters such as attack method, operational impact, and affected maritime subsector. This structured approach enables trend identification and highlights key data gaps. The second component is a case study analysis of three major cyber incidents. These were selected based on their operational severity, data availability, and representation of different subsectors within the maritime domain. Case studies offer a practical alternative for examining financial and operational impact in greater depth where macro-level generalisation is not possible. The analysis also reflects on the ethical and economic dimensions of cybersecurity investment and evaluates whether existing risk-based models adequately account for the systemic and cascading nature of cyber threats.

Overall, the methodology reflects a two-pronged strategy: first, enhancing data integrity through structured classification; and second, deriving insights through focused case evaluations. This design acknowledges both the opportunities and the limitations posed by the current state of maritime cyber incident data.

1.5 Contributions of the Study

This thesis offers a novel perspective on maritime cybersecurity by shifting the focus from technical vulnerabilities to the economic consequences of cyberattacks. It critically examined whether current publicly available data are sufficient to quantify macroeconomic impacts. A structured analytical framework was developed, combining quantitative trend analysis, qualitative case study evaluation, and a maritime-specific cyberattack taxonomy. This taxonomy standardises incident classification across fragmented sources, enabling multidimensional assessment of financial, operational, and

systemic impacts and supporting more consistent analysis and benchmarking for future research.

Through detailed examination of three major case studies, sector-specific vulnerabilities are identified, the effectiveness of mitigation strategies assessed, and the ethical tension between firm-level cost-benefit decisions and broader systemic risks is explored. Recommendations are proposed to improve to data collection and reporting practices, with the aim of contributing to the development of more transparent, reliable, and actionable cyber risk data within the maritime domain.

1.6 Outline of the Thesis

This thesis is structured into nine chapters. Chapter 1 introduces the research context, defines the research questions, and outlines the study's objectives and methodological approach. Chapter 2 presents a comprehensive literature review, covering the maritime cybersecurity landscape, key threat patterns, existing cyber incident databases, and economic impact assessment models. Chapter 3 details the mixed-methods research design, including the development of a structured taxonomy, the merging of two leading maritime cyber incident datasets, and the rationale for case study selection. Chapter 4 presents the core findings, offering a quantitative analysis of the dataset, the application of the taxonomy and Incident Severity Score (ISS) model, and three in-depth case studies. Chapter 5 provides a comparative and economic analysis of the case studies, drawing insights on vulnerability patterns, cost asymmetries, and strategic lessons. Chapter 6 discusses the broader implications of the research, including limitations of macroeconomic modelling, the utility of structured taxonomies, and the need for regulatory and institutional reform. Chapter 7 outlines the study's limitations, particularly regarding data completeness and methodological generalisability. Chapter 8 concludes the thesis and offers recommendations for policy, practice, and future research. Chapter 9 presents an executive summary, distilling the thesis' core contributions for a wider professional audience.

2 Background and Literature Review

The global maritime industry forms the backbone of international trade, facilitating approximately 80 per cent of global trade [1] by volume and over 70 per cent by value, with goods transported by sea and handled by ports worldwide [9]. This critical infrastructure faces numerous threats, including cyber threats, which carry profound economic ramifications. The global economy is heavily dependent on key maritime transport hubs. Significant disruption to any of them could and has lead to severe consequences across supply chains, affecting trade flows, destabilising insurance markets, and weakening the long-term competitiveness of maritime-dependent nations [10]

2.1 Introduction to Maritime Cybersecurity

Maritime operations long predate the advent of cyberspace, and their convergence is relatively recent development driven by digital transformation. Cyberspace is not only a global domain within the information environment, consisting of interdependent information technology (IT) infrastructures such as the Internet, telecommunications networks, and embedded processors, but also a time-dependent system of interconnected information systems and human users [11]. Its continuously evolving nature demands constant vigilance and adaptability, as stakeholders must respond swiftly to new threats, vulnerabilities, and innovations. Although cyberattacks are rarely categorised as acts of terrorism, their disruptive potential can resemble that of conventional threats. They have the capacity to cripple port operations, compromise navigation systems, and expose sensitive cargo data. Given the maritime sector's high degree of automation and interconnectivity, such attacks may also result in physical damage, endanger human lives, and cause environmental harm. In this sense, the asymmetry of cyber threats begins to mirror the disruptive logic of terrorism, where a relatively small act can yield outsized strategic consequences. Despite continuous improvements, the maritime industry continues to struggle with cyber resilience due to its dependence on legacy systems, weak regulatory oversight, and complex global supply chains [12].

Maritime trade plays a critical role global economy, extending its influence well beyond direct financial transactions. Research shows that GDP per capita is closely linked to maritime dependency [8]. Nations with more deepwater ports, better merchandise trade ratios, and stronger shipping connectivity tend to experience greater economic prosperity. Technological advancements and improved port access reduce transport costs, lower prices, increase global access to goods, and strengthen national economic output [8]. However, increasing reliance on digital technologies has introduced new vulnerabilities. Systems for port management, vessel navigation, and cargo tracking have expanded the attack surface, making critical maritime infrastructure a target for cybercriminals, state-sponsored groups, and hacktivists [13].

Digital transformation in maritime operations is a logical and inevitable development, aimed at improving efficiency, streamlining logistics, and enhancing operational safety. Advances in connected technologies enable greener, safer, and more efficient global shipping networks. In an increasingly competitive industry, digital tools represent a major opportunity for maritime companies [14]. The digitalisation and growing interconnectivity of maritime operations increasingly shift critical functions into cyberspace, expanding the sector's overall attack surface. Despite the rising frequency and sophistication of maritime cyberattacks, research on their economic consequences remain limited. While general cybersecurity impact studies exist, maritime-specific assessments of cyberattack costs and their broader economic effects are still underdeveloped.

This literature review prioritises empirical studies, technical analyses, and data-driven reports, excluding publications behind paywalls. It examines research that quantifies the costs of cyberattacks on ports and maritime infrastructure, alongside studies that contextualise these costs within broader economic frameworks. In doing so, it aims to identify practical methods for assessing economic impacts and to highlight persistent gaps requiring further investigation.

2.2 Challenges in Maritime Cybersecurity: People-Process-Technology

Despite growing awareness of cybersecurity risks, the maritime sector continues to struggle with underreporting, fragmented regulations, outdated infrastructure, and a significant workforce knowledge gap, all of which weaken its overall security posture.

Dependence on third-party service providers, legacy systems, and increasingly automated navigation technologies introduces additional vulnerabilities. These factors collectively introduce vulnerabilities that can be exploited by cybercriminals, state-sponsored actors, and opportunistic hackers [15].

In addition, structural and geopolitical risks further complicate the threat landscape. Strategic chokepoints, such as the Panama Canal, the Suez Canal, and major harbours present structural and geopolitical risks, that increase their attractiveness as cyber targets [15]. While not cyber nature, the 2021 Ever Given blockage starkly demonstrated how a single disruption can cascade through global maritime supply chains, underscoring the potential impact of a successful cyberattack on similar infrastructure [16]. To fully picture the cybersecurity challenges facing maritime economies, it is necessary to examine the sector through the lens of People, Processes, and Technology (PPT) with its complex operational and regulatory environment.

The PPT framework is widely used in cybersecurity analysis, but its application in the maritime domain requires the consideration of the sector's operational complexity, global interconnectivity, and historically low level of cybersecurity maturity [17]. These persistent gaps across human, procedural, and technological domains distinguish maritime cybersecurity from more conventional IT–OT (Information Technology – Operational Technology) environments and call for sector-specific solutions.

2.2.1 People: The Human Element

Major vulnerability in maritime cybersecurity lies in the human element. Many ship crew members, port operators, and logistics personnel lack sufficient cybersecurity training, making human error a frequent contributor to incidents [2], [17]. Common issues include falling victim to phishing attacks, mishandling credentials and neglecting basic cyber hygiene, which leaves critical systems exposed [18]. The shortage of specialised training programmes [19], [20] is further compounded by the global scarcity of cybersecurity professionals [21]. Unlike sectors such as aviation, finance, or energy, where cybersecurity training is standardised and mandatory, maritime often lacks consistent requirements. A longstanding culture that prioritises operational efficiency over safety and digital security further delays the adoption of digital safeguards [22].

Currently, there are no mandatory cybersecurity education requirements for seafarers under the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) [23], although the IMO recommends incorporating cyber risk management into safety management systems [24], implementation remains voluntary. In response to these gaps, several voluntary training initiatives have emerged, including Det Norske Veritas' (DNV), the e-learning modules on onboard vulnerabilities [25], the Maritime Institute of Technology and Graduate Studies (MITAGS) cybersecurity course [26], and the Maritime Cybersecurity Trained Professional (MarCybTPro) program [27]. The Estonian Maritime Academy has gone further, formally integrating cybersecurity into seafarer education, through undergraduate and postgraduate levels [28]. However, these efforts remain fragmented and inconsistent in scope, duration, and adoption. While the International Chamber of Shipping (ICS) provides Cyber Security Onboard Ships guidelines, they are advisory rather than enforceable within the domain.

The skills shortage continues to leave the industry vulnerable. A 2024 Fortinet report revealed that nearly 90% of organisations experienced breaches linked to inadequate cyber skills [21], [29]. Meanwhile, technology is reshaping seafarer roles. Increased reliance on automated systems has already reduced crew sizes [30], yet vessels often lack dedicated cybersecurity or IT personnel. Consequently, sailors without formal cybersecurity expertise are tasked with managing and repairing shipboard systems, often relying on minimal configurations to maintain simplicity [31]. This dependence on non-specialists not only increases the risk of misconfiguration but also complicates the implementation of robust cybersecurity protocols.

2.2.2 Process: The Operational and Regulatory Challenge

The maritime sector operates under a patchwork of fragmented and inconsistent cybersecurity regulations. Governance remains largely reactive, with many stakeholders taking action only after incidents occur rather than implementing preventive measures. This regulatory fragmentation weakens overall resilience and creates enforcement gaps across jurisdictions. Underreporting of cyber incidents remains a serious challenge. Concerns over reputational harm, legal liability, and operational disruption often deter disclosure [32], [33], [34]. The resulting lack of transparency hinders knowledge-sharing

and undermines collective risk assessment, limiting the industry's ability to learn from past incidents and strengthen its defences.

The complexity of maritime supply chains further compounds governance challenges. Operators often depend on external vendors and service providers whose cybersecurity standards vary widely. Some third-party actors lack even basic protections, increasing the risk of supply chain compromise [10]. Inadequate implementation of core security practices, such as access controls, encryption, and credential management remains common [18]. These process failures, although often linked to human error, reflect deeper organisational shortcomings in policy, oversight, and accountability. Given the sensitive data handled ranging from personal information to cargo routes and operational logs; weak governance exposes maritime actors to cybercrime, espionage, and even geopolitical conflict. Failures in cyber processes also carry physical consequences, as attacks on OT systems can disrupt services, endanger lives, and result in legal action [18].

Efforts to improve governance are underway. The IMO introduced Resolution MSC.428(98) requiring integration of cyber risk management into Safety Management Systems by 2021 [35], [36], Within the EU, the NIS2 Directive mandates cybersecurity provisions for critical infrastructure, including maritime operations [37]. However, adoption and enforcement remain uneven, particularly outside the EU, creating gaps across global trade routes. A more recent step toward consistency was taken by International Association of Classification Societies (IACS), which implemented two mandatory Unified Requirements: E26 (Cyber Resilience of Ships) and E27 (Cyber Resilience of Onboard Systems and Equipment) effective from January 2024 [38]. These set mandatory standards for ship-wide cyber resilience and onboard system protection, respectively. They apply to new vessels classed by IACS members and promote a lifecycle approach to cybersecurity, from design to operation.

Classification societies such as DNV, Lloyd’s Register, and Bureau Veritas have also developed voluntary cybersecurity certification schemes. Yet, without mandatory audits, adoption has been slow. Many operators delay investment until required by regulation or client pressure. Nonetheless, these societies continue to play a key role by issuing guidance, tracking emerging threats, and encouraging a culture of proactive risk management [39]. More details of the regulatory and governing bodies are provided in Appendix I.

2.2.3 Technology: The Digital Infrastructure Challenges

Maritime operations continue to rely heavily on legacy technologies. Many vessels still run outdated, unpatched software in Integrated Bridge Systems (IBS), Industrial Control Systems (ICS), and port-based IT infrastructure face similar issues. With ship lifespans ranging from 20 to 30 years, most onboard systems were not designed or built with cybersecurity in mind, leaving them highly susceptible to attacks [17]. Figure 1 illustrates the typical composition of maritime IT–OT architecture, where software and hardware jointly control physical devices in real time.

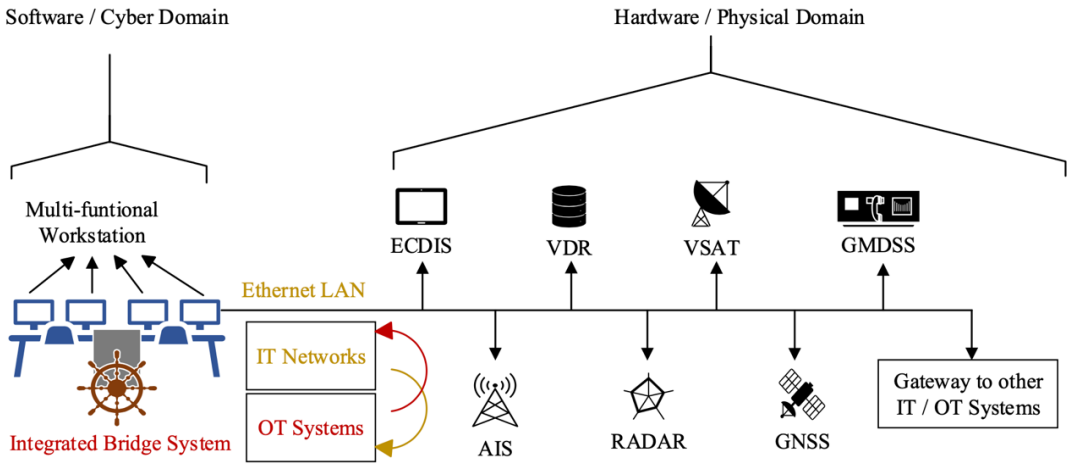


Figure 1 – Illustration of a typical maritime shipboard IT-OT system that combines software and hardware to monitor and control physical devices in real time [17]

Modernisation is slow. Operational constraints, regulatory inertia, and economic considerations delay IT upgrades across the sector. Meanwhile, ongoing digitalisation through Internet of Things (IoT) driven automation, cloud logistics platforms, and interconnected ship systems has significantly expanded the maritime attack surface. Increased IT–OT integration has exposed previously isolated components to cyber threats, often due to weak remote access controls, inadequate network segmentation, and insecure communications [30], [40].

One major cybersecurity gap is the absence of real-time threat monitoring. Few vessels or operators maintain dedicated Security Operations Centres (SOCs) for offshore assets. While shore-based SOCs exist, they rely on high-bandwidth connectivity, which is often unavailable at sea. Most vessels rely on Very Small Aperture Terminal (VSAT) satellite

networks, which are prone to signal interception, spoofing, and denial-of-service (DoS) attacks. Many still operate using outdated and insecure communication protocols, increasing exposure to eavesdropping and data tampering [17]. In parallel, jamming and spoofing of Global Navigation Satellite Systems (GNSS) remain viable attack vectors, capable of misrouting vessels disrupting operations [41].

Cyber-physical systems present another critical technological risk. Dynamic Positioning (DP) systems, essential for offshore operations, are increasingly targeted by cyberattacks. Threats such as GPS spoofing, malware, and unauthorised remote access can compromise DP functionality, causing vessel drift, loss of station-keeping, or propulsion failure. Research highlights the maritime sector's lack of standardised cybersecurity frameworks for cyber-physical risk assessment, leaving significant gaps in DP system protection [42]. The shift toward smart ports, AI-driven logistics, and autonomous shipping add another layer of complexity. These emerging technologies often outpace the development of security standards, resulting in inconsistent protection across platforms and jurisdictions. Many ports and shipping companies continue to rely on external IT providers, creating additional supply-chain vulnerabilities that can be exploited by [31].

2.2.4 Cybersecurity Investment Concerns

Although cybersecurity investment is increasing globally and within the maritime sector, underinvestment remains a persistent challenge. The global cybersecurity market is projected to grow at a compound annual growth rate (CAGR) of 14.3% [43], and 73% of maritime organisations report expanding cybersecurity budgets [39], indicating alignment with broader trends. However, perception of adequacy does not match investment levels: only 40% of maritime professionals feel their organisations invest sufficiently in cybersecurity [14]. This mismatch reflects broader structural and cultural challenges. The Maritime sector continues to exhibit a higher tolerance for cyber risk compared to other sectors. According to a 2023 survey, 61% of maritime professionals believe the industry should accept increased cyber risks to promote innovation and digitalisation, a notably higher rate than in sectors like energy and healthcare [39]. Such attitudes can delay proactive investments in critical defences.

Although average cybersecurity spending is rising, disparities persist. As of 2022, nearly two-thirds of maritime organisations were investing more than $100,000 annually [44], up from 54% in 2020 [2]. Yet these increases often fail to keep pace with growing threat

levels: the average cost of a maritime cyberattack rose from $182,000 in 2020 to $550,000 in 2022, with some operators incurring losses of up to $1.8 million [2]. Cyber insurance coverage also lags behind. Despite rising awareness of cyber threats, a substantial portion of the industry remains underinsured. Over one-third of operators have experienced cyber claims that were not covered [2], and study found 92% of potential cyberattack costs remain uninsured [45]. Across all sectors, 72% of companies still lack any source of cyber insurance [45].

Cost-saving pressures across the maritime industry driven by fuel efficiency targets, labour optimisation, and tight competition often result in cybersecurity being treated as an operational cost rather than a strategic investment. This short-term mindset undermines long-term resilience. A report by CyberOwl and HFW found that even as awareness increased, many operators failed to invest proportionately in protective measures [2]. Industry voices, such as DNV, emphasise that cybersecurity should be seen as a growth enabler and a safeguard for continuity, not just a compliance burden [46].

Finally, recent data from ENISA identifies ransomware as the most frequent cyber threat across the transport sector, accounting for 38% of reported incidents between January 2021 and October 2022. This is followed by data breaches at 30% [47]. Ransomware attacks have become a major source of operational downtime and cascading disruption in maritime logistics, further underscoring the urgent need for sustained cybersecurity investment.

2.3 Maritime Cyberattack Landscape: Database and Retrospective Analyses

This section critically analyses key studies on maritime cyberattacks, focusing on their methodologies, classifications, and contributions to understanding cyber risks in the maritime sector. The selected studies provide insights into cyber threat taxonomies, risk assessment models, and empirical analyses of cyber incidents.

2.3.1 Conceptual and Empirical Studies on Maritime Cybersecurity

Academic research into maritime cybersecurity has significantly expanded in recent years, offering a clearer view of the sector's evolving threat landscape, technical vulnerabilities, and organisational challenges. Several key studies have laid the

groundwork for understanding both the operational risks and broader implications of cyber threats in maritime contexts.

Meland et al. (2021) provide a foundational a retrospective analysis of 46 maritime cyber incidents from 2010 to 2020, identifying major attack vectors such as ransomware, GPS spoofing, AIS manipulation, phishing, and malware targeting bridge systems and port IT network [48]. While the study confirms that maritime cyber incidents are less frequent than those in other sectors, it demonstrates that their financial, operational, and reputational consequences can be disproportionately severe. The authors emphasise the role of cybercriminals, state-sponsored actors, and organised crime in targeting both vessels and shore-side infrastructure. A critical barrier identified is the persistent underreporting of incidents, which limits the effectiveness of risk assessment and weakens the sector's collective resilience. As shown in Figure 2, the rise in reported incidents coincides with increased IT–OT system integration, underscoring the urgent need for structured risk assessment models and economic impact evaluations.

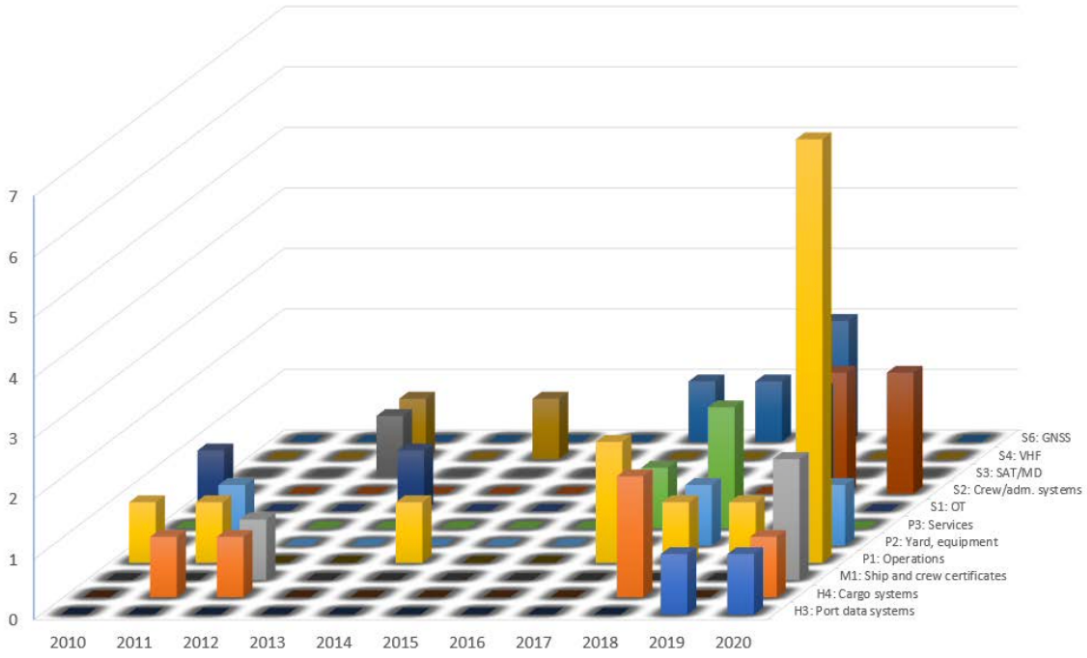


Figure 2 – Cyber incidents by year and attack vector [48]

Li et al. (2024) extend this analysis through a comprehensive review IT–OT vulnerabilities in maritime systems. They introduce a multi-dimensional taxonomy classifying cyberattacks by actors, vectors, and affected systems (Figure 3) [17]. Their work provides a detailed technical framework but omits deeper analysis of physical safety

risks, such as threats to human life and navigation integrity. While environmental impacts are briefly addressed, the study underrepresents the cascading failures that can result from compromised control systems. Moreover, the taxonomy offers only limited categorisation of attacker motivations and threat complexity, especially in cases involving ICS and SCADA platforms. These limitations highlight the need for a standardised taxonomy that can inform both threat modelling and economic assessment.

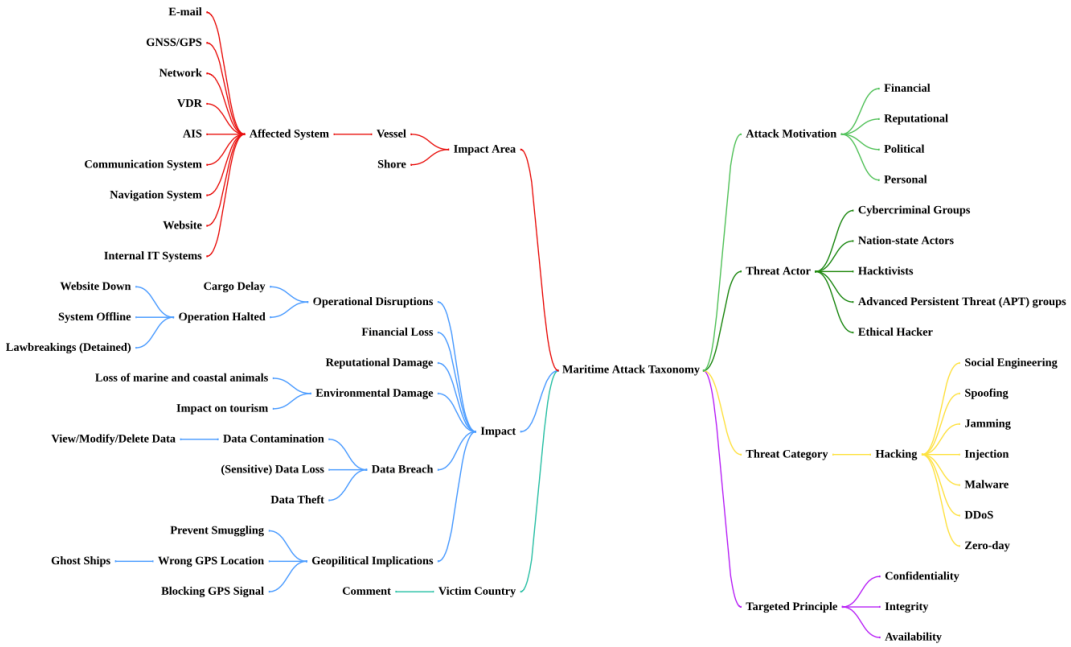


Figure 3 – Multi-dimensional maritime cyberattack taxonomy [17]

Further refinement of maritime cyber risk assessment comes from Mohsendokht et al. (2024) who apply a Bayesian Network (BN) to historical incident data to establish probabilistic dependencies among threats, affected sectors, and external risk factors [49]. Their analysis offers a valuable structure for quantifying the operational impact of cyberattacks and distinguishes between stationary and mobile maritime assets. One key insight is the identification of cyber-physical interdependencies, exemplified by the Port of Antwerp case, where attackers exploited IT systems to facilitate illegal cargo operations. While this study contributes significantly to cyber risk modelling, it is constrained by its reliance on the Maritime Cyber Attack Database (MCAD) data, which introduces potential biases. The authors acknowledge the lack of alternative datasets and the absence of integrated economic analysis, both of which limit the generalisability of the model and its practical application in investment planning. While Figure 2 (Meland et al.) illustrates the temporal distribution of cyber incidents by attack vector, Figure 4

(Mohsendokht et al.) builds on this trend by presenting incidents categorised by attack type, based on structured MCAD data. Despite similar visual patterns, the two seemingly continuation of each other; the differing categorisation approaches present the challenges of data standardisation and taxonomy alignment in maritime cybersecurity research.

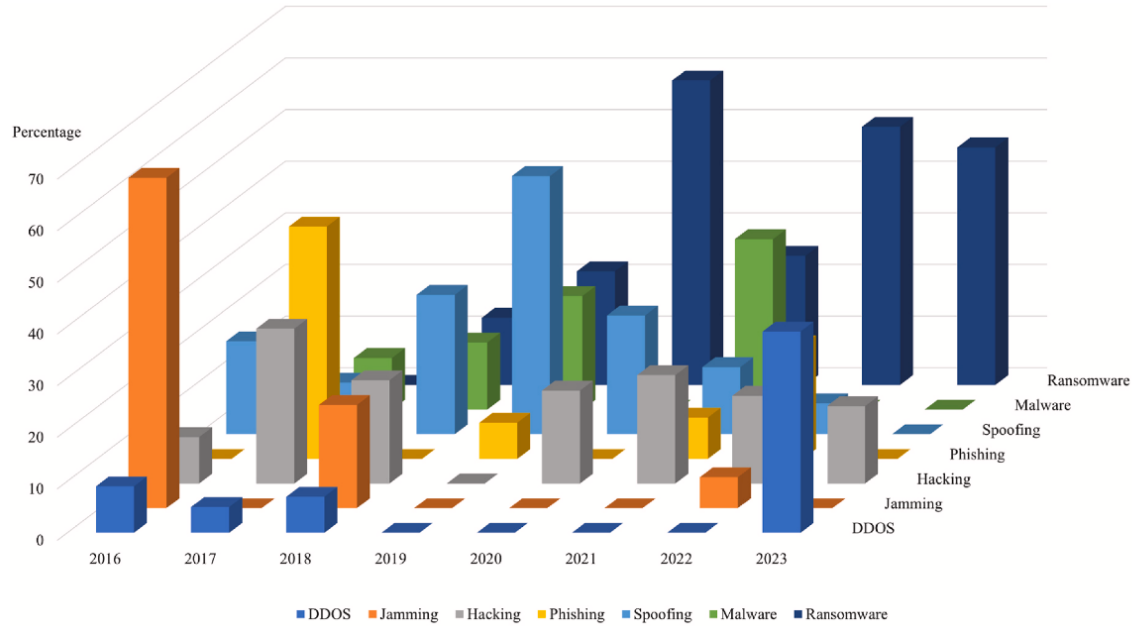


Figure 4 – Distribution of cyberattacks over 8 years [49]

Clavijo Mesa et al. (2024) offer a broader view by conducting a systematic review of 110 maritime cybersecurity studies. Their work maps global research trends, revealing that the United States, United Kingdom, and China lead in scholarly output, while Europe and the Asia-Pacific region emerge as key contributors. The study identifies eight dominant types of cyberattacks affecting maritime operations, spanning ransomware, unauthorised access, GPS spoofing, phishing, and attacks on cargo systems. Notably, their bibliometric analysis captures not only thematic focus but also publication dynamics, with a surge in output observed after 2015 and a peak between 2020 and 2023. This trend aligns with increased regulatory scrutiny and high-profile cyber incidents that elevated the topic on research agendas. As shown in Figure 5, the review provides a visual overview of research hotspots, keyword clusters, and geographic dispersion of contributions [50]. Despite the expanding literature, the authors highlight persistent gaps in risk assessment methodologies and the limited development of models for quantifying economic impacts. The study calls for more interdisciplinary approaches that link technical vulnerabilities to financial risk, regulatory needs, and systemic resilience.

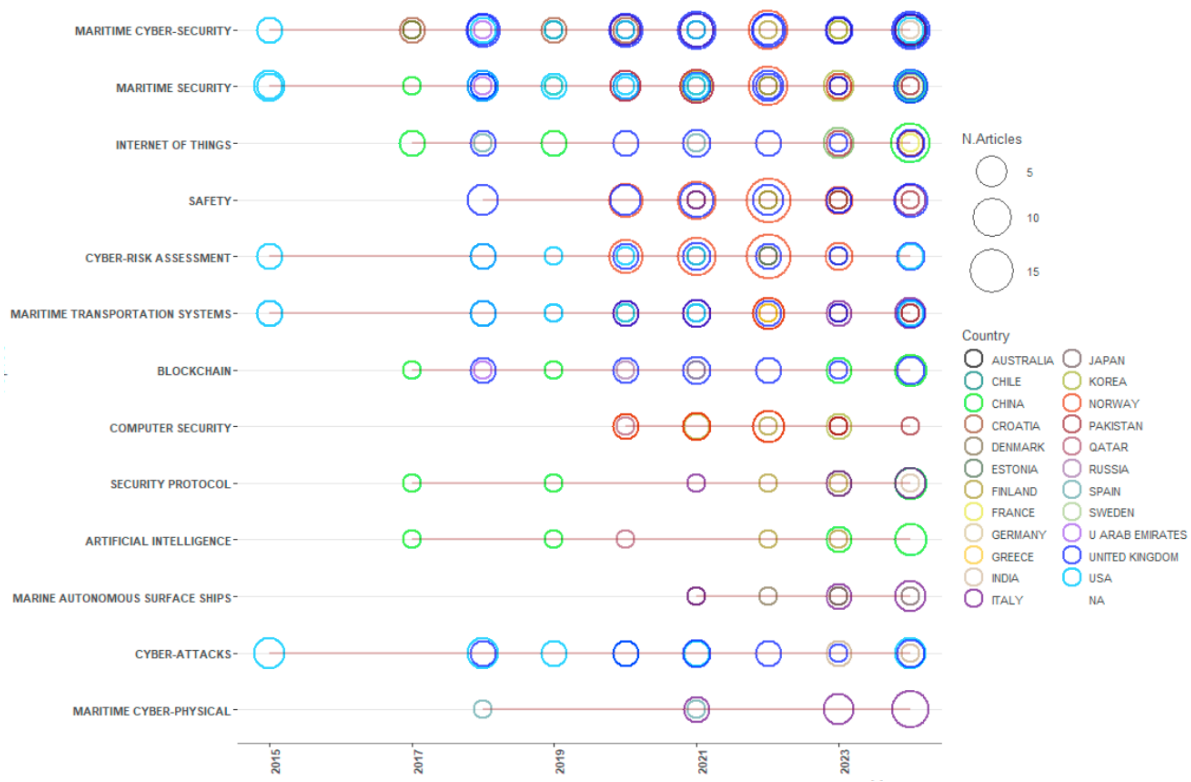
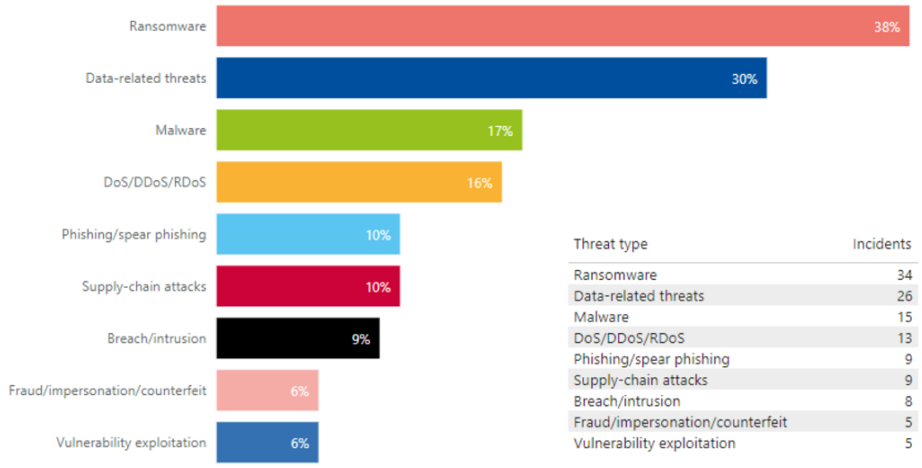


Figure 5 – Bibliometric overview: geographical distribution, recurring research topics, and publication trends [50]

Complementing these academic perspectives the European Union Agency for Cybersecurity (ENISA) published its 2023 updated Transport Threat Landscape, analysing 98 cyber incidents across the transport sector between January 2021 and October 2022 [47]. Although limited to a two-year window, the findings are statistically consistent with other long-term datasets and reinforce the maritime sector's position as a critical and increasingly targeted component of global logistics.

ENISA attributes the rise in reported maritime cyber incidents to both the growing threat landscape and improved visibility stemming from regulatory measures such as the original NIS Directive and the expanded NIS2. Ransomware remains the most prevalent threat across all transport sectors, followed by unauthorised access, data leaks, and Distributed Denial-of-Service (DDoS) attacks (Figures 6 and 7). Maritime entities, particularly those relying on third-party vendors, are shown to be highly exposed to supply chain attacks. While ENISA's analysis does not always quantify financial losses, it draws attention to significant operational and reputational consequences and identifies both cybercriminal and state-sponsored actors as prominent threat sources.



Threat type	Incidents
Ransomware	34
Data-related threats	26
Malware	15
DoS/DDoS/RDoS	13
Phishing/spear phishing	9
Supply-chain attacks	9
Breach/intrusion	8
Fraud/impersonation/counterfeit	5
Vulnerability exploitation	5

Figure 6 – Prime threats to the transport sector (January 2021 to October 2022) [2]

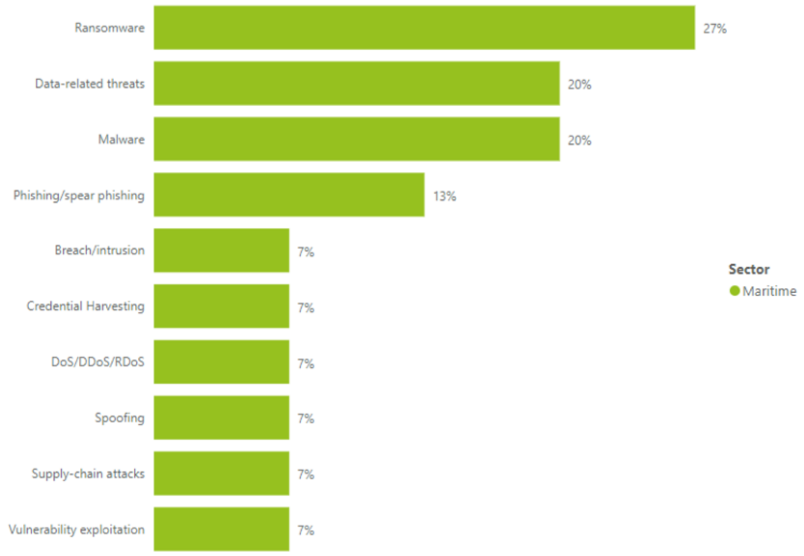


Figure 7 – Prime threats to Maritime transportation [47]

The report also addresses the growing convergence of cyber and physical domains. Attacks on IT systems increasingly lead to tangible consequences such as vessel rerouting or port shutdowns. Although digital impacts are more frequently reported, the relatively high proportion of physical effects in the maritime domain, compared to other transport sectors, suggests the sector's higher susceptibility and vulnerability to cyber-physical disruption (Figures 8 and 9). However, a significant share of incidents has outcomes listed as "unknown," suggesting continued challenges in reporting consistency and classification. ENISA's recommendations include adopting security-by-design principles, improving cross-sector collaboration, and strengthening incident disclosure mechanisms. While the report enhances visibility into maritime cyber threats, it also highlights ongoing data quality issues that hinder effective economic modelling and

policy development. These findings echo broader concerns within the academic literature regarding the persistent difficulty of quantifying the economic consequences of maritime cyberattacks.

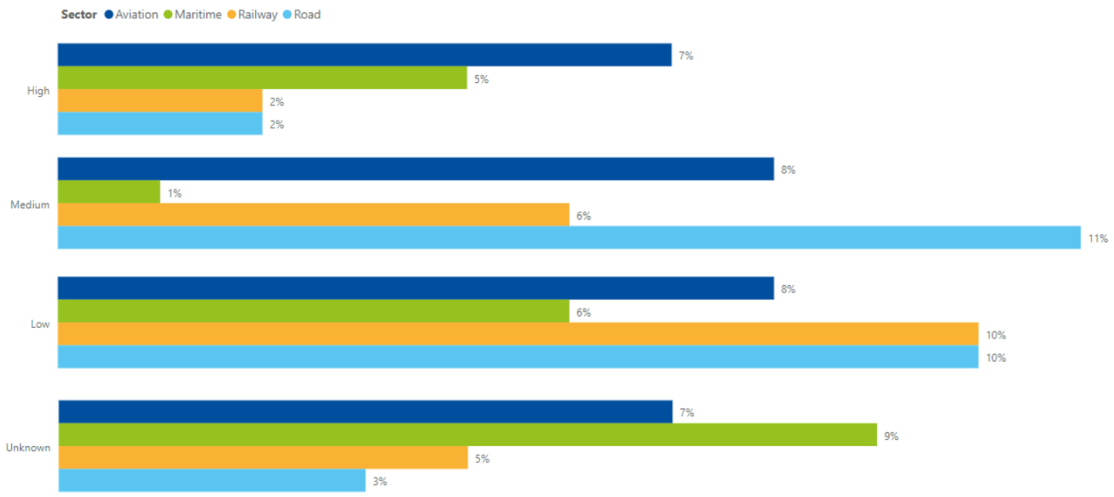


Figure 8 – Digital impact of cyberattacks [47]

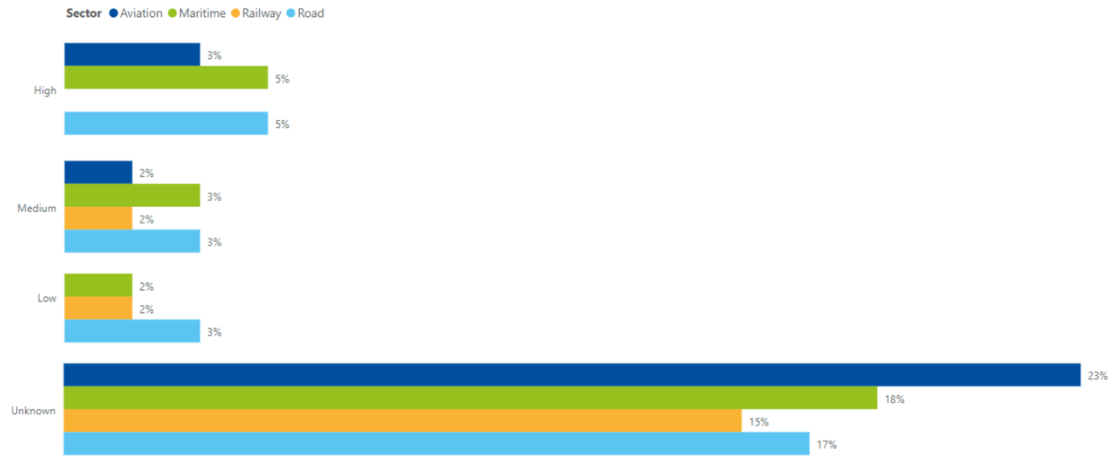


Figure 9 – Physical impact of cyberattacks [47]

2.3.2 Strategic Threats, Geoeconomic Weaponisation and State-Sponsored Actors

The maritime sector's central role in global trade, energy transportation, and supply chain stability has increasingly exposed it to state-sponsored cyber threats. Nation-state actors exploit vulnerabilities in maritime infrastructure not merely for espionage or disruption, but as a means of exerting economic coercion against adversaries. In this context, cyberattacks are no longer incidental or opportunistic, they have become strategic tools of economic warfare. These threats add a new dimension to the economic implications of maritime cybersecurity incidents, as cyber operations now seek to undermine not just

individual companies, but the functioning of global trade networks and critical logistics infrastructure [51].

Publicly available datasets, such as those analysed later in Section 2.3.3, significantly underrepresent the involvement of state-affiliated actors in maritime cyber incidents. However, more targeted threat assessments suggest a notable increase in nation-state focus on the sector. ENISA highlights that maritime operations, along with other transport infrastructure, are increasingly being attacked not solely for financial gain but also to destabilise essential services and induce broader economic instability [47]. Unlike conventional kinetic conflict, cyberattacks offer states a relatively low-cost, high-impact method of achieving strategic objectives under the cover of plausible deniability and without triggering military escalation [52]. This is visualised in Figure 10, indicating proportionally higher state-sponsored actors than other sectors of transportation. Evidence suggests that actors such as China, Russia, North Korea, and Iran have conducted cyber operations against port facilities, logistics platforms, and vessel navigation systems, often to gather intelligence, disrupt rival economies, or signal geopolitical intent [51].

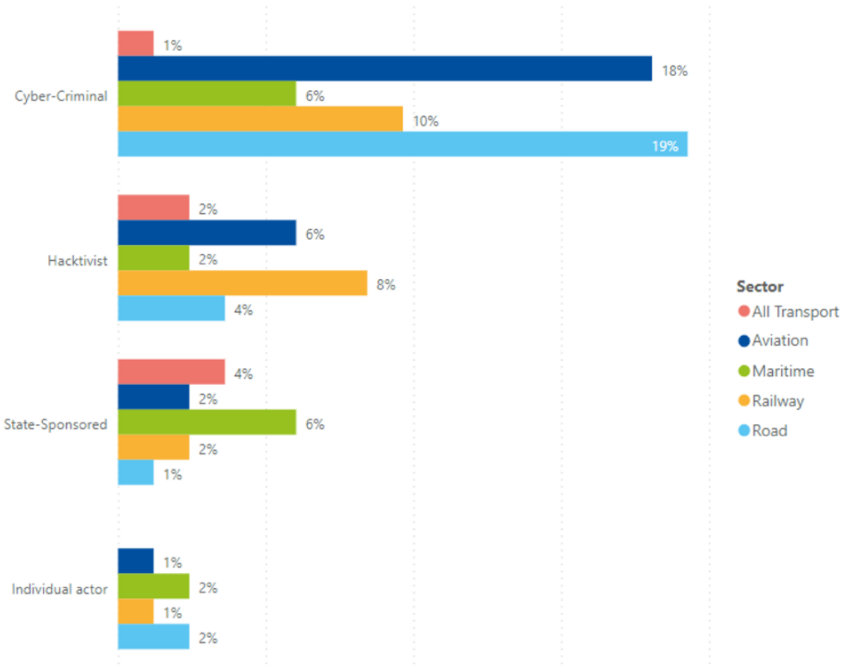


Figure 10 – Threat actors according to sectors within transportation 2021-2022 [47]

One of the most prominent tactics used in state-sponsored maritime cyber operations is Global Navigation Satellite System (GNSS) spoofing and jamming. Between 2016 and 2019, more than 1,300 instances of GPS interference affecting commercial vessels were

recorded, particularly in geopolitically sensitive regions [53]. These disruptions have intensified since 2022, with frequent incidents reported in the Mediterranean, Black Sea, Middle East, Baltic Sea, and Arctic regions [54]. Spoofing attacks compromise a vessel's navigational accuracy, posing serious operational risks and threatening maritime safety. Onshore, cyber intrusions into port management systems can lead to delayed cargo handling, disrupted shipping schedules, and destabilisation of regional trade flows. As illustrated in Figure 10, transportation sectors are increasingly affected by a diverse range of threat actors, while Figure 11 visualises the global spread of GPS interference on a typical day, highlighting the correlation between reduced navigational accuracy and suspected jamming zones [47], [55], [56].

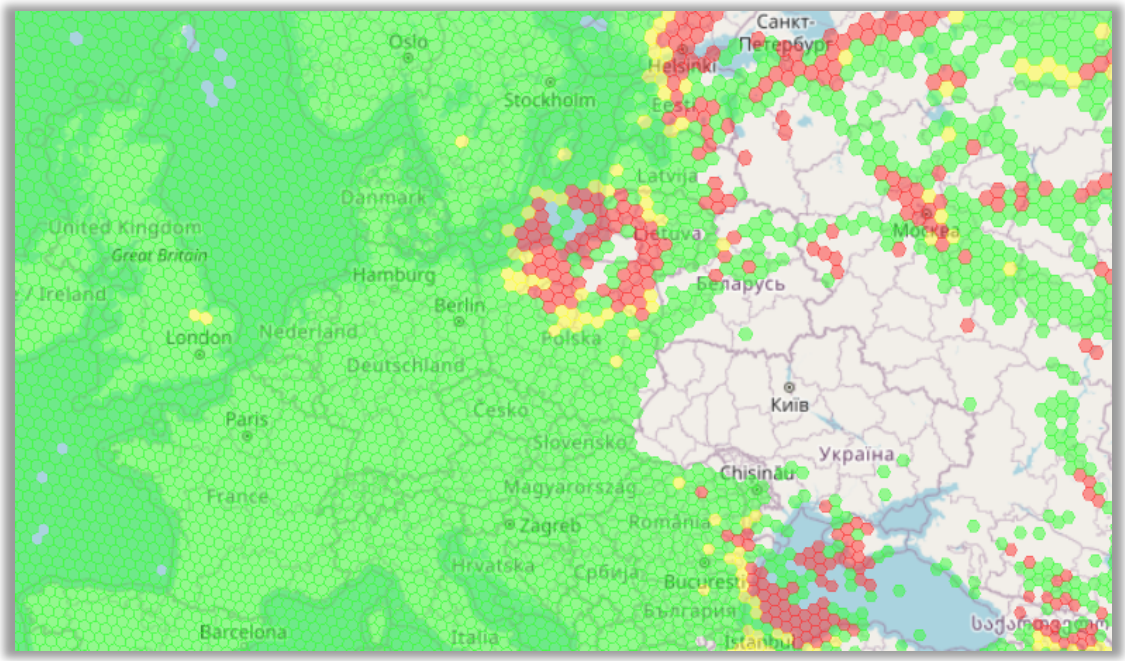


Figure 11 – Daily maps of GPS interference on February 27, 2025 [55]

The economic consequences of such cyber operations extend far beyond the direct losses suffered by targeted companies. Attacks on key maritime chokepoints, as the Suez Canal, Strait of Hormuz, and Malacca Strait can generate macroeconomic ripple effects. Disruptions to these critical transit routes delay oil shipments and container flows, inflating freight rates and global energy prices. Figure 12 shows the volume of daily petroleum transit through these regions reflecting the scale of potential impact [57]. While alternative routes may exist, they are often slower, less secure, or economically inefficient, thus amplifying the financial shock. Cascading effects are caused not only by halting geographical choke points, but companies that operate within the supply chain.

The 2017 NotPetya attack on Maersk offers a prominent example of how a single cyber operation attributed to a state-affiliated group can result in cascading effects across the maritime sector. The attack paralysed operations at 76 ports worldwide and inflicted estimated damages of $300 million, revealing how digital vulnerabilities can translate into severe global supply chain disruption [58] (presented in more detail in Chapter 5). Other notable incidents have similarly compromised port authorities, customs systems, and shipboard management platforms, [51], [59].

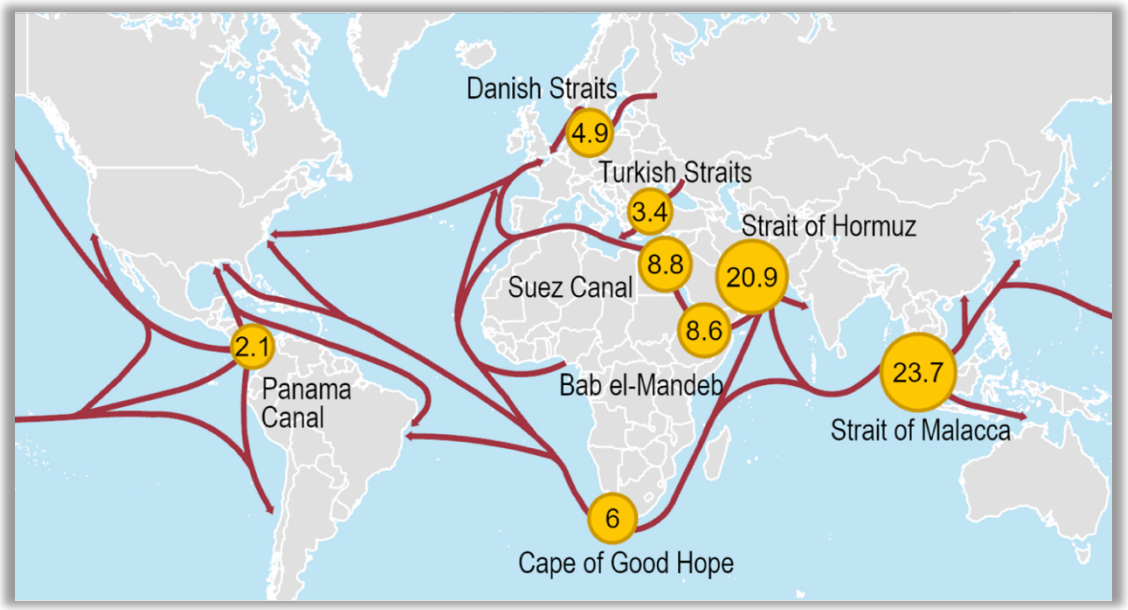


Figure 12 – Vulnerable global maritime chokepoints - Daily transit volumes of petroleum and other liquids through world maritime oil chokepoints (million barrels per day) (2023) [57]

The motivations behind state-sponsored cyberattacks in the maritime domain are diverse and strategically significant. These operations serve to coerce economic behaviour, conduct surveillance of vessel movements, steal proprietary technologies, and assert regional influence. Cyberattacks allow hostile states and revisionist regimes to degrade economic resilience and political stability in rival nations without engaging in overt conflict. This approach reflects a broader pattern of strategic competition in which adversaries operate below the threshold of armed confrontation, using persistent and deniable cyber activity to undermine global institutions and erode confidence in the international economic order. Cyberspace provides both state and non-state actors with the tools to wage long-term campaigns against maritime infrastructure and logistics, bypassing traditional deterrence frameworks while blurring the line between civilian and strategic targets [60].

Attribution remains one of the most persistent challenges in addressing these threats. The covert nature of cyber operations, combined with sophisticated obfuscation techniques, often prevents the definitive identification of perpetrators. Unknown is the amount of cyberattacks that never surface because the impact is thought to be some kind of malfunctioning, error, or goes unnoticed. While international bodies such as the IMO have issued guidelines encouraging the incorporation of cyber risk management into maritime governance frameworks [24], these remain non-binding and lack the enforcement capacity required to deter state-sponsored cyber aggression. As a result, significant regulatory and legal gaps persist, particularly in relation to geoeconomic cyber incidents. The absence of robust, enforceable international mechanisms leaves maritime operators increasingly vulnerable to covert strategic campaigns, which may evolve in sophistication and scale as geopolitical tensions continue to rise [2].

2.3.3 Maritime Cyberattack Databases: Strengths and Limitations

Reliable and structured data on maritime cyber incidents is essential for analysing threat patterns, quantifying the number of cyberattacks (NCA), and evaluating their operational and economic implications. Databases have emerged, compiled by academic institutions, government agencies, non-profit groups, and private industry. These databases vary in terms of access, scope, and methodological transparency. While some are open and publicly accessible, others remain closed due to confidentiality agreements, industry sensitivity, or commercial licensing.

Notable subscription-based or restricted-access platforms include the **Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC)** [61], which supports incident reporting and real-time intelligence exchange among U.S.-based maritime stakeholders; the **CSO Alliance Maritime Cyber Alliance** [62], which offers a secure portal for cyber incident reporting within the commercial shipping industry. The Repository of Industrial Security Incidents (RISI) is a subscription database that includes maritime-relevant incidents targeting industrial control systems. In addition, the **U.S. Coast Guard** publishes selected bulletins and alerts on maritime cybersecurity incidents via its public Maritime Cyber Resource Center, though these are not maintained as a structured, quarriable dataset [63].

For the purposes of academic research and quantitative analysis, only a few databases provide open, structured, and maritime-specific incident data. Among these, two stand

out for their comprehensiveness and accessibility: the **Maritime Cyber Attack Database (MCAD)** [59], hosted by NHL Stenden University of Applied Sciences in the Netherlands, and the **ADMIRAL database** [64], curated by France's Maritime Computer Emergency Response Team (M-CERT). Both datasets are publicly available, focused exclusively on maritime domains, and provide incident-level metadata that includes attack method, victim type, sectoral classification, and temporal-spatial characteristics. These features make them uniquely suitable for identifying patterns in maritime cyberattacks and for estimating the NCA in support of this thesis's initial empirical analysis. The following subsections critically examine each database's structure, strengths, and limitations.

The MCAD, is an open-access initiative developed by the Maritime IT Security Research Group at NHL Stenden University of Applied Sciences. Launched in 2021 and publicly accessible via URL: maritimecybersecurity.nl, it consolidates over 290 documented cyber incidents affecting the Global Maritime Transportation System (GMTS) between 2001 and 2023 and represents one of the most structured and comprehensive public resources dedicated exclusively to maritime cybersecurity. MCAD provides researchers, policymakers, and industry professionals with a valuable resource for analysing cyber threats within the GMTS. Its comprehensive structure allows for both technical investigation and high-level trend visualisation, facilitating broader insight into cyber risk exposure across the sector.

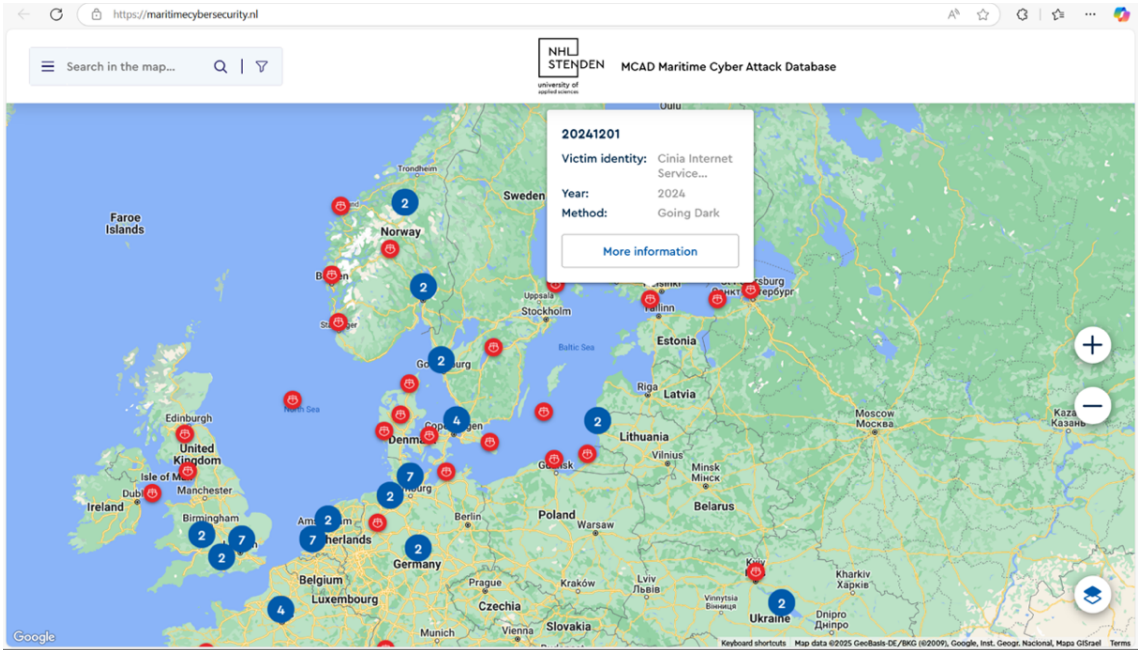


Figure 13 – MCAD map format representation [59]

Designed as a cyber threat intelligence (CTI) tool, MCAD addresses the sector's long-standing challenge of fragmented and underreported incident data. The platform draws on a wide range of open sources including peer-reviewed research, media coverage, government disclosures, and cybersecurity vendor reports; and organises the information in a structured format aligned with MITRE's Structured Threat Information eXpression (STIX) model. Each entry includes metadata such as attack method, affected system (e.g., port, vessel, or offshore unit), victim identity and country, incident location (including GPS coordinates where possible), and impact type. Users can interact with a dynamic map interface to filter incidents by year, region, or attack type (Figures 13 and 14).

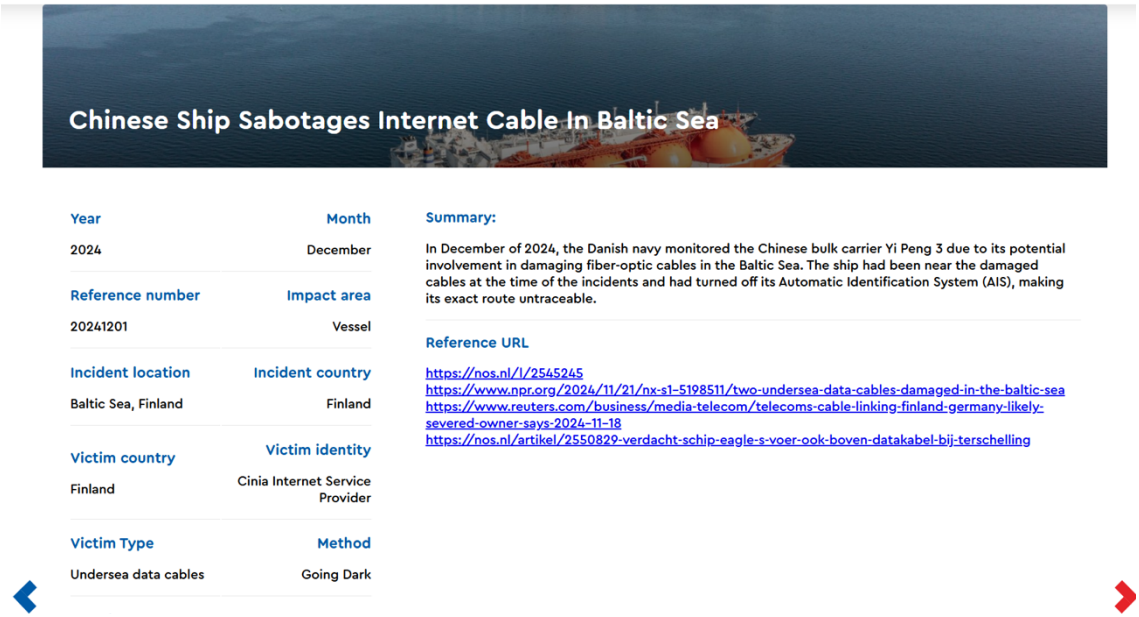


Figure 14 – MCAD databased example of recorded attack on Chinese ship sabotage on internet cable in the Baltic Sea [59]

MCAD's strengths lie in its transparency, quarriable interface, and structured maritime-specific taxonomy. It supports both academic and industry use cases by enabling high-level trend analysis, sector-specific breakdowns, and longitudinal visualisation. Pijpker et al. (2024) preprint formally introduces the database and presents aggregated statistics across multiple threat categories [65]. Notably, the database reveals a marked rise in incidents from 2020 onward, with ransomware emerging as the dominant attack method, accounting for over half of cases where method is known (Figure 15). The dataset also enables geopolitical attribution: incidents attributed to Russia, China, North Korea, and Iran collectively account for 80% of attacks with known origin, while most frequent

victims are based on OECD economies: United States, United Kingdom, Germany, and South Korea (Figure 16).

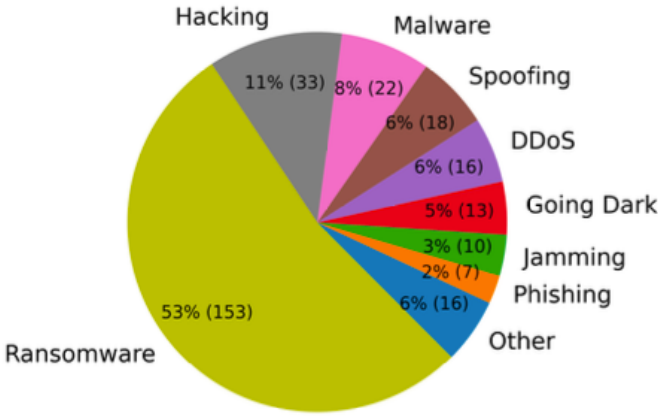


Figure 15 – Proportions of incidents in MCAD employing different attack methods [65]

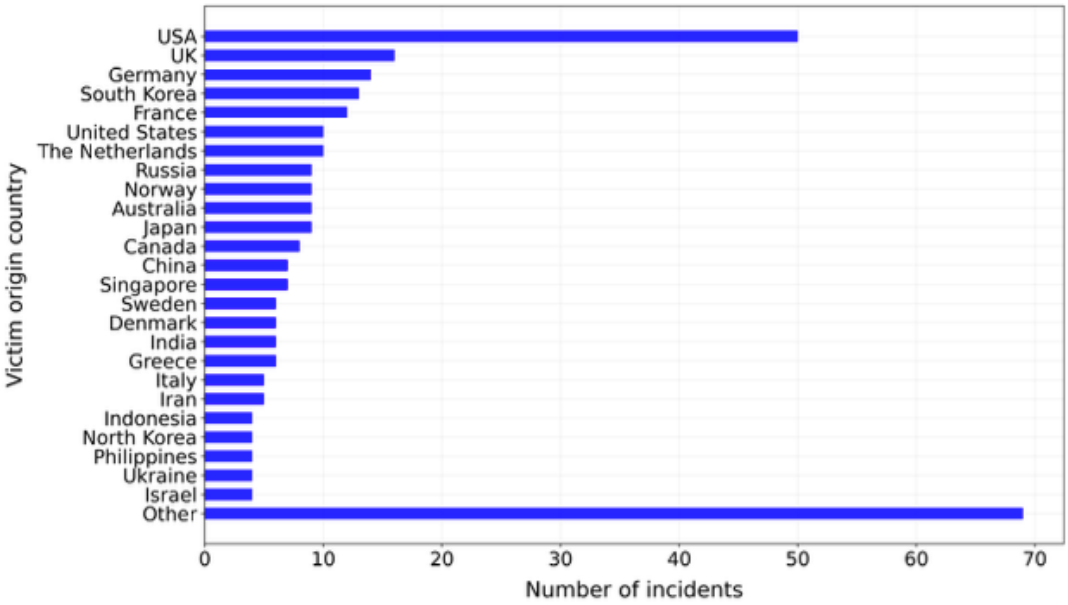


Figure 16 –- Frequencies of incidents targeting victim organisations from different countries. Only incidents where victim country is known are included [65]

Despite its contributions, MCAD presents notable methodological limitations. In 2021, a substantial upgrade introduced more than 260 additional incidents, yet earlier time period was not retrospectively revised under the new framework. This methodological discontinuity creates a potential distortion in longitudinal trend analyses, exaggerating post-2020 incident growth. Its attacker attribution lacks granularity and precision: while dataset lists country of origin, it does not reliably distinguish between cybercriminal activity and state-sponsored campaigns, complicating strategic risk and adversary profiling. Other shortcomings are in incident classification, victim identification, and

geolocation. For example, one Vancouver-based malware attack was incorrectly attributed to Canada instead of the United States, while some GNSS spoofing events have been mislabelled as DoS attacks. These inconsistencies necessitated additional cross-validation and data cleaning during this thesis's empirical analysis. Despite its limitations, MCAD marks a major advancement in maritime cybersecurity research. Its structured data format, visual tools, make it a valuable resource for analysts. However, interpretations must be made with caution due to attribution ambiguities, inconsistent taxonomy application, and data validation gaps.

The other database available for research is the Advanced Dataset of Maritime cyber Incidents ReleAsed for Literature (ADMIRAL) [64]. It is an open-access maritime cyber incident repository curated by the Maritime Computer Emergency Response Team (M-CERT) under France Cyber Maritime. Launched in 2017, ADMIRAL is designed to support maritime cybersecurity education, risk awareness, and academic research by providing a structured account of publicly disclosed cyber incidents affecting the maritime sector. As of March 2025, the dataset contains 473 recorded incidents spanning 1980 to 2024, representing 64 countries and 22 maritime subsectors, categorised into 16 incident types. Although both datasets share the objective of documenting maritime cyber incidents over roughly the same two-decade period, their contents differ significantly in scope, classification, and emphasis. This divergence highlights how institutional perspective and data curation methods influence and shape the results of trend analyses. For example, the same incident may be categorised differently or excluded entirely, which introduces uncertainty in efforts to quantify NCA, sectoral exposure or economic impact.

A key strength of ADMIRAL is in its sector-specific granularity, that enables researchers to examine how specific maritime operations (e.g., ports, offshore platforms, cargo management systems) have been affected over time. However, the classification framework differs significantly from MCAD, complicating direct comparisons and reinforcing the broader challenge of taxonomic inconsistency in maritime cyber incident reporting. As illustrated in Figures 17 and 18, discrepancies in threat categorisation and temporal patterning across ADMIRAL and MCAD demonstrate how methodological decisions affect analytical outcomes. These differences do not necessarily indicate inaccuracy but represent the absence of standardised, universally accepted maritime cyber taxonomy. In these two graphs the main attack methods represented identified in each

database can be compared. Both datasets capture the same trend in overall volume, however the attack types vary significantly.

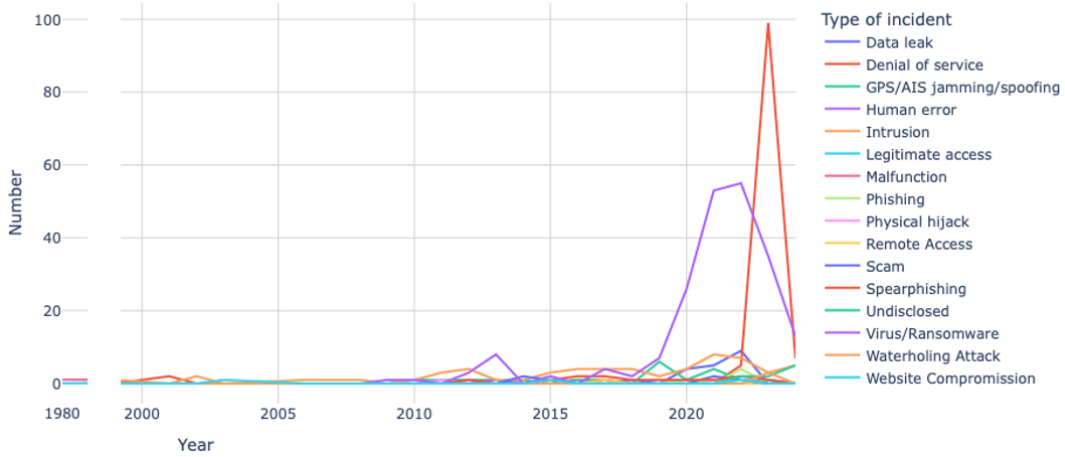


Figure 17 – Evolution of maritime cybersecurity incident types publicly disclosed over the years (according to ADMIRAL database) [64]

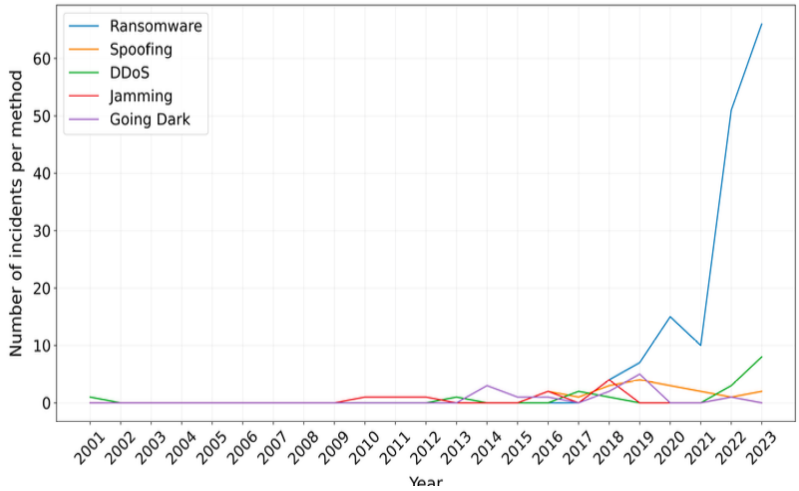


Figure 18 – Frequency of incidents in MCAD involving five main attack methods (according to MCAD database) [65]

Despite its utility, ADMIRAL also exhibits notable limitations. Duplicate entries are present across the dataset, some justifiably reflecting incidents with multi-vector or multi-sector impacts, but others appearing redundant without explanation, thus inflating aggregate counts. Many entries also suffer from incomplete descriptions, with vague or missing details regarding technical methods, threat actors, or consequences. In addition, the database contains several incidents that do not clearly qualify as either cyberattacks or in some rare cases maritime events, such as software failures lacking indicators of malicious activity (e.g., entries 1980_001, 2017_005). These findings necessitated careful dataset refinement before use in quantitative analysis. The database's classification of threat actors also presents conceptual overlap and interpretive challenges (Figure 19).

Their taxonomy does not make clear distinction between “type of threat actor” or their “motivation”. As shown in Figure 16, categories such as cybercrime (47.8%), hacktivism (23.7%), and politically motivated attacks (1.2%) may not always be mutually exclusive, while state-sponsored activity is recorded in only 0.2% of cases, a figure that appears extremely low given increasing geopolitical interest in maritime infrastructure targeting, and the figure does contradict other earlier mentioned reports.

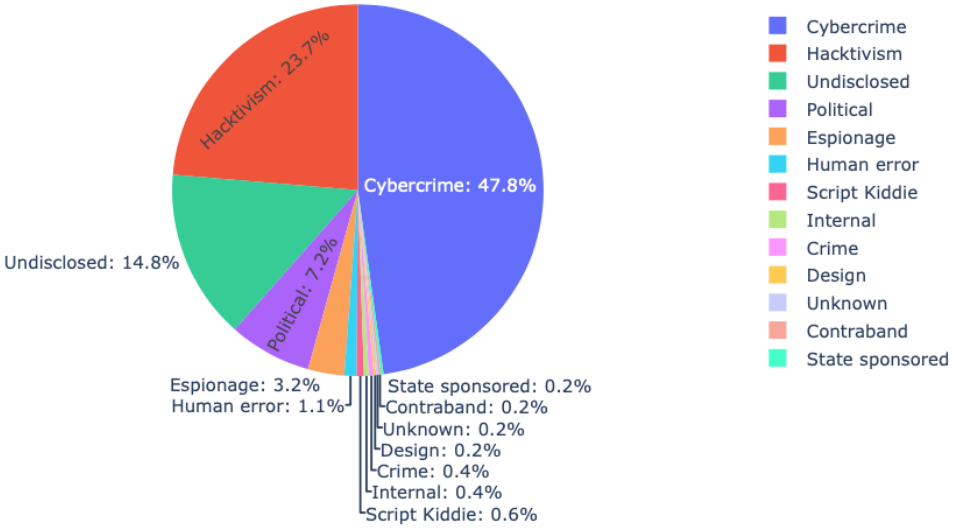


Figure 19 – Distribution of incident origins for publicly disclosed maritime cybersecurity incidents [64]

Geographic distribution further reflects the dataset’s institutional origin. As a French-managed platform, ADMIRAL shows a notably higher share of incidents involving French entities (Figure 20), in contrast with the more internationally distributed scope of MCAD (Figure 13). While this does not imply deliberate bias, it highlights how institutional perspective and source selection can shape the resulting threat landscape.

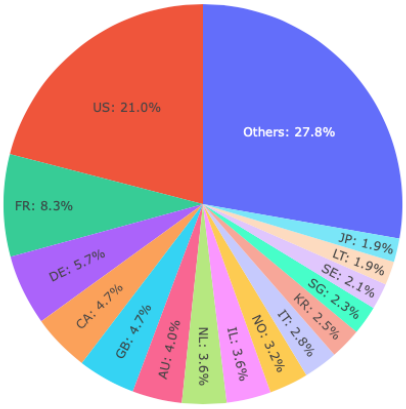


Figure 20 – Top 15 victim countries of maritime Cybersecurity incidents publicly disclosed [64]

The comparative analysis of MCAD and ADMIRAL highlights the broader challenge of maritime cyber threat research: in the absence of a harmonised taxonomy and standardised classification methodology, differences in data structure, inclusion criteria, and institutional perspective can significantly shape analytical outcomes. These discrepancies do not necessarily reflect inaccuracies but underscore the need for cautious interpretation and transparent methodological framing in maritime cybersecurity studies.

2.3.4 Summary of Gaps in Maritime Cyberattack Literature and Data

Despite a growing body of research on maritime cybersecurity, significant gaps remain in data quality, methodological consistency, and economic impact analysis. Much of the existing literature focuses on technical vulnerabilities and attack typologies but lacks integration with economic risk assessment frameworks. The absence of a standardised categorisation and definitions hinders comparative studies; while underreporting (or inaccessible data) and inconsistent incident classification reduce the reliability of available datasets. Publicly accessible sources such as the MCAD and ADMIRAL offer valuable insights, yet both are constrained by data omissions, regional biases, and definitional inconsistencies. Moreover, state-sponsored threats are often underrepresented or obscured, complicating threat attribution and strategic risk modelling. The limitations underscore the need for more structured data collection, cross-disciplinary methodologies, and improved transparency to enable meaningful evaluation of the economic consequences of maritime cyberattacks. The accessible data quantity suggests that the recorded incidents are only mere fraction of what the reality might be.

2.4 Economic Impact of Maritime Cyberattacks

The increasing digitalisation of maritime sector has amplified its exposure to cyber threats, making the assessment of economic impact a priority for both researchers and industry stakeholders. However, as discussed in previous section, reliable and standardised data on cyber incidents in the maritime domain remain scarce [10]. Most publicly available records are either incomplete, based on incident narratives, or suffer from inconsistent classification and disclosure practices. While there are potentially severe reputational, legal, and regulatory effects, they are particularly difficult to quantify. Even direct financial losses are frequently reported with limited transparency and may evolve over time [47]. This section critically evaluates existing economic modelling

approaches that aim to quantify the cost of cyberattacks and discusses their relevance and limitations in the context of the maritime sector. The findings serve to explain why macroeconomic estimation was originally intended in this thesis but ultimately deemed unfeasible due to data constraints.

Among the most widely cited models in economic impact estimation are Input–Output (I-O) Models and Dynamic Inoperability Input–Output Models (DIIM). These macroeconomic tools analyse interdependencies between sectors using national accounts data to estimate cascading effects. They offer a structure approach to quantify cascading effects of cyberattacks across industries between and have been successfully applied in critical infrastructure modelling [7], [66]. However, their application in the maritime domain is limited by the absence of maritime-specific cyber incident data and the inability to isolate port and vessel operations within aggregated supply chain flows. Maritime transport is deeply embedded in multi-sectoral global logistics chains, and most economic models lack the granularity to reflect this complexity accurately. Moreover, the time-series data required to calibrate DIIM models are rarely available in the maritime sector, particularly when it comes to digital disruption.

Event study methodologies evaluate financial impacts by analysing stock price fluctuations before and after reported cyber incidents. This approach is well established in financial economics and can capture short-term investor reactions to security breaches [7]. Yet its relevance to maritime cyber risk remains limited. Many maritime companies are privately held or form subsidiaries within diversified conglomerates, making stock market analysis an imprecise measure of incident impact. Even in the case of listed firms such as Maersk, stock prices are affected by global economic factors, geopolitical tensions, and logistical trends confounding any attribution of market response to a specific cyberattack, as demonstrated in the case study analysis in Chapter 5. Therefore, this method fails to offer a consistent or sector-wide estimation model.

Cyber insurance and actuarial models offer a different perspective. These rely on historical claims data to calculate average losses associated with various types of cyber incidents [2], [66], [67]. Theoretically, they can include indirect costs often excluded from direct impact assessments, such as legal fees, reputational damage, and business interruption. However, their utility in the maritime context is severely limited (at least at the moment). Many maritime organisations remain uninsured or underinsured against

cyber threats, and when insurance is held, confidentiality agreements often prevent public disclosure of claims data. Consequently, reliable actuarial datasets specific to the sector are either inaccessible or non-existent. As this thesis relies solely on open-source data, therefore this modelling was excluded from the analytical framework. Several studies have proposed macro-level risk projection models that correlate cyberattack costs with national economic indicators such as GDP, number of cyberattacks, and technological readiness indices like the ICT Development Index (IDI) [6], [66], [67].

These models aim to estimate systemic risk and aggregate cyber losses at national or global scales, offering potential value for economists and policymakers assessing long-term exposure. However, such models tend to generalise risk at an abstract level that does not account for the specific characteristics of the maritime sector. Data on maritime cyber incidents remains limited and inconsistently classified across jurisdictions, making it difficult to isolate sector-specific patterns from national datasets. Furthermore, digital readiness indices such as the IDI (or even the newer AI Preparedness Index) primarily reflect terrestrial connectivity or governance structures, and do not account for maritime-specific IT-OT integration, vessel-level digitalisation, or port logistics vulnerabilities. While these macro-indices point in a promising direction, any calculation based on incomplete or imbalanced maritime cyber data risks producing misleading or non-representative results.

In response to the shortcomings of generalised frameworks, a limited body of research has explored sector-specific models tailored to maritime operations. For instance, Weaver et al. [68] employed optimisation-based simulations using a Nearly-Orthogonal Latin Hypercube (NOLH) design to estimate port-level operational losses. Similarly, Tam et al. [69] introduced the Cyber-Physical Econometric Model (CyPEM), which integrates cyber risk with inter-sectoral dependencies to model the shockwaves from attacks on port systems. These efforts represent significant progress but are constrained by their dependence on sensitive operational datasets, computational complexity, and assumptions that may not generalise across diverse port infrastructures (or the entire maritime sector). Furthermore, the limited number of validated maritime cyber incidents complicates parameter calibration, reducing model reliability.

A more qualitative approach involves scenario-based assessments and historical case studies. These draw on both real-world events and simulated scenarios to model potential

disruptions and their consequences. Studies by Soner et al. [70] and Turner et al. [71] illustrate this approach, through analysing ransomware and malware attack scenarios across different maritime contexts. While such assessments can uncover systemic weaknesses and provide rich insights into operational impact, their reliance on assumptions and narrative modelling limits their generalisability and reproducibility. Their interpretive nature limits their reproducibility, comparability, and scalability across regions or timeframes.

Despite the diversity of the variety of available models, a recurring obstacle in all frameworks is the lack of reliable, standardised, and openly accessible maritime cyber incident data. This absence is not a result of methodological incompatibility but a consequence of fragmented regulatory oversight, inconsistent incident disclosure, and reputational concerns that discourage reporting. The limited granularity of available data prevents meaningful econometric modelling at either global or regional levels. For this reason, the thesis concludes that current macroeconomic or statistical models cannot be meaningfully applied to assess the cost of maritime cyberattacks across countries or time periods. This assessment led to a shift in thesis scope. As data environment proved insufficient to support macroeconomic modelling, the thesis pivots toward a dual focus: first, the development of a maritime cyberattack database supported by a structured taxonomy to enable future impact analysis; and second, a comparative case study approach that illustrates the diversity of economic impacts through detailed analysis of selected incidents. Table 1 below summarises the key methodologies and evaluates their relevance to maritime cyber risk assessment:

Table 1 – Economic impact evaluation methodologies comparison

Model	Strength	Limitations
I-O Model	Captures cascading effects, applicable to multiple industries	Lacks maritime-specific focus, requires national economic data
Event Study (Stock Market Reactions)	Captures real-time financial impact	Excludes non-public companies, high market volatility skews results
Cyber Insurance and Risk Models	Uses actuarial data for realistic cost estimations	Limited access to insurance claims, does not include non-insured entities or geopolitical attacks
Global GDP-IDI-NCA Models	Provides macroeconomic cost estimates, useful for policymakers	Lacks maritime specificity, relies on broad indicators that may misrepresent impact
Econometric Model	Transparent methodology, adaptable for various sectors	Not tailored to maritime cyber incidents

Optimization Model	High granularity in port disruptions, data-driven	Computationally intensive, requires extensive operational data
CyPEM	It models systemic risks and integrates cyber-physical aspects	Complex parameter estimation, maritime cyberattack data scarcity
Scenario-Based Model	Provides real-world and hypothetical insights, highlights systemic vulnerabilities	High reliance on assumptions, limited economic quantification

Looking forward, the refinement of hybrid models that integrate actuarial, scenario-based, and macroeconomic elements could enhance maritime cyber risk assessment. Progress depends on improved incident reporting, regulatory harmonisation, and anonymised data sharing mechanisms. If supported by structured, sector-specific data collection, existing economic models can eventually be adapted to produce scalable, reproducible, and actionable estimates of the true cost of cyberattacks in the maritime domain.

2.5 Gaps in the Literature

While existing literature on maritime cybersecurity provides substantial insights into technical vulnerabilities, threat taxonomies, and risk assessment models, gaps remain in the assessment of the economic impacts of cyberattacks on the sector. The key gaps identified are as follows.

2.5.1 Lack of Standardised Economic Impact Models

Existing macroeconomic and risk estimation models such as input-output, event studies, or insurance-based frameworks, either generalise across sectors or lack the granularity to account for maritime-specific operational structures. Their applicability is limited due to insufficient sectoral data and the inability to isolate the maritime component in national or global indicators.

2.5.2 Absence of a Unified and Scalable Quantification Framework

While some studies suggest theoretical frameworks for quantifying cyber risk, there is no operationalised, scalable approach currently applied to maritime cyberattack data. This thesis addresses this gap by introducing a taxonomy-based classification system and severity scoring model, offering a structured foundation for future quantification efforts rather than a finalised framework.

2.5.3 Fragmented and Incomplete Incident Data

Open-source datasets, are constrained by inconsistent entries, overlapping incidents, and missing metadata. Many attacks remain undisclosed due to various reason, severely limiting the empirical basis for macroeconomic analysis.

2.5.4 Lack of Structured Maritime Cyber Incident Data Collection

Absence of comprehensive taxonomy that integrates both economic and operational attributes of maritime cyberattacks. This gap is addressed here by developing a multi-dimensional classification system tailored to maritime realities, enabling comparative analysis and severity evaluation.

2.5.5 Limited Integration of Economic and Cyber-Physical Risk Models

While existing maritime cybersecurity research acknowledges the convergence of IT and OT systems, few studies systematically explore the cascading effects of cyberattacks on physical operations, vessel safety, and human lives. The limited integration of cyber-physical risk analysis restricts understanding of real-world consequences, particularly regarding navigation failures, cargo mismanagement, and environmental hazards. This remains a recognised but underdeveloped area of study.

2.5.6 Inconsistent Terminologies and Classification Standards

A lack of common taxonomies, terminologies across the research landscape complicates cross-study comparison and dataset merging. By aligning MCAD and ADMIRAL under a unified schema, this thesis makes an original contribution toward taxonomy

3 Research Methods

3.1 Research Design and Approach

This study was initially motivated by the ambition to calculate the macroeconomic consequences of cyberattacks targeting maritime economies. The early hypothesis was informed by insights from the Thomas Murray report [6], which demonstrated a measurable correlation between cyberattack frequency, GDP growth, and levels of digital development. It was reasoned that, given the maritime sector's foundational role in enabling global trade, cyberattacks affecting maritime operations could cause economic impacts even greater than those observed in other industries.

The early phase of the research focused on compiling macroeconomic indicators for major maritime nations or regions. While these variables were accessible through established sources such as the World Bank and e-Governance Academy, obtaining consistent and sufficient data on maritime-specific cyberattacks proved considerably more challenging. The number of documented incidents was disproportionately low when compared to global statistics, highlighting the severe underreporting and fragmentation in publicly available data. As a result, the research direction was revised. Two open-source cyberattack datasets the MCAD and the ADMIRAL database were assessed and merged to obtain the NCA. However, it became evident during this process that the quantity and quality of incident data were insufficient to support a statistically sound macroeconomic analysis. Many nations had no reported incidents at all, while others exhibited overlapping or inconsistently classified events. Although macroeconomic indicators such as GDP and DDL were successfully collected attempting to correlate maritime-specific cyber incidents with them, under such conditions would have led to biased and unreliable conclusions.

This realisation prompted a methodological shift: from pursuing a top-down econometric model to developing a taxonomy-driven mixed-methods approach. The revised strategy prioritised assessing whether it is possible to meaningfully estimate the economic impact of maritime cyberattacks using currently available data. Instead of attempting precise

macroeconomic calculations, the research focused on exploring the potential for such analysis through structured data and case-based evidence. The new approach involved three main components: first, cleaning and standardising a merged dataset from two open-source maritime cyber incident databases; second, developing a novel taxonomy to categorise incidents across operational, technical, and impact dimensions; and third, conducting in-depth case study analyses of three major cyberattacks. In parallel, the study examined cybersecurity investment from a cost-benefit perspective and critically reflected on the limitations of existing data, offering implications for policy development and future modelling frameworks.

This chapter outlines each of these methodological components in detail, explaining how they contribute to answering the research questions and exploring the broader feasibility of measuring the macroeconomic effects of maritime cyberattacks.

3.2 Data Collection and Processing

A structured, multi-source data collection process was employed to enable a meaningful assessment of the economic consequences of cyberattacks on maritime operations. The data collection phase aimed to establish a comprehensive dataset that enables economic impact analysis addresses measurement challenges and facilitates comparative case studies.

3.2.1 Data Sources

Data were sourced from both primary and secondary materials. The primary sources included the MCAD, a structured dataset documenting global maritime incidents from 2001 to 2025, and the ADMIRAL database, curated by France Cyber Maritime and covering incidents from 1980 to 2024. Secondary sources included industry reports, cybersecurity publications, regulatory frameworks issued by organisations such as the IMO, NIST, and ENISA, and forensic analyses and operational impact disclosures from documented case studies.

3.2.2 Data Merging and Standardisation

Merging the MCAD and ADMIRAL datasets required a multi-step standardisation process. Terminologies were aligned using a newly developed maritime cyberattack taxonomy. Duplicate incidents, often listed under variant names or partial metadata were

consolidated, while misclassified events were re-evaluated and reclassified, particularly those with incorrectly assigned vectors or victim sectors. External validation was performed using open-source intelligence and cybersecurity publications. The final cleaned dataset forms the analytical foundation for trend analysis in Chapter 4 and aided the case study selection for Chapter 5.

3.3 Development of a Maritime Cyberattack Taxonomy

A key contribution of this research is the development of a structured maritime cyberattack taxonomy, which does not currently exist in academic literature or industry frameworks. While NIST, ENISA, and IMO guidelines provide cybersecurity classification systems for threat and risk assessment, none are specifically tailored to documenting and analysing maritime cyberattacks. Principles that guided data restructuring was keeping it simple and concise, while making sure scalability for the future; ensuring reliability, credibility and validity; and addressing the ethics of data collation in general.

3.3.1 Data Compilation and Taxonomy Development

Through the systematic analysis of MCAD and ADMIRAL datasets, the study developed a novel classification taxonomy. This taxonomy enables accurate incident classification across multiple dimensions, facilitates longitudinal and cross-sectoral trend analysis, and supports financial impact estimation. It also strengthens risk identification, informs incident response evaluation, and reveals regulatory blind spots. The taxonomy was iteratively refined through manual validation, open-source research, and integration of intelligence from ransomware disclosures and cybersecurity reports. The analytical approach of this study comprises two integrated strands, aimed at evaluating whether current data and analytical tools are sufficient to estimate the economic impact of maritime cyberattacks and, if not, to identify the limitations and underlying causes.

3.3.2 Case Study Selection and Justification

Recognising that underreporting and incomplete cost disclosure in publicly available cyberattack databases prevent solid conclusions for sectoral or macroeconomic impact analysis, this research prioritised detailed case studies as the primary method for assessing economic consequences. Case studies were selected to address the limitations of

underreported and inconsistently quantified incident data. These studies enable financial evaluation of direct and indirect losses, examination of operational disruption and cascading effects, and assessment of cybersecurity response strategies. Selection was guided by criteria such as the severity of impact, availability of financial and operational data, diversity of attack vectors and affected entities, and the broader strategic relevance of each case.

3.3.3 Selected Case Studies

The three case studies selected are the 2017 NotPetya attack on Maersk, which disrupted global shipping; the 2020 Ragnar Locker ransomware attack on CMA CGM; and the 2021 ransomware incident affecting South Africa's Transnet port infrastructure. Each case illustrates a distinct typology of maritime cyberattack and highlights different dimensions of economic and systemic risk.

3.3.4 Quantitative Analysis

The quantitative component of the analysis focuses on identifying trends and patterns within a structured dataset of maritime cyber incidents. Temporal and spatial dynamics were evaluated by analysing changes in incident frequency, attack vectors, sectoral targeting, and geographical distribution over time. A custom Incident Severity Score (ISS) was applied to measure the relative impact of incidents across operational, financial, and safety domains. Financial impact estimates were included where available, drawing from public disclosures and benchmark reports, with clear limitations regarding completeness and statistical generalisability. While the primary emphasis of Chapter 4 is on quantitative pattern recognition, these insights laid the foundation for the comparative and qualitative evaluations conducted in the subsequent case studies.

3.4 Cost-Benefit Considerations in Cybersecurity Investments

This thesis incorporates cost-benefit considerations into the broader analytical framework by qualitatively comparing cybersecurity investment levels to documented incident consequences. This was achieved by reviewing industry reports, post-incident evaluations, and case-specific investment actions (e.g., Maersk and Transnet). While quantitative modelling of return on investment was not feasible due to data constraints, financial indicators, where available were examined to assess whether investment levels

appeared proportionate to risk exposure. These reflections informed the comparative and strategic analysis later conducted in Chapter 5.

3.5 Data Processing and Analytical Tools

Data processing and analysis were conducted using Microsoft Excel and Python, enabling statistical summarisation and trend visualisation. Graphs, tables, charts and classification schemes were created with Microsoft Excel, draw.io, and XMind.

3.6 Data Limitations and Challenges

This research acknowledges significant limitations within available maritime cyberattack data, particularly regarding financial disclosures and cross-sectoral impact mapping. Underreporting remains a pervasive issue, driven by reputational risks, regulatory inconsistencies, and the covert nature of many cyber incidents. As R. Ottis observes, "a victim of a truly successful cyberattack will never be aware of the attack, instead blaming their apparent misfortune on mistakes of their staff or accidental failure of their technology [72]. Several critical limitations affected the analysis. Most incident records lacked comprehensive cost data, especially for indirect losses such as legal exposure, productivity decline, or reputational damage. Cost estimation methods varied significantly across sources, hindering comparison. The fragmentation of existing cyber incident databases required extensive manual validation due to inconsistent classification standards, overlapping entries, and diverging timeframes. To address these issues, a multi-source validation strategy was applied, integrating grey literature and industry reports. The challenges reflect the broader systemic difficulties in estimating macroeconomic consequences from maritime cyberattack data alone.

3.7 Validation and Reliability

To ensure reliability, incident records were cross-referenced across various sources, measured against regulatory filings. Priority was given to primary disclosures, such as company reports and insurance documents, in cases of conflicting accounts. Duplicate records were resolved by matching date, target, vector, and impact characteristics. The final dataset was classified using a consistent taxonomy (Appendix II), ensuring comparability and future adaptability.

3.8 Ethical Considerations

This research adheres to ethical standards for data use, privacy, and transparency. All information was drawn from publicly available sources; no personal or confidential data was processed. Sensitive incidents were not included, and financial uncertainty as acknowledged through transparent citation. References to any underground activity were based on public web documentation, without direct interaction. The study maintains academic integrity and aims to contribute constructively to policy and maritime risk awareness.

3.9 Abandoned Econometric Modelling Path: Justification and Lessons Learned

An early aim of this thesis was to replicate and adapt an existing econometric model, most notably the economic analysis of Thomas Murray analytics on calculating the cost of cyberattacks [6]. Their approach relied on the availability of macroeconomic indicators, digitalisation indices, and cyberattack frequency per country. The intent was to narrow this framework to the maritime sector, using sector-specific incident data to perform a panel regression analysis correlating cyberattack frequency or severity with economic outcomes such as trade throughput or GDP growth. However, this direction proved unfeasible mostly due to data scarcity and geographic incompleteness. Most maritime cyberattacks are not reported or lack economic quantification, making regression dependent variables unreliable, and many countries (or regions) had zero or unverified incident entries, preventing consistent cross-country comparisons. Maritime specific indexes on digitalisation, cybersecurity readiness, do not yet exist in a globally standardised or complete form. By analysing databases, and online incident reports, sampling bias was revealed. Incidents are clustered around countries with better reporting practices, inflating regional comparisons and weakening the statistical power. Despite exploratory attempts to regroup data by world regions, the incident volumes remained too low for credible modelling. Instead of forcing econometric methods on insufficient data, the research pivoted toward the development of a robust maritime cyberattack taxonomy and structured database, aiming to enable future quantification, aiming to create the bases for the planned analysis. This shift ultimately enriched the study by highlighting what is needed before sector-specific econometric analysis can be viably pursued.

4 Findings and Analysis

This chapter presents the core quantitative findings of the research, aiming to bridge the gap between the technical characteristics of maritime cyberattacks with their broader economic and operational consequences. It is grounded in a newly consolidated dataset that merges the two leading publicly available maritime cyberattack databases. These sources were harmonised and integrated using a novel taxonomy developed as part of this thesis to classify incidents by attack type, severity, impact area, and associated economic indicators. The chapter is structured as follows: First section details the process of dataset consolidation and classification (Section 4.1 – 4.3), followed by a series of quantitative insights derived from structured analysis (Section 4.4). This includes trends in attack type, operational consequences, financial data availability, attribution, and severity. The chapter addresses and reflects on data quality and methodological constraints across multiple sections, particularly addressing limitations encountered during scoring and analysis. Insights derived from this chapter inform the broader discussion on the economic cost of maritime cyberattacks and support the feasibility assessment linked to the main research question and sub-question RQ1. The in-depth case studies, which further contextualise these findings and explore individual incidents in greater detail, are presented separately in Chapter 5.

4.1 Dataset Consolidation and Taxonomy Development

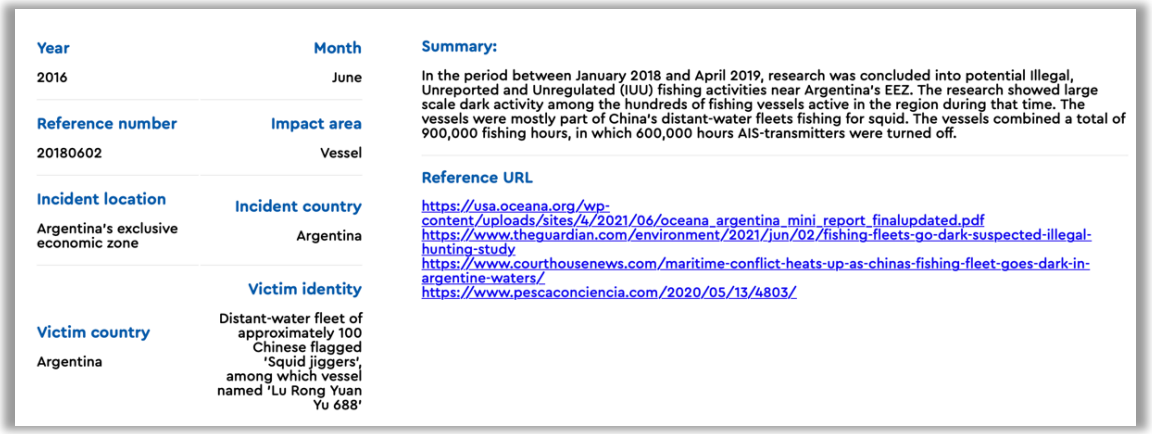
4.1.1 Overview of the Merged Dataset

The analytical foundation of this research is a consolidated dataset composed of two publicly accessible cyber incident databases: the MCAD and the ADMIRAL database (introduced in Section 2.3.3). At the time of analysis, MCAD contained 337 incidents and ADMIRAL 473. While both cover roughly the same time period and are collected with the same scope and aim, they present incidents using different formats and classification conventions. Prior to analysis, both datasets were converted to a unified format to enable cross-comparison. To ensure consistency, all entries were cleaned, deduplicated and

manually verified. This included cross referencing events with open-source intelligence (OSINT), third party reports, relevant publications and news articles. Duplicates were identified based on matching incident titles, dates, affected organisations, and similar technical characteristics. Some incidents were found to appear in both databases under different identifiers and descriptions. After consolidation, the merged dataset comprised approximately 600 unique and verified records. This harmonisation process allowed the integration of multiple data fields into a consistent analytical framework. Wherever data was incomplete or ambiguously labelled, additional research was undertaken to supplement missing values. This included identifying the correct victim organisation, clarifying the nature of the attack, and specifying affected infrastructure or assets. The cleaning process revealed substantial inconsistencies in both datasets, ranging from incomplete location data and errors in timestamps to misattributed actors or incorrect sector classifications.

4.1.2 Cleaning Challenges and Case Example

A notable challenge in dataset consolidation was the ambiguous or inconsistent classification of incidents. Many entries lacked clear indicators of whether a digital system was deliberately targeted or merely exploited to support a physical crime. For example, MCAD case 20180602 (Figure 21) describes a series of illegal fishing incidents involving the deactivation of Automatic Identification System (AIS) devices by Chinese-flagged vessels operating in Argentina's Exclusive Economic Zone (EEZ). Although the



Year
2016

Month
June

Reference number
20180602

Impact area
Vessel

Incident location
Argentina's exclusive economic zone

Incident country
Argentina

Victim identity
Distant-water fleet of approximately 100 Chinese flagged 'Squid jiggers', among which vessel named 'Lu Rong Yuan Yu 688'

Victim country
Argentina

Summary:
In the period between January 2018 and April 2019, research was concluded into potential Illegal, Unreported and Unregulated (IUU) fishing activities near Argentina's EEZ. The research showed large scale dark activity among the hundreds of fishing vessels active in the region during that time. The vessels were mostly part of China's distant-water fleets fishing for squid. The vessels combined a total of 900,000 fishing hours, in which 600,000 hours AIS-transmitters were turned off.

Reference URL
https://usa.oceana.org/wp-content/uploads/sites/4/2021/06/oceana_argentina_mini_report_finalupdated.pdf
https://www.theguardian.com/environment/2021/jun/02/fishing-fleets-go-dark-suspected-illegal-hunting-study
https://www.courthousenews.com/maritime-conflict-heats-up-as-chinas-fishing-fleet-goes-dark-in-argentine-waters/
https://www.pescaconciencia.com/2020/05/13/4803/

Figure 21– Cyber incident case reference number 20180602 from MCAD database [73]

case involves digital manipulation, the vessels were not cyberattack-victims in the traditional sense, but they actively disabled their AIS systems to avoid detection while

conducting illegal activity. This introduces a definitional challenge: should the deliberate exploitation of a digital system for concealment be classified as a cyberattack, particularly when it does not involve an external intruder or malicious software? As the indecent is not stand alone one, but a pattern appearing regularly, it needs attention.

4.2 Taxonomy Development and Application

4.2.1 Rationale and Design Objectives

To enable structured analysis and overcome the inconsistencies observed in existing maritime cyber incident datasets, a custom Maritime Cyberattack Taxonomy was developed as part of this study. The primary purpose of the taxonomy is to provide a standardised framework for classifying cyber incidents in the maritime domain, enabling more meaningful assessment of operational, technical, and economic consequences. While source databases like MCAD and ADMIRAL provide basic information on incident type, year, and affected entity, they often lack the depth required for trend analysis, economic-, forensic insight, or severity assessment. Furthermore, discrepancies in classification and terminology across the two datasets limit the reliability of any cross-comparative study unless harmonised using a consistent set of criteria.

Figure 22 – Maritime Cyberattack Taxonomy visualisation [own research]

The custom taxonomy (Figure 22) introduced in this thesis addresses these challenges by incorporating technical, contextual, and impact-related fields complementing the original datasets. It offers a granular, multidimensional structure suitable for academic analysis and policy evaluation. Specific additions include fields for attacker attribution, origin country, underlying motivation, vulnerability exploited, persistence mechanisms, lateral movement, and techniques used to gain access or maintain presence. These additions improve the explanatory power of each record and allow for richer profiling of threat actors and attack characteristics.

4.2.2 Impact Classification and Response Evaluation

Beyond the technical dimensions of an attack, the taxonomy also captures its consequences through an integrated impact assessment module. This includes indicators of confidentiality, integrity, and availability (CIA), financial damage, reputational harm, environmental impact, cascading effects on supply chains, and risks to human safety. These dimensions are often not quantified in maritime cyberattack databases but are essential for assessing economic cost, strategic severity, and systemic vulnerability. Where available, details were added regarding response measures, such as time to detection, the effectiveness of mitigation efforts, and follow-up policy or regulatory responses. Further additions track whether organisations were found to have violated any cybersecurity regulations or failed to implement preventive measures that could have mitigated the attack.

These additions allow for the identification of gaps in incident response and support a broader understanding of why some incidents escalate while others remain contained. They also offer insights into sector-wide weaknesses and the varying levels of cyber maturity across different maritime domains.

4.2.3 Nature of Attack Classification

Innovation of the taxonomy development is the introduction of classification field titled "*Nature of Attack."* This parameter distinguishes incidents on the degree and type of physical or digital integration involved. It uses five main categories: cyber-only, cyber-physical, cyber-assisted, cyber-enabled, and non-cyber This typology enables nuanced filtering of incidents that do not meet standard cyberattack definitions, without entirely

excluding them from trend analysis. Definitions and representative examples for each category are summarised in Table 2.

Table 2 – Definition of Nature of Attack category

Category	Definition	Example
Cyber-Only	A purely digital incident with no direct physical-world impact	**Phishing, credential theft, website spoofing, ransomware on IT systems.**
Cyber-Physical	A cyberattack disrupting or controlling physical systems or infrastructure.	**GPS jamming of navigation, ransomware on OT controlling engines / cranes / ICS.**
Cyber-Assisted	Cyber activities supporting physical operations, such as deception or concealment.	**AIS spoofing to disguise a vessel's location or cargo manipulation.**
Cyber-Enabled	Cyber tools used to facilitate traditional crimes, not inherently cyber-dependent.	**AIS deactivation to evade tracking or falsified cargo records**
Non-Cyber	Incidents not involving malicious cyber activity.	**Human error, system malfunctions faulty programming,**

4.2.4 Benefits and Validation Insights

During the manual application of this taxonomy to the validated dataset, many entries required reinterpretation or correction. Some were reclassified entirely. For example, incidents originally described as general malware infections were found after inspection to involve ransomware targeting OT environments, thus changing their classification from Cyber-Only to Cyber-Physical. Others, like AIS spoofing and signal jamming, were repositioned from vague digital disruption into more appropriate categories under Cyber-Assisted or Cyber-Enabled, based on technical details and attacker intent.

In some cases, incident descriptions conflated victim and perpetrator roles, particularly in scenarios involving illegal trade or piracy facilitated by cyber means. These ambiguities were resolved through manual validation, supported by publicly available documentation and investigative reports.

The application of the taxonomy not only helped cleanse and reorganise the dataset but also enhanced its analytical potential. It enabled cross-sectional filtering, sectoral profiling, and the identification of underreported threat vectors. Despite remaining limitations in data availability especially for financial and legal outcomes, the structured approach allowed for a more credible and standardised analysis.

4.3 Incident Severity Scoring (ISS) Framework

4.3.1 Purpose and Conceptual Foundation

Taxonomy developed supports systematic classification of incident types and characteristics, but it did not on its own provide a means to compare the overall impact severity of incidents. To address this, a hybrid Incident Severity Score (ISS) model was developed and applied across the validated dataset. The ISS is designed to evaluate the magnitude and complexity of consequences resulting from maritime cyber incidents capturing not just whether an incident occurred, but how disruptive or damaging it was in measurable terms. The ISS, therefore, complements the taxonomy by introducing a structured and repeatable scoring system that is applied across cases with diverse attributes. It allows for prioritising high-severity incidents and aggregating trends across key impact domains. The ISS does not replace qualitative analysis or expert judgement but serves as a tool for standardising impact assessment within the constraints of open-source data.

4.3.2 Scoring Methodology and Structure

The ISS framework comprises ten core parameters, each corresponding to a distinct impact domain. These include: the nature of the victim organisation (e.g., critical infrastructure or private firm), involvement of OT, compromise of sensitive data, operational downtime, financial loss, reputational or legal consequences, cascading impacts on supply chains, environmental effects, risks to human safety, and regulatory or legal action following the incident. The prime aim was to create a method to filter for different impacts. The first score is therefore a simple binary score. The Boolean Impact Score, ranging from 0 to 10, records the number of impact domains triggered in a binary format. This reflects the breadth of the incident, indicating how many different categories were affected regardless of severity within each. To better assess the actual impact of events each incident was scored using another complementary scale. The Weighted ISS Score, which ranges from 0 to 14, assigns differentiated values to each parameter based on its criticality. Parameters such as OT disruption, human safety, and financial loss carry greater weight than, for example, reputational effects or supply chain delays.

This dual-scoring structure allows the model to distinguish between narrowly focused but severe incidents and widespread but moderate-impact ones. For example, a ransomware

attack that causes extensive operational downtime and financial loss, but does not affect safety, data confidentiality, or the environment, may score high on the weighted scale but moderate on the Boolean scale.

Scoring criteria (weighting) were adapted according to existing maritime cybersecurity frameworks and international guidance, including the BIMCO Guidelines on Cyber Security Onboard Ships (2021), IMO Resolution MSC.428(98), and the NIST Cybersecurity Framework. Aligning the model with practical maritime risk considerations and regulatory relevance.

4.3.3 Application and Analytical Use

The ISS was manually applied to each validated incident for which sufficient data was available. Where precise figures were unavailable, conservative estimates were made based on source triangulation and impact indicators. For example, if a port system was reported to have suffered a prolonged shutdown without further details, a minimum score was assigned for operational downtime, while financial or safety-related scores were left at zero unless additional evidence supported inclusion. This way the ISS enabled the identification of high-impact incidents that involved multiple critical dimensions of harm. These included attacks on navigation systems resulting in loss of control at sea, ransomware incidents that halted port operations, and cyber-assisted cases where digital tools facilitated physical hijacking or fuel theft. Pattern emerging from this scoring exercise are presented in Section 4.4.8 and Table 6.

This framework also enabled comparative evaluation across attack types. For instance, most Cyber-Only incidents scored lower on the ISS than Cyber-Physical or Cyber-Assisted events, reflecting the more tangible and measurable consequences of the latter. However, this scoring asymmetry may inadvertently mirror sectoral biases, where incidents without physical manifestations are perceived as less critical or urgent. Many Cyber-Only events (e.g., credential theft or persistent phishing campaigns, intrusions seemingly without consequences) serve as entry points to more disruptive operations or erode trust in digital infrastructure over time. The tendency to underestimate such risks in favour of more immediate, physical threats may lead to underinvestment in cybersecurity. Turning collected data into measurable indicators, such as those used in the ISS, can help build a more balanced risk assessment model that considers both direct and hidden consequences of cyber incidents. At the centre of this approach is the value

and utility of data: meaningful, structured information is essential to measure, control, and monitor whether an organisation, the sector, or processes are moving in the right direction. This concept is important in understanding risk perception, decision-making shaping policy frameworks.

4.3.4 Limitations and Considerations

While the ISS model offers a structured approach to incident impact assessment, it is subject to limitations. Chief among these is data availability. Many incidents lack sufficient technical detail, verified financial loss estimates, or precise descriptions of operational consequences. As a result, several ISS scores may underestimate true impact. Additionally, scoring involves a degree of subjectivity, particularly in interpreting ambiguous reports or deciding whether a given parameter was affected. Although criteria were formalised to the extent possible and cross-validated, inconsistencies are inevitable given the reliance on open-source and anecdotal data.

The ISS model is not intended to function as a universal benchmark or definitive severity index. Rather, it offers as an experimental prototype, designed to facilitate exploratory analysis and stimulate discussion about how impact should be measured in maritime cybersecurity. Future iterations may refine the model using machine-readable formats, probabilistic weighting, or industry-specific modifiers.

4.4 Quantitative Analysis of the Merged Dataset

This section presents the analytical results derived from examining 146 maritime cyber incidents (data subset) that were manually cleaned, verified, and structured using the custom taxonomy introduced in Section 4.2. Each incident was reassessed for consistency, enriched with contextual detail where possible, and scored using the hybrid ISS framework introduced in Section 4.3. Table 3 presents the characteristics of the data subset, not including non-cyber incidents.

Although the dataset enables exploration of trends across attack types, sectors, vectors, attribution, and impact severity, it does not support reliable macroeconomic modelling. This limitation stems not from a lack of technical detail, but from the incomplete and inconsistently reported nature of incident data. Particularly the true number of attacks and their geographic attribution is unreliable, and too few to make reliable calculations or

estimations. Many cyber incidents remain undisclosed or are reported only in aggregated form. There are several entries in the source databases aggregate dozens or hundreds of incidents over a longer span of time, making it impossible to establish a comprehensive, location-specific picture of maritime cyberattacks. High-impact incidents are disproportionately represented due to media visibility or political sensitivity, while lower-profile or less severe events often go unreported. In 2023, over 17 million cybercrime incidents were reported globally [74], yet only a few hundred maritime-specific cases have been documented with the necessary granularity for analysis. This disparity reflects the persistent underreporting and fragmented visibility, that is the core challenge highlighted in RQ2 regarding the feasibility of quantifying economic impact on a macro scale.

Table 3 – General characteristics of the data subset (2001 – 2020)

Metric	Value	%
Total incidents in sub-dataset	146	100 %
Incidents present in both sources	63	43 %
Cyber-only attacks	110	77 %
Cyber-physical attacks	16	~11%
Cyber Enabled or Assisted attacks	14	~10 %
Identifiable adversary	73	50%
Possible financial implications	91	~63%
Information on financial impact	28	~ 20%
Estimate of the financial losses	10	~7%
operational downtime	64	46%
possible cascading impacts	85	min 57%
potential or elevated risk to human safety	44	30%
actual harm to human safety	5	~3%

4.4.1 Nature of Attacks

Among the 146 verified incidents, the majority (~ 77%) are classified Cyber-Only. These involve purely digital disruptions such as phishing, ransomware, malware propagation, or credential theft targeting IT systems. While lacking direct physical consequences, these incidents frequently resulted in operational interruptions, reputational damage, or

financial loss. Cyber-Physical incidents accounted for approximately 11% of the dataset. These attacks directly impacted OT systems, including vessel navigation tools, engine control mechanisms, or industrial systems within ports. A clear example is the 2017 cyberattack on a German-owned 8,250 TEU container ship, which lost steering control for nearly ten hours due to compromised navigation systems. Although no collision occurred, the vessel drifted without manoeuvrability until external IT specialists boarded to restore control. Despite the absence of material damage, the attack had direct operational and safety consequences, qualifying it as a Cyber-Physical event under the classification model used in this study. The remaining ~10% comprised Cyber-Assisted or Cyber-Enabled incidents, where digital tools were used to facilitate illicit physical operations or enhance the effectiveness of conventional crimes. One illustrative case involved a 2010–2011 breach in a Greek shipping company's shore-based Wi-Fi. Hackers gained accessed to real-time vessel schedules and relayed them to pirate groups, resulting in targeted attacks at sea. While the hackers did not carry out physical violence, their actions directly enabled it, placing the incident in the Cyber-Assisted category.

This reveals, that the maritime cyber threat landscape is still dominated by conventional digital attacks yet increasingly punctuated by hybrid incidents that blur the boundary between cyber and physical consequences. As operational systems become more interconnected with digital platforms, attacks that originate in cyberspace are increasingly capable of producing tangible physical effects either directly or by enabling real-world events. The implications of this shift are explored further through severity scoring in Section 4.4.8.

4.4.2 Attack Methods and Vectors

Analysis of the recorded attack methods in the validated data subset reveals a clear dominance of malware-based attacks across the sector. Out of 146 confirmed incidents, 33 involved general malware infections and an additional 32 attributed to specifically ransomware campaigns. These figures underscore the prevalence of disruptive and financially motivated attacks, particularly those aimed at disabling business operations, encrypting data, or forcing downtime on port and shipping systems. Unauthorised system access was recorded in 24 incidents and ranked third overall. Though this rises and important analytical interpretation, as malware deployment typically presupposes that an unauthorised access has already happened. This phenomenon is likely attributable to

reporting conventions: in many records, malware is highlighted as the main impact or outcome, while the access vector enabling it is omitted or inferred only indirectly. However, unauthorised access, without confirmed deployment of malware, often involving compromised credentials, brute-force logins, or exploitation of week authentication mechanisms, are also behind data breaches and espionage-style campaigns as well.

Other identified methods include GPS and GNSS interference (19 cases), as well as AIS manipulation (14 cases), involving spoofing or deactivation of vessel location signals. These attacks targeted maritime navigation systems with the intent to mislead surveillance, obscure vessel identity, or disrupt routing—posing significant risks to operational safety. Less frequently documented were data breaches and espionage-style campaigns (7 incidents), DDoS attacks, and business email compromise (BEC), which reflect either commercial targeting or more covert attempts to extract sensitive operational information. At the tail end of the distribution were incidents involving SQL injection, insider manipulation, and blackmail or sextortion—some of which occurred outside traditional vessel infrastructure but nonetheless affected maritime entities. Figure 23 illustrates the full distribution of recorded attack methods between 2001 and 2020.

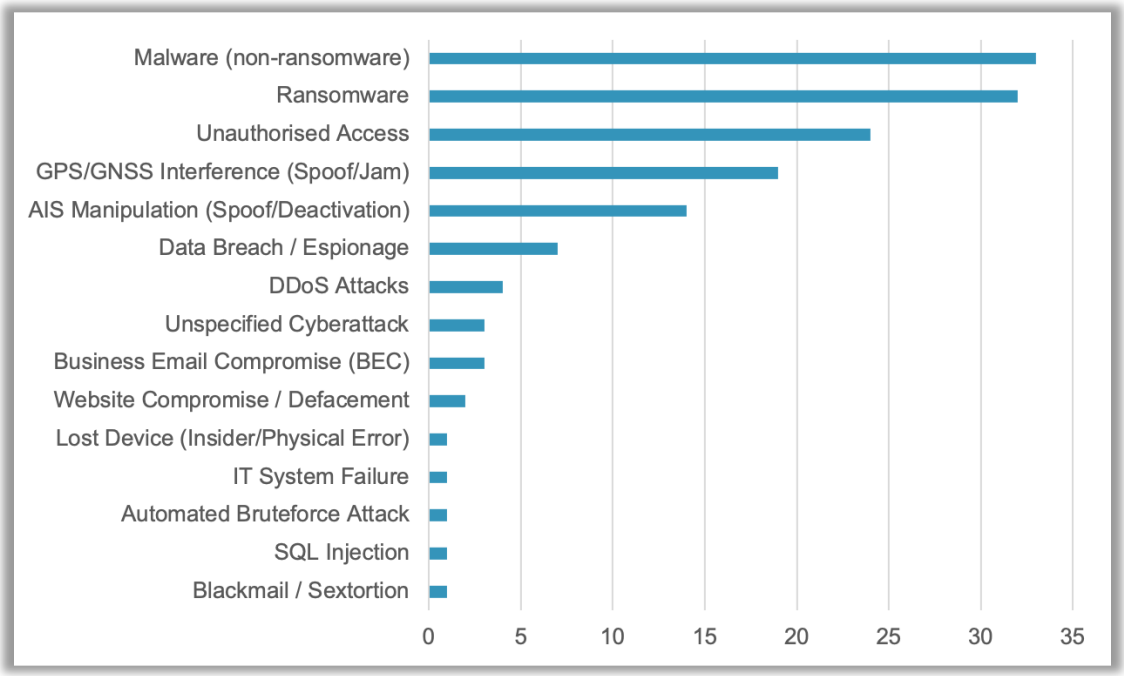


Figure 23 – Distribution of Attack Methods in data subset (2001- 2020)

While attack methods describe what was done, attack vectors refer to the initial entry point through which adversaries gained access to target systems. These vectors are less consistently documented in existing maritime cyber incident databases and often had to be inferred through supplementary sources such as reports or investigative journalism. Nevertheless, they are analytically valuable in identifying sectoral weaknesses and preventative priorities.

As shown in Figure 24, the most frequently reported vector was "general unauthorised access," which applied to 24 cases and typically lacked further detail. Phishing and social engineering are highly prominent, appearing in 19 confirmed cases and increasing to 27 when spear-phishing is included. These incidents targeted maritime personnel, often through deceptive emails or messages designed to induce credential compromise, malicious link activation, or fraudulent financial activity.

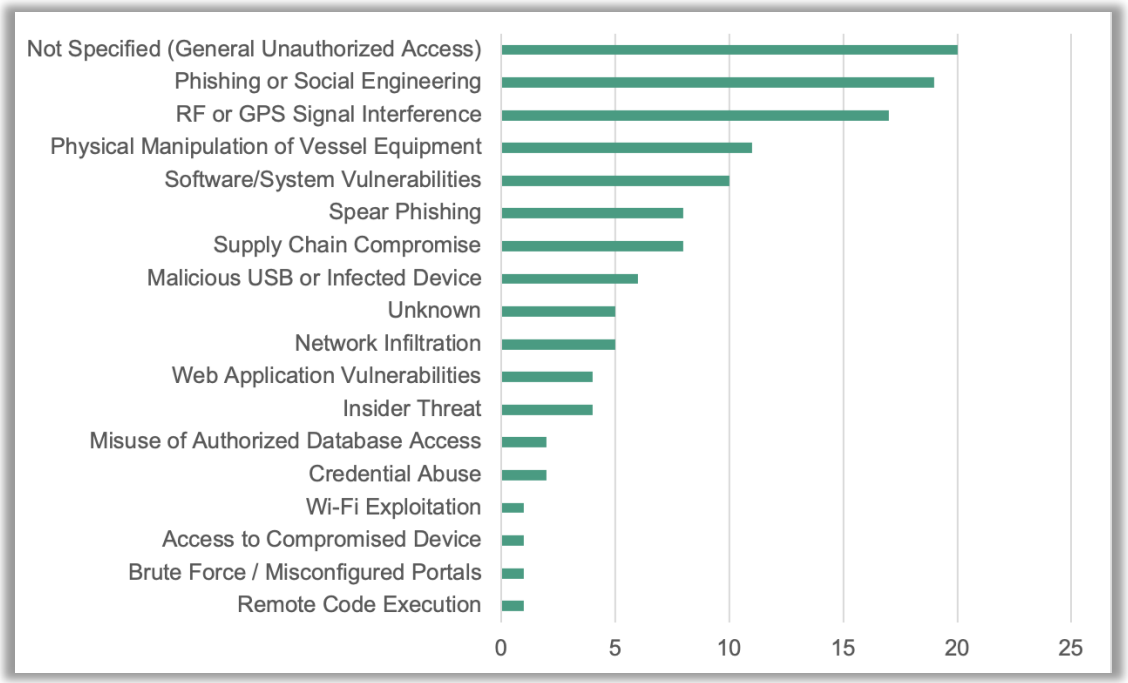


Figure 24 – Distribution of Attack Vectors in data subset (2001- 2020)

RF or GPS signal interference was documented in 17 cases, revealing how attackers exploit navigation technologies as entry points or manipulation surfaces. Physical manipulation of vessel systems, including USB-based compromise and unauthorised access to onboard terminals was found in 11 cases, reflecting maritime-specific risks associated with isolated and under-supervised control environments. Software or system vulnerabilities accounted for 10 incidents, and supply chain compromise was identified

in eight, highlighting the importance of third-party risk management in interconnected maritime IT environments. Less frequent vectors included infected removable media (6 cases), network infiltration (5), web application vulnerabilities (4), and insider threats (4), the latter of which often involved former employees or poorly monitored internal systems. Credential abuse, brute-force attempts, remote code execution, and misuse of database access were also recorded in low numbers but nonetheless indicate the broad range of access methods employed.

Five incidents in the dataset had no identifiable entry vector, while an additional twenty were described only in general terms as involving "unauthorised access," without technical clarification. This limited attribution reflects a broader gap in cyber incident reporting. While attack methods are often disclosed, the attack vector is far less frequently made public. Media reports and even formal statements tend to focus on the outcome of an incident rather than on how access was gained. This omission is not accidental. The details surrounding how an attacker penetrated a system often involve sensitive organisational practices, such as weak password management, unpatched vulnerabilities, or successful phishing attempts. Disclosing these mechanisms could expose operational weaknesses or invite further targeting. Consequently, such information is typically restricted to internal reports produced by digital forensics or incident response teams and is rarely included in open-source datasets.

This limitation is due to the boundaries of OSINT in mapping the full anatomy of maritime cyberattacks. While it is often possible to identify how disruption occurred, the lack of publicly available information on attack vectors makes it harder to develop tailored and sector-specific defences. Although, beyond the scope of this chapter, the findings suggest that introducing secure and, where necessary, anonymised incident-sharing mechanisms could help improve the accuracy of cyber incident reporting and analysis and hence support more actionable risk assessments.

The dual analysis of methods and vectors taken together highlights the complex, layered nature of maritime cyber threats. Attackers frequently rely on low-cost, high-yield IT-based methods such as phishing or ransomware, while more sophisticated actors exploit sector-specific weaknesses in navigation systems, physical infrastructure, or logistics platforms. As the maritime industry continues to digitise and integrate with global trade networks, these patterns project the importance of implementing layered defences,

conducting regular employee awareness training, and securing both shore-side and shipboard systems against a wide spectrum of attack techniques

4.4.3 Temporal Trends

The temporal distribution of validated incidents between 2001 and 2020 reveals a steady increase in reported maritime cyberattacks, particularly after 2010. In the early 2000s, only a handful of incidents were recorded annually, reflecting either low threat activity or, more likely, the absence of systematic detection and reporting mechanisms. From 2010 onwards, a gradual rise is observable, with a marked escalation in the frequency of incidents between 2017 and 2020 (see Figure 25).

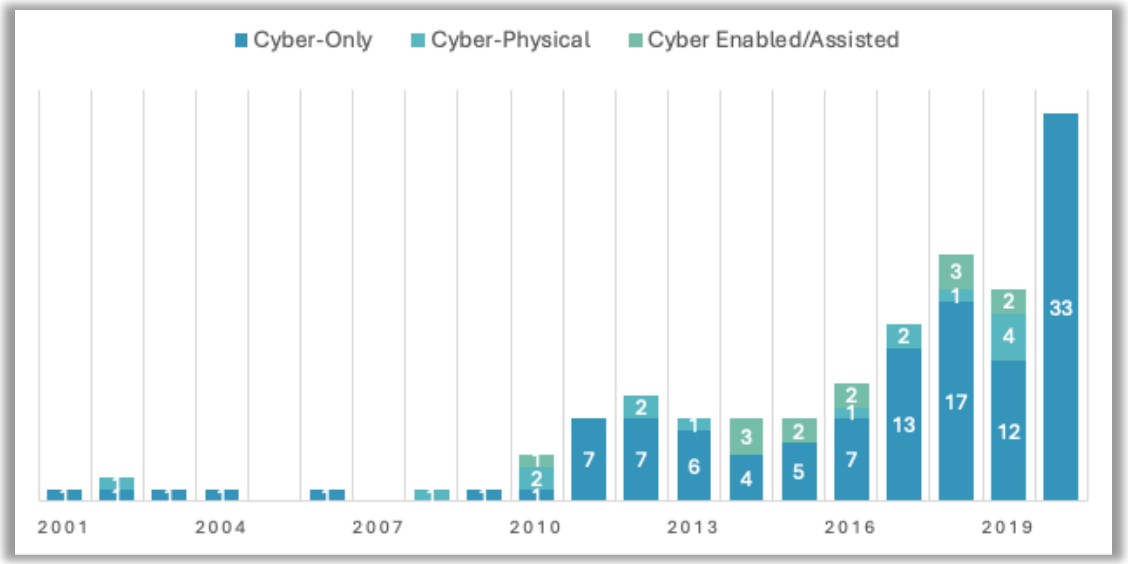


Figure 25 – Distribution of cyberattacks over time and Nature of Attack (2001-2020)

This increase likely reflects a combination of factors. First, the maritime sector has undergone significant digital transformation in the past decade, integrating OT, industrial control systems, and connected logistics infrastructure, thus expanding the attack surface. Second, awareness of cybersecurity risks has improved, and so has the willingness and the obligation of organisations to report incidents. Third, the rise may also be attributed to the growing capabilities of cybercriminals and state-affiliated actors to exploit maritime-specific vulnerabilities. This observed growth in incident frequency cannot be interpreted as a complete or exhaustive record of cyber activity within the maritime domain. As discussed earlier, the dataset used for this analysis is drawn from publicly reported or open-source verified incidents. Many cyberattacks, particularly those

involving espionage, commercial theft, or reputational risks remain unreported or are disclosed only in vague terms.

A notable trend within this timeline is the increasing share of hybrid incidents, especially Cyber-Physical and Cyber-Assisted attacks, among the most impactful cases in the latter half of the period. Within the thirty highest-severity incidents (as measured by the ISS model), these hybrid attacks were disproportionately represented. This suggests that the maritime sector is not only facing more frequent attacks but also more complex and operationally disruptive ones. The convergence between digital and physical threat domains appears to be sharpening, as attackers exploit OT systems, navigational tools, and embedded vessel technologies to extend the reach of their operations. These patterns align with the broader evolution of the cyber threat landscape, in which attackers move beyond IT environments to exploit physical processes and operational dependencies. For maritime organisations, this implies that cybersecurity must be addressed not just as an IT governance issue but as a core component of safety, continuity, and strategic risk management.

4.4.4 Adversary Attribution

Adversary attribution remains a significant challenge in maritime cyber incident reporting. However, partial attribution was possible in approximately 110 of the 146 validated cases, based either on direct reporting or pattern-based inference (Figure 26). Among these, state-sponsored actors were the most frequently identified, responsible for 45 incidents. These operations often exhibited high levels of sophistication and were directed at critical maritime infrastructure, suggesting strategic intent aligned with national interests. Among the cases with some level of attribution, state-sponsored actors were the most frequently identified group, linked to 45 incidents. These operations often targeted critical maritime infrastructure, such as ports, shipping logistics, offshore platforms, or naval defence systems, and were typically characterised by a high degree of technical sophistication and strategic intent. Examples include GPS interference, malware implants in OT systems, or ransomware attacks suspected to mask data exfiltration. Eleven incidents (10%), the attackers were described as state-affiliated actors. These are groups with suspected indirect links to government entities or acting with tacit approval. This attribution category reflects the growing use of cyber operations in grey-zone

conflict, where plausible deniability is maintained by outsourcing disruptive actions to patriotic hackers, contracted teams, or intelligence proxies.

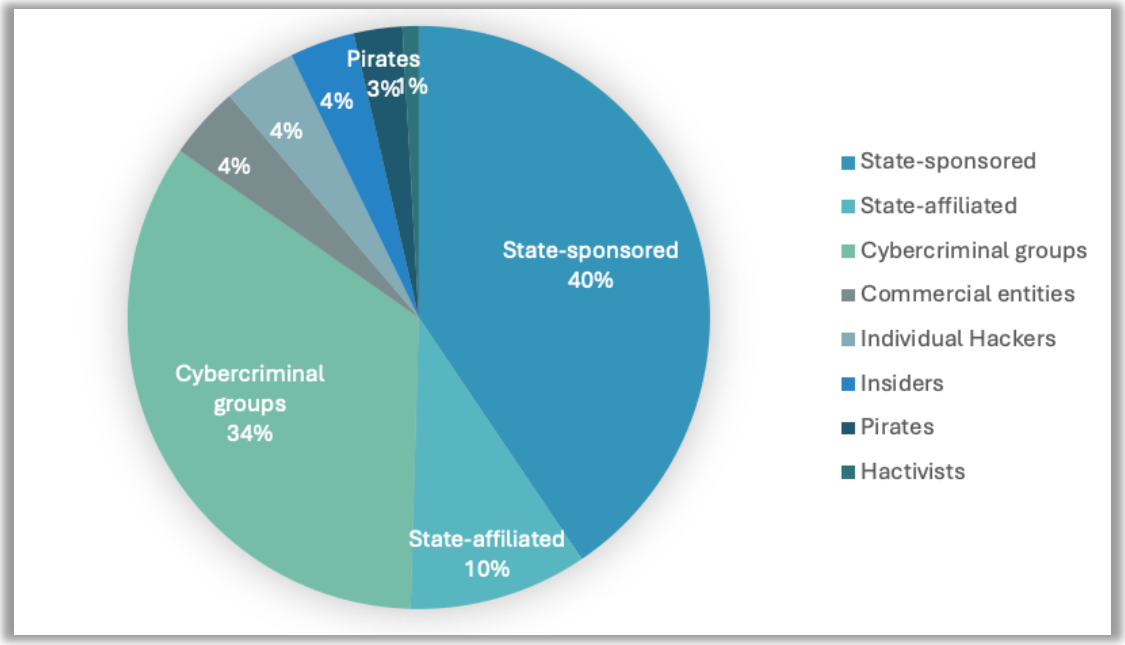


Figure 26 – Threat actor types identified in data subset (2001- 2020)

38 incidents could be attributed to cybercriminal groups, reflecting their continued targeting of financially valuable maritime operations. These actors typically deployed ransomware, launched phishing campaigns, or conducted fraud against port authorities, shipping companies, or associated logistics operators. While financially motivated, the disruption caused by these attacks often extended beyond economic loss, affecting supply chains and operational continuity.

Other attribution categories, including commercial insiders, individual hackers, pirate groups, and hacktivists, were identified in far fewer cases, each accounting for three to four incidents. Hacktivist activity was particularly rare in the maritime dataset, with only one recorded case, suggesting that ideological or protest-driven attacks are not a prominent feature in this sector. In several cases, attribution to a specific threat actor group was not possible, but the origin country of the operation could still be identified based on technical forensics, infrastructure links, or geopolitical context. Country-level attribution was possible in 68 incidents (Figure 27), although confidence levels varied depending on the sources.

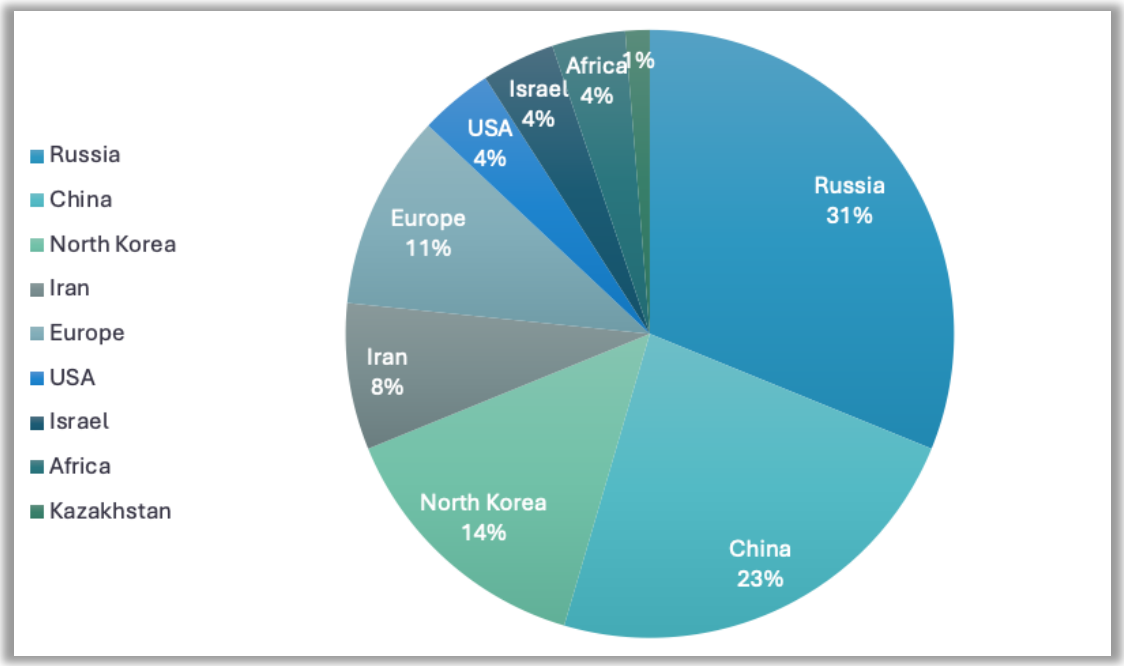


Figure 27 – County level attribution of incidents identified in data subset (2001-2020)

Among these, Russia was the most frequently cited origin, linked to 24 incidents (31%), China followed by 18 (23%) and North Korea with 11 (14%). These three countries accounted for over two-thirds of all country-attributed incidents and are consistent of with global patterns of cyber operations directed against critical infrastructure sectors. Other implicated countries included Iran (8 incidents), European states (6), and the United States and Israel (3 each). A small number of cases referenced suspected actors in West Africa, Morocco, or Kazakhstan, reflecting either regional piracy-facilitated cyber operations or localised fraud campaigns.

An additional 43 incidents were classified as involving unknown actors, while in 22 cases the attribution was "not specified," highlighting the continued opacity surrounding attribution. These findings reinforce the maritime domain's exposure to both strategic and profit-driven cyber threats, frequently emanating from jurisdictions with limited regulatory oversight or geopolitical tensions' reflection on global maritime domain.

4.4.5 Sectoral and Operational Impact

The sectoral distribution of maritime cyberattacks within the validated data subset indicates that a limited number of industry domains have experienced a higher concentration of incidents. As shown in Figure 28, the port and terminal operations sector was the most frequently affected, with 30 recorded incidents. These attacks often targeted

port IT systems, cargo handling platforms, crane operations, and booking systems, resulting in significant disruption to shipping schedules and global supply chains. The operational consequences ranged from temporary disruptions and delays to large-scale logistical breakdowns. Maritime logistics and shipping companies were also heavily affected, reflecting the growing digital integration of fleet management systems and enterprise IT platforms. Naval defence operations and contractors accounted for 20 incidents, many of which involved state-linked adversaries targeting military maritime assets or affiliated contractors. Although fewer in number, these incidents tended to be more severe and often involved exploitation of OT systems or sustained surveillance campaigns.

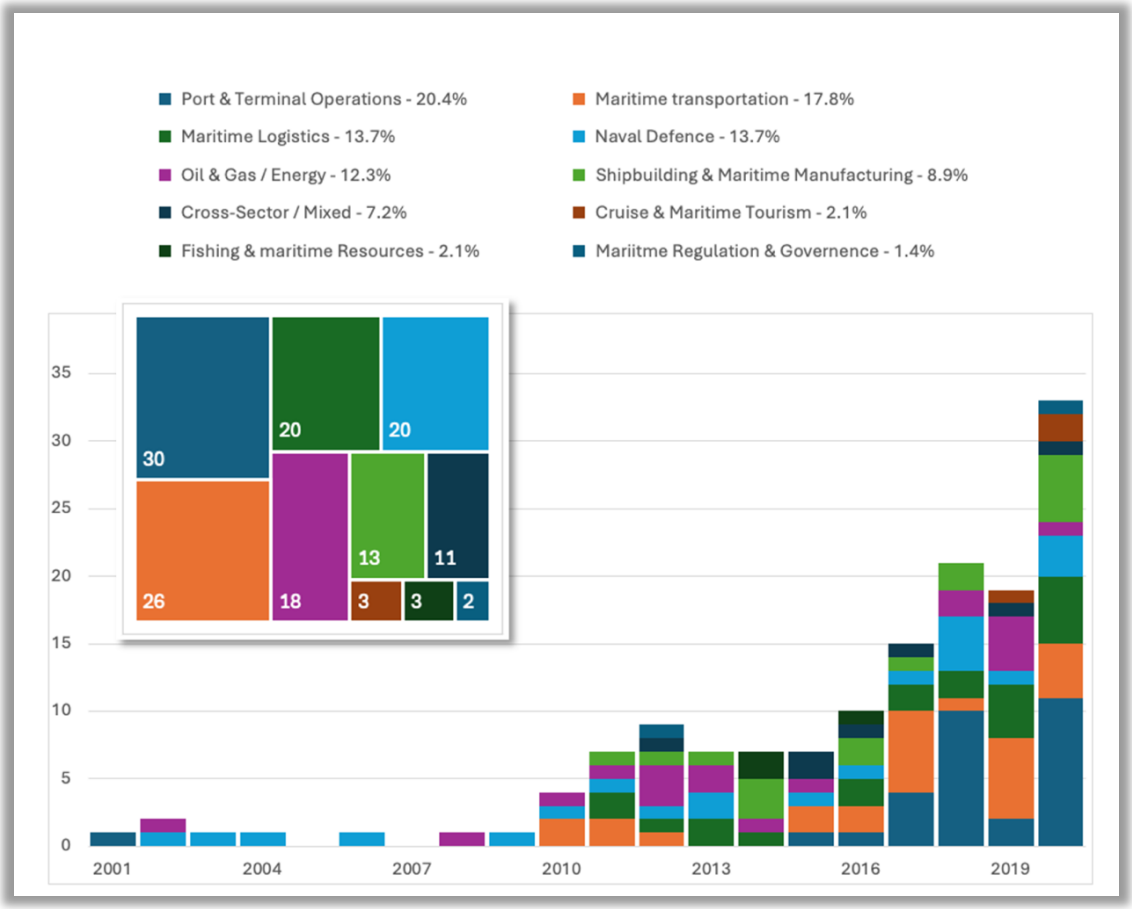


Figure 28 – Sectoral distribution of maritime cyberattacks (2001-2020)

Other affected sector includes oil and gas infrastructure, including offshore platforms and energy transport vessels (18 attacks), shipbuilding (13 incidents), cruise operations (3), and fishing industry (3). While the low number of incidents in the latter categories may reflect underreporting, especially given reputational sensitivities, it also suggests that

large-scale commercial shipping and port-facing logistics remain the primary targets due to their visibility, interconnectivity, and economic significance. Eleven cases could not be cleanly assigned to single sector, proved overlapping or ambiguous, particularly in incidents that affected multiple parties across a supply chain or ecosystem.

In parallel to sectoral classification, the taxonomy also provides a four-part typology to describe operational distribution of each incident. This classification helps distinguish not only where cyberattacks occurred but its operational context (Table 4). Applying this categorisation to the data subset, 105 of the 146 validated incidents were classified as shore-based, confirming that land-based maritime systems, such as port networks, shipping company headquarters, or logistics platforms remain the most frequently targeted environments. These systems are often exposed through enterprise software, web-based access points, and third-party integrations. Offshore incidents, where vessels were actively sailing at the time of the attack, accounted for 25 cases. These included GPS spoofing during navigation, unauthorised access to shipboard networks, and ransomware or malware infections affecting onboard control systems.

Table 4 – Operational distribution categories

Category	Definition	Example
Shore-Based	Cyber incidents affecting land-based maritime infrastructure.	**Attacks on container terminals, logistics hubs, and port IT systems (e.g., JNPCT ransomware attack).**
Offshore	Cyberattacks on vessels while actively sailing in open waters.	**GPS spoofing of tankers in the Persian Gulf**
Port-Based	Incidents affecting vessels while docked in ports or inside territorial waters.	**Ferries experiencing GPS jamming while at dock (Bornholmslinjen GPS jamming incident).**
At-Sea	Incidents affecting maritime navigation and tracking systems on vessels in open waters, with no land-based infrastructure directly involved.	**AIS spoofing of Russian tankers, GNSS jamming in the Black Sea.**

Twelve cases were categorised as at-sea, meaning they specifically affected tracking or navigation systems in open waters, without direct involvement of shore-based infrastructure. These attacks primarily relied on signal interference, such as GNSS jamming or AIS spoofing, and were often difficult to trace or verify in real time. Port-based incidents, attacks affecting vessels docked at ports were observed in only two cases, though it is possible that underreporting obscures a higher actual number. In two further

cases, the operational environment could not be conclusively determined due to limited available information.

4.4.6 Safety and Operational Disruption

Beyond economic losses and data compromise, many maritime cyber incidents in the dataset resulted in operational disturbances and, in a smaller number of cases, direct safety risks to crew, cargo, or infrastructure. These impacts were assessed through structured fields in the taxonomy and further quantified using the ISS framework introduced in Section 4.3.

Approximately 46% of the validated incidents (67 cases) in the data subset indicated some form of operational downtime, ranging from minor service interruptions to prolonged shutdowns of port infrastructure or shipboard systems. These disruptions affected a range of functions, including cargo processing, terminal operations, and navigational scheduling. In several cases, logistical bottlenecks cascaded across regional port clusters, highlighting the critical dependency of maritime trade on uninterrupted digital infrastructure. In parallel, 30% of incidents included references to elevated risk to human safety, typically involving the loss of navigational accuracy, communication failures, or compromised OT systems. Examples included GPS jamming, AIS spoofing, or interference with propulsion and steering mechanisms. While such incidents did not always result in visible accidents, they placed crews and vessels in precarious situations, particularly in congested waters, during adverse weather conditions, or in geopolitically sensitive zones.

Actual physical harm, confirmed injuries, was documented in approximately 3% of cases. Although relatively rare in the current dataset, these cases demonstrate that cyber involved incidents have the potential to produce tangible physical consequences. Furthermore, due to underreporting and limited disclosure of near-miss scenarios, the true extent of such outcomes may be underrepresented in open-source data. The recurring presence of safety-related indicators, even in the absence of confirmed physical damage, points to a growing concern across the maritime domain. As digitalisation advances, threats once confined to office IT systems are increasingly capable of reaching core vessel operations and automated terminal environments. These findings reaffirm the need to treat cybersecurity not merely as a matter of compliance or data protection, but as a key component of maritime safety and operational resilience.

4.4.7 Financial Dimensions

Financial implications were mentioned in at least 63% of recorded incidents; however, precise loss estimates were disclosed in only approximately 7% of records. An estimated 20% of incidents provided partial or vague financial impact references, such as “millions in damages” or “significant loss of revenue.” The limited granularity and inconsistency of financial reporting, combined with the lack of standardised loss assessment methodologies, make it difficult to aggregate meaningful cost figures. In many instances, organisations refrained from publishing damage estimates, either to protect their reputation, comply with insurance or legal advice, or due to the difficulty of isolating direct costs from secondary losses. Even when financial data is disclosed, it often reflects preliminary estimates that do not account for long-term reputational damage, supply chain interruption, or future risk mitigation spending.

Among the few cases where confirmed financial figures were publicly released, losses varied significantly in scale. The most severe case in the dataset was the 2017 NotPetya attack on Maersk, with damages estimated at $300 million, including costs related to terminal outages, system restoration, and delayed cargo movement. Similarly, the CMA CGM ransomware attack in 2020 was reported to have caused tens of millions of dollars in disruption-related expenses. Other notable examples included ransomware attacks that led to ransom payments, port shutdowns, or extended downtime, although the precise cost of these incidents often remains undisclosed. Table 5 presents incidents within the data subset that included confirmed financial loss data. However, it is important to note that the majority of economic consequences in maritime cyberattacks likely remain underreported or underestimated, particularly in cases where costs are absorbed internally or spread across insurance mechanisms.

While Table 5 includes only cases with clearly reported financial figures, several high-impact incidents were excluded due to the absence of verifiable estimates, despite evidently involving significant economic consequences. For example, the 2013 grounding of the USS Guardian (MCM-5) (ADMIRAL database: 2013_003) [75], led to the total loss of the U.S. Navy minesweeper and a $1.97 million environmental compensation payment to the Philippines for damage to the Tubbataha Reef. Although the event was not formally confirmed as a cyberattack, it stemmed from a compromised

Electronic Nautical Chart (ENC), highlighting how digital system failure, whether malicious or accidental can lead to substantial material and financial repercussions.

Table 5 – Maritime cyberattacks with financial estimates (2001 – 2020)

	Incident	Year	Region	Estimated losses	Notes
1	Veneyuela Oli Facility Cyber Sabotage	2002	South America	**$ Billions**	Estimated millions due to halted production and damaged systems, Billions in lost revenue
2	NotPetya on Maersk	2017	Europe / Global	**~ $300 million**	Operational disruption and full IT rebuild
3	CMA CGM Ransomware Attack by Ragnar Locker	2020	Europe	**< $50 million**	Operational disruption
4	Business Email Compromise (BEC) and Fraudent Bunker Fuel Transaction Targeting WFS	2014	North America	**$18 million lost**	fraudulent transaction, + costs for legal proceedings
5	Vessel 'MT Kerala' Hijacking and Cyber-Assisted Fuel Theft	2014	West Africa, Europe	**$10 million**	stolen oil + operational costs + security enhancements post-event
6	Business Email Compromise (BEC) attack on Nautilus Minerals	2014	North America	**$10 million**	due to fraudulent transaction
7	London Offshore Consultants (LOC) Ransomware Attack	2019	Europe	**$6.1 million**	ransom demand Additional financial losses from downtime and data recovery efforts
8	Gold Galleon Maritime BEC Attacks	2017	Global	**$3.9 million**	Attempted theft of at least; actual losses may differ
9	Business Email Compromise - Shipping company in Limassol	2015	Europe	**$644,000**	Legitimate invoice, false bank account
10	Ex-Navy Couple Sold Data of Over 9,000 People on Dark Web	2018	North America	**$160,000**	illicitly earned from data sale - Potential financial loss for victims due to identity theft
11	Clarksons PLC (Shipbroker) Data Breach and Ransom Demand	2017	Europe	**5% decrease**	in stock value following the incident

Other omitted examples include ransomware attacks or regulatory penalties for cybersecurity failings, where figures were reported only partially. These include the CAN Financial ransomware incident (March 2021), reportedly involving a $40 million ransom payment [76], among the largest known in the sector, and the $6.25 million fine imposed on Carnival Corporation for cybersecurity deficiencies [77]. While not maritime-

exclusive, such cases reflect the broader trend of underreported or underestimated losses in digital maritime ecosystems. These examples suggest that the true scope of cyber-related financial consequences is likely much larger than what is documented in existing maritime databases. This limitation, compounded by selective disclosure, reputational risk concerns, and fragmented reporting.

4.4.8 Severity Score Patterns

The application of the Incident Severity Score (ISS) to the validated data subset enabled a structured, comparative analysis of impact severity across maritime cyber incidents. Each entry was evaluated using the dual-scoring model outlined in Section 4.3, comprising a Boolean Score that reflects the number of affected impact domains, and a Weighted Score that adjusts for the relative criticality of each domain. This approach allowed for the identification of both high-intensity incidents with narrow focus and broader, multi-dimensional events with systemic consequences.

Across the dataset, most incidents clustered within the moderate severity range. The median Boolean Score was 4.5, while the median Weighted Score stood at 4.3, suggesting that although many incidents affected multiple dimensions, their critical impact was often contained (or concealed). Lower-severity events typically involved phishing, credential compromise, or malware targeting administrative IT systems, cases that disrupted digital operations but did not extend into safety-critical or financial domains.

Aa small number of high-scoring outliers (reaching scores of 9 or 11) demonstrate that serious, high-impact cyberattacks, though less frequent, do occur. Overall, this distribution reflects a sector experiencing regular operational disruption and risk (as shown in Table 6 and Appendix III presents the 30 most severe incidents recorded between 2001 and 2020). Among the highest scoring events the majority were classified as Cyber-Physical or Cyber-Assisted. Their high ISS values were driven by the convergence of physical and digital disruption, elevated safety risk, and cross-sectoral or international consequences. Several analytical patterns emerged from this scoring process. First, incidents targeting OT environments were consistently associated with higher severity, both in terms of technical complexity and human or economic impact. Second, attacks involving supply chain effects or sectoral interdependencies tended to register elevated ISS values due to the multiplicity of affected actors and systems. Third, although Cyber-Only attacks comprised the majority of all incidents by count, they

accounted for only a minority of the highest-severity cases. This aligns with the expectation that disruptions limited to IT environments are generally easier to contain and recover from, particularly when core logistics operations are unaffected.

To address the incomplete or inconclusive nature of many open-source incident reports, a conservative scoring method was applied. Where an impact domain was plausibly affected but not explicitly confirmed, a minimal score was assigned: 0.5 on the Weighted scale or 1 on the Boolean scale. This allowed inclusion of ambiguous but significant incidents while maintaining methodological consistency. However, this conservative approach may have underestimated the true impact of some events, particularly where safety concerns or reputational effects were hinted at but not detailed in public documentation.

Table 6 – Top 10 highest-scoring incidents by ISS

Incident	Year	Nature of Attack	ISS (b/w)	Notes
MT Kerala Hijacking	2014	Cyber-Assisted	**8/11**	$10 million fuel stolen, crew harmed
Stena Impero Seizure	2019	Cyber-Physical	**8/11**	British tanker seized, 19 crew held
Venezuela Oil Sabotage	2002	Cyber-Physical	**9/10.5**	Production halted, economic damage
NotPetya on Maersk	2017	Cyber-only	**7/9**	~$300M loss, 45K PCs affected
Pacific Energy SCADA Tampering	2008	Cyber-Physical	**7/8.5**	Leak detection disabled, shutdown
Iranian Offshore Platforms	2012	Cyber-Physical	**7/8.5**	Disruption via malware
Drilling Rig Malware	2010	Cyber-Physical	**7/8.5**	19-day downtime
Illicit Transfer - East China Sea	2018	Cyber-Assisted	**9/8**	AIS dark activity, illegal cargo
Illicit Transfer - Ningbo/Nampo	2019	Cyber-Enabled	**9/8**	Coordinated AIS blackout
Shamoon on Aramco	2012	Cyber-only	**6/8**	30,000 PCs wiped, oil halted

The ISS incorporates modifiers to reflect the relative importance of the victim entity, assigning higher weights to incidents involving critical infrastructure, large-scale logistics hubs, or nationally significant assets. A further extension was introduced to represent spillover effects, measuring the degree to which an incident's impact propagated across multiple operational, geographic, or sectoral vectors. These additional layers enhanced

the granularity of the scoring process and supported a more context-sensitive evaluation of severity. ISS values have to be interpreted as composite indicators rather than absolute measures. No single domain, whether downtime, economic loss, or safety risk can independently define the full severity of a cyber incident. A temporary disruption to a back-office IT service may score similarly to a short-term OT interruption on paper, but their operational consequences differ considerably depending on system function and strategic importance. The weighted ISS structure allows such distinctions to be accounted for, offering a more robust estimate of relative impact across the dataset.

While the current model remains exploratory, its analytical utility is evident. The ISS facilitated trend identification, highlighted the disproportionate consequences of Cyber-Physical and Cyber-Assisted incidents, and enabled preliminary comparisons that could be replicated in other critical infrastructure sectors. Future development of the model (i.e., through probabilistic scaling, machine-readable scoring templates, or cross-sector benchmarking) could strengthen its function as a sector-wide impact estimation tool. Nonetheless, its effectiveness will remain tied to the continued improvement of incident reporting practices, transparency mechanisms, and data-sharing protocols in the maritime domain.

4.4.9 Structural Data Challenges and Verification Issues

Despite the use of the structured taxonomy and incident scoring framework, key data limitations persist. A substantial number of publicly reported maritime cyber incidents lack precise financial details, technical descriptions, or regulatory outcomes. In some cases, entries were found to contain attribution errors or misidentified victims. For example, MCAD case 20221141 mistakenly listed "Sarmin Services Ltd" in the UK, whereas the actual target was Samrin Services Pvt Ltd, a non-maritime company based in India. Similarly, case 20200905 conflated two distinct firms (Metapack Ltd. and Overseas Express Shipping Company) creating ambiguity over the true victim of a ransomware incident. Some cases can be traced to imported typos that has caused misidentification.

These discrepancies necessitate rigorous verification and highlight the risks of drawing conclusions from unvalidated data, even within widely cited sources. While the taxonomy applied in this study enables improved classification and filtering, the quality and granularity of available data remain uneven. As a result, some impact assessments may

understate the true consequences of cyber incidents, and comparative analysis remains constrained by reporting opacity.

4.4.10 Conclusion to the Quantitative Analysis

The structured analysis of 146 validated maritime cyber incidents between 2001 and 2020 demonstrates that while the majority of recorded events were classified as Cyber-Only, the most severe consequences were predominantly linked to Cyber-Physical and Cyber-Assisted operations. These high-impact incidents often involved OT, posed direct safety risks, or caused cascading disruptions across supply chains, factors that significantly elevated their severity scores.

Recurring attack vectors included phishing, unauthorised access, and RF-based manipulation of navigation systems, while the most frequently targeted sectors were port operations, maritime logistics, and offshore energy infrastructure. Attribution data points to both financially motivated cybercriminals and state-sponsored actors, with notable geographic patterns concentrated in Russia, China, and North Korea. Despite these insights, significant data limitations remain, particularly in relation to financial disclosures, legal consequences, and technical forensics. With these gaps remaining the application of robust macroeconomic models and sector-wide risk estimations are cumbersome.

The hybrid ISS model and custom taxonomy introduced in this study provided a repeatable framework to classify and compare diverse incidents. Yet, the overall reliability of analytical conclusions remains constrained by the quality and completeness of available data. Future research and industry coordination will need to prioritise structured incident documentation and cross-sector information sharing to enable a more accurate assessment of systemic risk.

The following chapter builds on this quantitative foundation by examining three high-impact case studies in detail. These illustrate how cyber incidents unfold in real-world operational contexts, what costs they incur, and how varying levels of preparedness shape organisational response and recovery.

5 Case Study Analyses

This chapter presents a comparative analysis of three major cyber incidents in the maritime domain, each affecting a critical logistics actor at different points in time and across diverse geopolitical and operational contexts. The selected case studies: A.P. Møller–Maersk (2017), CMA CGM (2020), and Transnet SOC Ltd (2021), illustrate the evolving threat landscape, varied attacker motivations, and the differing capacities of maritime organisations to respond and recover. Each case is examined through a structured lens, covering incident summaries, malware characteristics, operational and financial impacts, regulatory responses, and long-term organisational consequences. The chapter demonstrates how similar attack vectors yield to vastly different outcomes depending on digital maturity, institutional resilience, and governance frameworks.

5.1 Case Study 1: MAERSK and the NotPetya Wiper Attack

A state-backed cyberweapon with global unintended consequences

5.1.1 Incident Summary

On 27 June 2017, A.P. Møller–Maersk, the world's largest container shipping company at the time, became the most high-profile victim of the NotPetya cyberattack. Although initially misidentified as ransomware, NotPetya was, in fact, a wiper malware designed to irreversibly destroy data. The attack originated in Ukraine and propagated globally by exploiting the EternalBlue vulnerability, a now-infamous exploit originally developed by the U.S. National Security Agency and later leaked by the Shadow Brokers group [5], [78], [79]. Maersk's infection occurred through a compromised software update for M.E.Doc, a Ukrainian accounting application widely used by local businesses. Within minutes, the malware had propagated through Maersk's global IT infrastructure, disabling core digital systems and forcing the company to shut down its worldwide network. Despite the severity of the breach, Maersk managed to contain the incident's operational impact to a 20% reduction in trading volume over the ten-day crisis period, an outcome that drew attention for both the scale of disruption and the resilience demonstrated in response [58]. Figure 29 illustrates the ransomware lock screen message displayed on employee terminals during the incident, symbolising the immediate and visible nature of the disruption [80].

5.1.2 Victim: A.P. Moller – Maersk at the Time of the Attack.

In 2017, A.P. Møller–Maersk was operating in more than 130 countries, with a workforce of approximately 88,000 employees. Its subsidiaries including Maersk Line, APM Terminals, and Damco together controlled nearly 20% of the global container shipping capacity and oversaw operations at 76 ports worldwide and deployed a fleet of around 800 vessels[78]. This expansive footprint positioned Maersk as a central actor in international trade, with digital systems underpinning complex supply chain functions. The company's global logistics network was highly reliant on centralised IT systems, a design choice that enhanced operational efficiency but also made it particularly vulnerable to fast-moving, self-propagating malware. Once infected, the lack of internal segmentation enabled the malware to spread unchecked across business units and geographic regions. As of 2024, Maersk remains one of the world's top three container shipping companies, maintaining a market share of approximately 14–15% of global TEU capacity [79], [81]. The company is a key participant within the maritime logistics its absence from the supply chain causes systemic risk, a fact, that became strikingly evident during the NotPetya incident.

5.1.3 The Malware: NotPetya

NotPetya exemplifies the use of cyberweapons in geopolitical conflict, disguised as financially motivated ransomware. Although infected systems displayed a ransom demand, there was no mechanism to decrypt affected files, and in most cases, the malware irreversibly overwrote the Master Boot Record (MBR), rendering systems permanently unusable [78], [82]. NotPetya leveraged a combination of propagation and privilege escalation tools. It spread laterally using the EternalBlue exploit, a vulnerability in the Server Message Block (SMB) protocol originally developed by the NSA and later leaked to the public, and employed credential harvesting tools such as Mimikatz. Once inside a network, NotPetya used PsExec to traverse systems with administrative rights, accelerating its spread across enterprise environments [83]. The malware's entry point into Maersk's infrastructure was a compromised update to the Ukrainian accounting software M.E.Doc, widely used by firms doing business in Ukraine. This infection vector allowed the malware to target Ukrainian organisations initially; however, its aggressive propagation design quickly extended collateral damage to global corporations, including Maersk, FedEx, Merck, Mondelez, and DLA Piper (as well as Russian based companies).

Figure 29 – Maersk NotPetya cyberattack illustration [80]

Attribution analyses linked NotPetya to the Russian military intelligence agency (GRU), marking it as a state-sponsored cyberweapon deployed amid geopolitical tensions between Russia and Ukraine. It is now widely regarded as one of the most destructive cyberattacks in history, with estimated global losses exceeding $10 billion [5]. Table 7 summarises the key technical characteristics of the NotPetya malware, and the broader unfolding NotPetya attack, and its trajectory beyond Ukrainian borders, is illustrated in Figure 30, which visualises how a regionalised cyber weapon cascaded into a global economic disruption [84].

Table 7 – NotPetya malware summary

Attribute	**Details**
Type:	Wiper (masked as ransomware)
Attacker identity	Russian GRU (Military Intelligence) –state-sponsored
Attacker origin	Russia
Tactics	Rapid self-propagation, destructive payload disguised as ransom
Attack vector	Compromised software update (M.E.Doc)
Exploitation method:	EternalBlue (SMB vulnerability), Mimikatz (credential harvesting), and PsExec (lateral movement)
Encryption / Destruction:	permanently overwrote the master boot record (MBR), rendering systems inoperable.

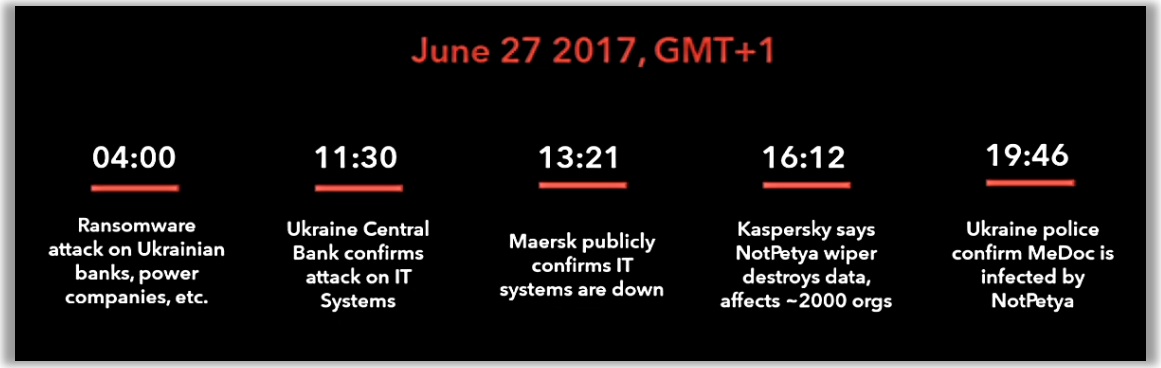


Figure 30 – Unfolding of NotPetya attack [84]

5.1.4 Operational Disruptions

The operational impact of the attack on Maersk was both immediate and extensive. Approximately 49,000 laptops, 1,200 applications, and 1,000 servers were disabled across Maersk's global network, servers were rendered inoperable within hours of the initial compromise. Seventeen of the company's 76 port terminals were temporarily shut down, including major logistics hubs such as the Port of Los Angeles. The core online booking platform (Maerskline.com) remained inoperable for eight days, forcing the company to revert to manual operations for all critical logistics coordination. Employees resorted to ad-hoc tools such as WhatsApp and personal emails to manage shipping schedules and communicate with customers [5], [78].

Full restoration of booking systems and terminal functionality took several weeks. The rebuilding process required replacement and reinstallation of approximately 45,000 PCs, 4,000 servers, and over 2,500 applications [78]. The extent of these system failures demonstrates the degree to which digital infrastructure had become essential to Maersk's business model and, conversely, the scale of vulnerability exposed by inadequate segmentation and insufficient resilience planning.

5.1.5 Short-Term and Med-Term Impact

In the immediate consequences were severe. In the ten days following the incident, Maersk reported an estimated 20% reduction in trading volume, primarily due to inability to process bookings, manage cargo movements, or maintain normal operations. Revenue from several shipping container lines froze, and port delays further disrupted logistics [58]. The attack's ripple effects extended far beyond Maersk's internal systems. For example, the shutdown of the Elizabeth terminal at the Port of New Jersey caused major

congestion, with an estimated 2,500 trucks per day affected by delayed access and processing. These disruptions resulted in tens of millions of dollars in losses for trucking firms and logistics providers operating in the region [5].

On a broader level, Maersk's global customers were forced to reroute cargo through alternative channels at significant cost. Some resorted to last-minute air freight to maintain supply chain continuity, while others incurred spoilage risks as refrigerated containers remained stranded without adequate power. Production halts and inventory shortages emerged as secondary effects, further amplifying the economic consequences of the operational standstill. While the company managed to resume digital functionality in stages over several weeks, full restoration of integrated services required a complete rebuild of IT systems and applications. In this sense, the medium-term impact of the attack extended well beyond the initial disruption period, with recovery operations continuing even after external service continuity was nominally re-established [58], [78].

5.1.6 Long-Term Impact and Cybersecurity Enhancements

Following the crisis, Maersk undertook on one of the most comprehensive IT recovery efforts recorded in maritime cyber history. The company rebuilt its entire IT infrastructure over a matter of weeks, restoring 45,000 PCs, 4,000 servers, and over 2,500 applications [78]. In parallel, Maersk invested heavily in cybersecurity upgrades, including the implementation of multi-factor authentication, enhanced network segmentation, and the restructuring of its IT governance model [85]. These efforts were not only technical but strategic, The incident catalysed a broader organisational shift in how cyber risk was perceived and managed. Maersk's leadership treated the breach as a strategic inflection point transforming a crisis into a foundation for digital resilience. Investments extended to infrastructure modernisation, revised business continuity planning, and increased executive-level oversight of cybersecurity decision-making. At the same time, the company issued financial compensation in the form of seven-figure reimbursements to select customers affected by the disruption. Which gesture helped reinforce customer confidence, and maintain business trust despite reputational damage on the wake [5], [85].

Taken together, these strategic responses have shown Maersk's ability to recover from one of the most destructive cyberattacks in corporate history and also setting a very high benchmark for post-incident transformation in the maritime sector.

5.1.7 Financial Impact

Maersk publicly reported losses between $250 million and $300 million, encompassing lost revenue, business disruption, and recovery costs [5]. Relative to its annual revenue of $30.9 billion in 2017, this represented approximately 1% of turnover [86]. Despite the substantial figure, Maersk maintained its expectations for underlying profit for the year, suggesting a remarkable degree of financial resilience. However, these official figures do not capture the broader indirect costs arising from widespread operational disruptions, port closures, and cascading effects across the supply chain. For instance, the shutdown of the Elizabeth terminal at the Port of New Jersey led to extensive truck congestion, with delays stretching for days. Approximately 2,500 trucks per day were affected, leading to estimated costs for trucking companies in the tens of millions of dollars [5].

The global supply chain impact was equally significant. Ships were delayed, port operations stalled and refrigerated containers carrying perishable goods faced spoilage risks due to unavailable power supplies. Maersk's customers had to reroute cargo at high last-minute fees or resort to expensive air freight to avoid production halts, further amplifying economic costs.

5.1.8 Global and Macroeconomic Implications

Although Maersk was among the most visibly affected entities, the NotPetya attack caused disruption on a global scale, inflicting collateral damage far beyond its initial target region. In Ukraine, the epicentre of the attack NotPetya paralysed major sectors, including government agencies, banks, transportation systems, and healthcare institutions. The cumulative disruption was estimated to reduce Ukraine's national GDP by approximately 0.5% [87]. Global cost estimated to be over $10 billion although precise figures vary depending on methodology [78]. What is evident, however, is that multinational corporations with even limited operational exposure to Ukraine were vulnerable to cascading damage due to interconnected IT systems and supply chains. This characteristic transformed NotPetya from a targeted act of cyber sabotage into a globally disruptive event. Several high-profile, multinational corporations reported significant financial losses directly linked to NotPetya. These included firms across a broad range of industries including pharmaceuticals and logistics to legal services and construction materials [88].Table 8 presents a non-exhaustive list of affected companies, their sectors, and reported or estimated financial losses.

Table 8 – An uncomplete list of companies impacted of NotPetya cyberattack in 2017

Company	Country	Sector	Estimated Loss / Impact
A.P. Moller–Maersk	Denmark	Shipping & Logistics	~$200–300 million Operational halted [5]
Merck & Co.	USA	Pharmaceuticals	~$1400 million[88], [89] Manufacturing and R&D impacted.
FedEx (TNT Express)	USA Netherlands	Logistics	~$300–400 million [88], [90]
Mondelez International	USA	Food & Beverage	~$188 million in impact. Disrupted orders, manufacturing, and logistics [88], [91], [92]
Cadbury (owned by Mondelez)	Australia	Food	Production lines in Tasmania halted [93]
Saint-Gobain	France	Construction Materials	~$384 million Manufacturing systems affected [5].
Reckitt Benckiser	UK	Consumer Goods	~$117 million loss in sales. Product delivery affected. [92]
Nuance Communications	USA	Healthcare IT	$92 million revenue loss; patient transcription systems was down [92], [94].
DLA Piper	USA / Global	Legal	Offices globally shut down temporarily. Internal systems disabled. 15,000 hours of paid overtime to rebuild of IT system [95].
Heritage Valley Health System	USA	Healthcare	Regional hospital system in Pennsylvania disrupted. Later fined for $950 000 noncompliance with HIPAA [96].
WPP	UK	Advertising & Media	$15 million – IT systems down across multiple offices., impact limited due to not fully integrate systems [92].
EVRAZ	Russia	Steel Manufacturing	Reported systems disruption [97].
Rosneft	Russia	Oil & Energy	Claimed no operational disruption but **confirmed target** [97].

The inclusion of healthcare providers such as Heritage Valley Health System, where patient services, surgeries, and diagnostics were interrupted demonstrates the societal risks posed by large-scale cyber incidents. In 2024, the organisation was fined $950,000 under the HIPAA Security Rule for failing to maintain appropriate safeguards for patient data, underscoring how cyberattacks can produce both immediate disruptions and delayed regulatory consequences [96]. The maritime sector, by contrast, lacked equivalent mandatory cybersecurity regulations at the time of the Maersk incident. This regulatory gap left maritime operators without the enforcement frameworks necessary to ensure adequate digital safeguards. The systemic vulnerabilities exposed also reinforce the need for sector-specific regulation, not only to protect operational continuity but also to mitigate cross-sector economic risk in an increasingly interconnected digital ecosystem.

5.1.9 Stock Market Responses

The stock market reaction to NotPetya was immediate but relatively short-lived. Companies such as FedEx (FDX), Mondelez International (MDLZ), and Merck & Co (MRK) experienced initial drops in trade volumes and share prices. However, the longer-term stock performance of affected firms indicates a pattern of resilience. As shown in Figure 31, the share prices of these companies largely recovered in the months following the attack, influenced more by broader market trends and company-specific developments than by the cyber incident itself [98]. For example, despite incurring substantial losses, Merck's share value remained relatively stable over time, buoyed by the firm's overall financial health and sector performance. This trajectory suggests that while cyberattacks can cause significant short-term financial disruption, their longer-term effects on stock valuations may be limited, especially for large, diversified firms with sufficient resources and investor confidence. In this respect, the market's response to NotPetya highlights a potential underestimation of structural cyber risk, particularly in sectors, such as maritime logistics, where operational disruptions can have systemic consequences.

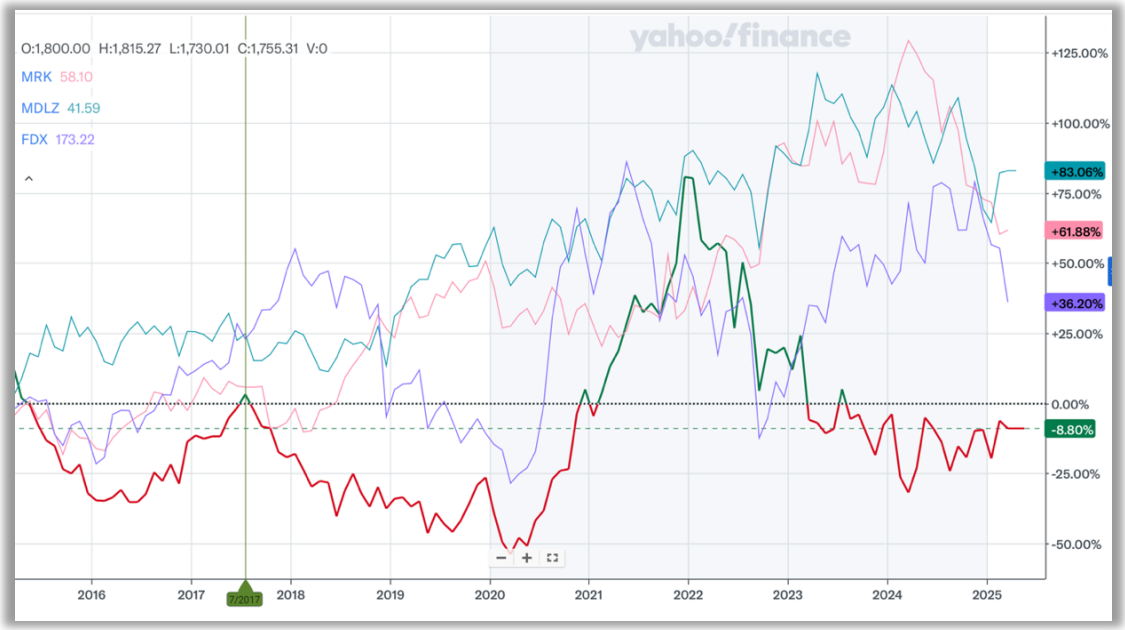


Figure 31 – Comparative Stock Price Performance of NotPetya-Affected Companies (2016–2025) [98]

5.1.10 Insurance Fallout and Legal Disputes

The NotPetya attack exposed significant limitations in the global insurance industry's capacity to absorb cyber risk, particularly in a case involving state-attributed attacks. Although many affected companies held cyber or business interruption policies, these often proved insufficient or inapplicable due to their exclusions based on the nature of the

incident. As one of the most high-profile legal disputes arising from the attack was initiated by Merck & Co., who filed a $1.4 billion claim to recover losses incurred during the incident [89], [99]. Insurers initially rejected the claim, citing the “act of war” exclusion clause, which is traditionally applied to armed conflict. Merck contested this interpretation in court, arguing that the clause was never intended to cover cyberattacks. In 2023, the parties reached a confidential settlement, establishing a significant legal precedent: cyberattacks, even when attributed to nation-states, may not automatically fall under war exclusions [100].

In contrast, multiple sources suggest that Maersk absorbed a substantial portion of its estimated $250–300 million losses internally, possibly due to limited cyber insurance coverage [91], [101]. The broader impact of NotPetya led to significant shifts in the insurance market. Industry leaders, including Lloyd’s of London, subsequently redefined policy wordings to limit or exclude coverage for cyber incidents involving nation-state actors [102]. These changes marked a shift in how insurers assess geopolitical cyber risk, while also raising questions about the long-term viability of insurance as a reliable mitigation tool for complex cyber threats.

A persistent ambiguity is defining what constitutes “cyberwarfare” further complicates the issue. In a 2025 interview, Tom Clementi, CEO of Pool Re, the UK’s state-backed reinsurer warned that the blurred boundary between cyberterrorism and cyberwarfare could render existing schemes increasingly obsolete unless clearer guidance is introduced [103]. Clementi emphasised that many cyber insurance policies may not be triggered in cases of state-backed attacks, raising concerns that national governments could increasingly become insurers of last resort in catastrophic cyber scenarios.

5.1.11 Conclusion

The NotPetya attack on A.P. Møller–Maersk remains a landmark incident in maritime cybersecurity history. It demonstrated how a state-sponsored cyberweapon, initially intended to destabilise a geopolitical adversary, can inflict indiscriminate global economic damage through interconnected digital system. Although Maersk was not a direct target, the company became one of the most severely affected, with operations crippled across 130 countries and dozens of ports. Despite the disruptions, the company succeeded in limiting its long-term financial losses and strategically leveraged the incident to enhance its cybersecurity posture.

5.2 Case Study 2: CMA CGM and the Ragnar Locker Ransomware

A modern test of maritime cyber resilience and regulatory readiness

5.2.1 Incident Summary

On 28 September 2020, CMA CGM, one of the world's largest shipping and logistics companies detected a cyberattack affecting its peripheral servers. As a precautionary measure, the company immediately suspended external access to core digital platforms, including customer portals, websites, and email systems, to prevent the malware from spreading further. The attack disrupted operations globally, resulting in booking outages, internal communication failures, and terminal delays [104]. Within days, attribution pointed to the Ragnar Locker ransomware group, known for targeting high-value organisations using double extortion techniques. The attackers demanded that CMA CGM contact them within 48 hours to negotiate a ransom in exchange for decryption keys and to prevent the publication of stolen data. CMA CGM publicly acknowledged the breach and began a phased restoration of services, with regular updates posted on its corporate website. Full digital service functionality was restored by 11 October 2020 [104], [105], [106], [107]. Figure 32 presents a screenshot from CMA CGM's website informing customers about the attack, part of the company's effort to maintain transparent communication throughout the incident [108].

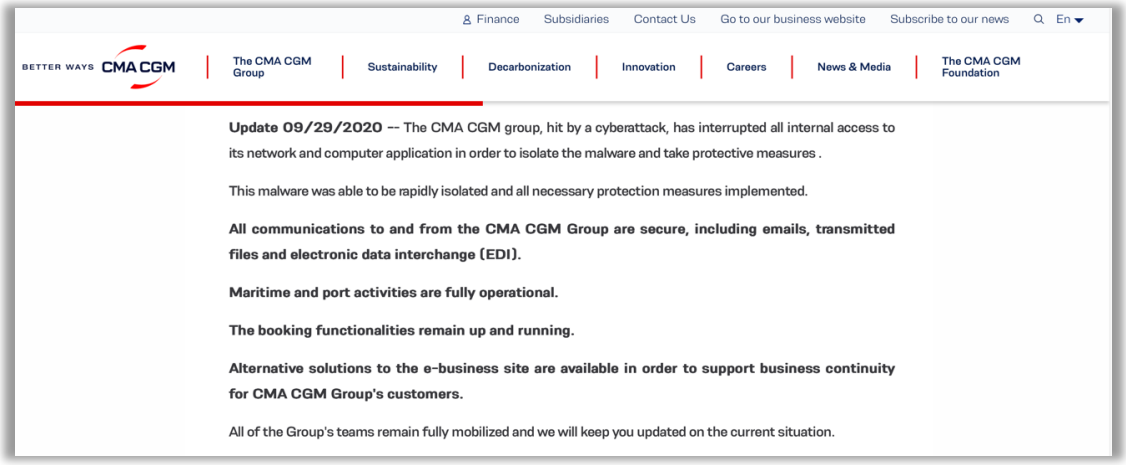


Figure 32 – Notice on CMA CGM webpage informing about the cyberattack [108]

5.2.2 Victim: CMA CGM Group

Compagnie Maritime d'Affrètement – Compagnie Générale Maritime (CMA CGM), headquartered in Marseille, France, is a global leader in container transport and logistics.

By 2020 the company operated in over 160 countries with a fleet of more than 650 vessels, servicing 420 ports worldwide. That year, CMA CGM ranked as the fourth largest container shipping company globally, handling approximately 23 million TEUs and reported annual revenues exceeding $31 billion [109]. At the time of the attack, it ranked as the fourth-largest container shipping company globally. CMA CGM had positioned itself as a technological and environmental innovator within the maritime sector. A key milestone was the launch of the “Jacques Saadé,” the world’s first LNG-powered ultra-large container ship, which symbolised the company’s dual commitment to sustainable shipping and digital transformation. This vessel’s inaugural arrival at the Port of Zeebrugge in 2020 marked a significant moment for the firm’s operational strategy and public image. Figure 35 depicts the vessel during its first docking at the Port of Zeebrugge, Belgium.

Figure 33 – The "Jacques Saadé," first of its size giant container ships, in port of Zeebrugge [110]

5.2.3 The Malware: Ragnar Locker

Ragnar Locker is a ransomware variant first identified in 2019 and is known for its focus on high-value enterprise targets across critical infrastructure sectors. It employs a double extortion strategy: after encrypting a victim’s files, attackers threaten to release exfiltrated data publicly if the ransom is not paid. This approach increases pressure on organisations to settle, particularly when sensitive corporate, customer, or financial records are involve [111]. The group operates under a Ransomware-as-a-Service (RaaS) model, allowing

affiliates to deploy the malware while sharing ransom proceeds. Industries previously affected by Ragnar Locker include energy, logistics, manufacturing, and retail. The malware typically infiltrates systems via spear phishing or exploitation of Remote Desktop Protocol (RDP) vulnerabilities, followed by privilege escalation and lateral movement across Windows environments.

In CMA CGM's case, threat actors reportedly exfiltrated internal data before initiating file encryption. The attackers then demanded a ransom—though the amount was never publicly disclosed—in exchange for a decryption key and a promise not to publish the stolen files. Shortly after the breach, screenshots believed to originate from Ragnar Locker's dark web leak site appeared online. These screenshots displayed directory structures from CMA CGM's internal systems, raising concerns over the potential exposure of financial records, customer data, and sensitive operational information [106]. Table 9 summarises the technical attributes of the Ragnar Locker ransomware, while Figure 34 illustrates the timeline of the incident, from the initial detection and service suspension on 28 September, through the identification of the attacker, and culminating with the full restoration of digital services by 12 October 2020.

Table 9 – summary of Ragnar Locker

Attribute	Details
Type:	Ransomware
Attacker identity	Ragnar Locker – financially motivated threat actor active since at least 2019
Attacker origin	unknown (likely Eastern Europe, per general threat intelligence)
Tactics	Double extortion – file encryption + threat of leaked data
Attack vector	Likely spear phishing or exploitation of Remote Desktop Protocol (RDP) vulnerabilities
Exploitation method:	Privilege escalation and lateral movement inside Windows environments
Destruction / Encryption	Strong AES encryption with RSA key wrapping (hybrid model)

5.2.4 Operational Disruptions

The ransomware attack forced CMA CGM to suspend access to key digital platforms, including booking systems, container tracking tools, and document processing services. These outages disrupted global e-commerce operations and internal communications, affecting customer service and logistical coordination. However the digital disruptions,

maritime shipping and port operations continued. While vessels remained active and terminals functional, inefficiencies emerged due to limited access to core systems. Staff relied on manual workarounds and alternative channels to manage bookings and documentation [112]. The incident demonstrated CMA CGM's ability to sustain essential operations under pressure, demonstrating the value of business continuity planning in mitigating the impact of cyberattack.

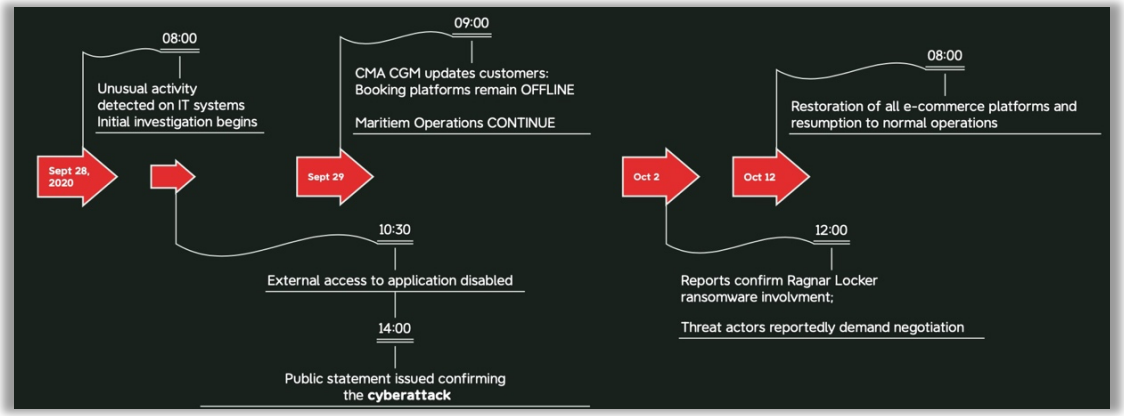


Figure 34 – Timeline of cyberattack on CMA CGM [created by author]

5.2.5 Short-Term Actions, Impact, and cybersecurity regulation compliance

In response to the attack, CMA CGM enacted immediate containment measures. Customers were redirected to alternative booking channels while digital services were gradually restored. The company mobilised internal resources and external cybersecurity experts to investigate the breach, restore affected systems, and enhance technical defences. Recognising its legal obligations under European data protection law, CMA CGM notified France's data protection authority (CNIL) and engaged closely with ANSSI (Agence nationale de la sécurité des systèmes d'information). These steps ensured compliance with the General Data Protection Regulation (GDPR), particularly in relation to breach notification and risk mitigation requirements [113]

Operational continuity was prioritised with regulatory responsiveness. Although booking capabilities remained limited during the outage, CMA CGM's communication strategy centred around public service updates helped to maintain transparency with customers and partners. The incident revealed the growing regulatory scrutiny on cybersecurity incidents in the maritime domain and underscored the importance of aligning incident response with both technical recovery and legal accountability

5.2.6 Mid- and Long-Term Impacts

Although CMA CGM successfully restored its core services within two weeks, the incident left a lasting imprint on both the maritime and cybersecurity industries. It prompted the company – as well as the broader sector – to reassess and strengthen cybersecurity protocols in an effort to mitigate future risks. In September 2021, CMA CGM disclosed a separate cyber incident involving the compromise of customer personally identifiable information (PII) [114]. While unrelated to the 2020 Ragnar Locker attack, the disclosure further highlighted the ongoing vulnerability of digital platforms in maritime logistics. The Ragnar Locker incident also contributed to raising broader industry awareness around the risks associated with OT–IT convergence. It reinforced the urgency of adopting structured cyber risk frameworks such as the BIMCO Guidelines and the IMO 2021 cybersecurity mandates, which were in development at the time [115].

5.2.7 Financial Impact and Organisational Response

Despite the operational disruption caused by the Ragnar Locker attack, CMA CGM's overall financial performance in 2020 remained strong. The company reported a net income of $1.75 billion, marking a significant recovery from the $229 million loss recorded the previous year. This growth was primarily driven by pandemic-induced surges in freight demand, increased shipping rates, and constrained global supply chains [113]. According to the company's 2020 Consolidated Financial Statements, the direct financial impact of the cyberattack was estimated to be below $50 million. Section 3.8 of the report states:

> "*The impact resulting from this incident can be estimated to be below USD 50 million. The Group's cyber liability insurance may cover part of the financial loss but it is currently too early to predict the extent and timing of any cyber liability insurance indemnification*" [113].

This relatively modest financial impact suggests that CMA CGM effectively limited its financial exposure, likely aided by timely containment measures, an established recovery plan, and effective business continuity strategies. However, broader effects such as reputational harm or diminished customer confidence are inherently more difficult to quantify. As of the close of the 2020 reporting period, no public confirmation had been provided regarding any insurance indemnity recovery. Following the attack, the company

emphasised digital resilience. Although the 2021 financial statements did not disclose specific cybersecurity expenditure, the company highlighted ongoing investments into digital platforms, customer-facing technologies, and innovation initiatives through CMA CGM Ventures [116]. These initiatives included enhancing end-to-end supply chain visibility, deploying AI-driven customer service solutions, and investing in logistics technology start-ups. Most of which strategies likely influenced by the lessons of the 2020 incident. As CMA CGM is a privately held company, no publicly available stock performance data exists to assess direct market valuation impacts. Nevertheless, the company's financial trajectory remained highly positive following the attack, culminating in a record profit of $17.9 billion in 2021[116]. This outcome suggests that the ransomware incident had no lasting detrimental effect on CMA CGM's overall financial position.

5.2.8 Conclusion

The 2020 ransomware attack on CMA CGM demonstrated how rapid containment, transparent communication and regulatory compliance can effectively mitigate the consequences of a major cyber incident. While the attack temporarily disrupted digital services and raised concerns over potential data exposure, the company's response limited both operational damage and financial loss. The estimated direct cost of the incident was relatively modest given the scale of CMA CGM's operations. The maritime and port activities continued during the digital outage, supported by contingency measures that preserved business continuity. The company's ability to recover without lasting reputational or financial harm reflects the effectiveness of its crisis management and resilience planning. More broadly, the incident contributed to growing awareness of cybersecurity as a strategic imperative in maritime logistics. It reinforced the importance of adhering to evolving regulatory standards and investing in long-term digital transformation.

5.3 Case Study 3: Transnet and the Death Kitty Ransomware Attack

National chokepoint disrupted: cyber vulnerability, crisis convergence with systematic risk

5.3.1 Incident Summary

On 22 July 2021, Transnet SOC Ltd, South Africa's state-owned freight and port operator was hit by a ransomware attack that paralysed digital operations at several major maritime gateways, including the ports of Durban, Ngqura, Port Elizabeth, and Cape Town [117]. In response, Transnet declared force majeure, citing unforeseen and uncontrollable circumstances, and reverted to manual procedures across its port systems. The cyberattack halted critical logistics functions such as vessel scheduling, cargo tracking, customs clearance, and gate operations. The Port of Durban, which processes over 60% of the nation's container traffic, was most affected, with mounting vessel queues and delays cascading through the regional supply chain.

The incident unfolded just days after widespread civil unrest and looting in KwaZulu-Natal and Gauteng provinces, prompting early speculation of coordinated sabotage. However, forensic analyses later attributed the breach to financially motivated cybercriminals rather than politically driven actors. Regardless of attribution, the attack compounded existing fragilities in South Africa's logistics infrastructure already strained by pandemic-related disruptions, workforce shortages, and ageing assets [117].

Transnet's 2021 Integrated Report confirmed that systems were taken offline, business continuity protocols were activated, and all IT infrastructure had to be restored or rebuilt. The company maintained that no data was exfiltrated and that the integrity of its financial and operational records remained intact [118]. The breach marked a turning point in South Africa's cybersecurity discourse, elevating awareness of digital vulnerabilities across its logistics sector and triggering broader discussions around port resilience, national infrastructure protection, and maritime cybersecurity governance [117].

5.3.2 Victim: Transnet SOC Ltd

Transnet SOC Ltd is South Africa's state-owned logistics operator, responsible for managing the country's core freight transport infrastructure including rail, ports, and pipelines. With over 55,000 employees and annual revenues exceeding ZAR 67 billion (~ $3.9 billion in 2021), Transnet plays a foundational role in enabling domestic and

regional trade [118], [119] Through its operating division, Transnet Port Terminals (TPT), the company oversees seven commercial ports and serves as the largest container facility in sub-Saharan Africa. Durban alone handles more than 60% of South Africa's container volumes and functions as an important logistics hub for landlocked neighbouring countries such as Zambia, Zimbabwe, and the Democratic Republic of Congo [120]. Figure 35 is a picture of the Port of Durban, showing its size and its strategic importance as a continental chokepoint for maritime commerce [121].

Figure 35 – Port of Durban [121]

At the time of the cyberattack, Transnet was already under considerable strain. The COVID-19 pandemic had disrupted global and domestic supply chains, infrastructure maintenance had fallen behind schedule, and violent civil unrest in KwaZulu-Natal had damaged key freight corridors. Dealing with workforce shortages further undermined resilience. These overlapping stressors amplified the company's exposure to systemic risk, particularly as the ports were already reliant on digital tools for vessel scheduling, yard planning, cargo tracking, and customs clearance[122]. The ransomware targeted these digital systems, including the Navis N4 Terminal Operating System Transnet's core platform for coordinating berthing, container handling, and gate access. Therefore, the disruption halted time-critical port activities and rippled outward through interconnected freight and trade systems. In the broader context, Transnet's performance had already been deteriorating, and the trend continued. Between 2019 and 2023, the company moved

from a profit of $275.3 million to a loss of over $313 million at the port terminal level [123]. With total debt exceeding $6 billion, underinvestment became a chronic issue, leading to frequent equipment breakdowns, cargo congestion, and reputational decline. The Port of Durban, once ranked 45th globally on Lloyd's List, had fallen to 79th by 2022. The World Bank's Container Port Performance Index (CPPI) placed it near the bottom: 341st out of 348 ports in 2022, and 398th out of 405 by 2023 [124], [125]. In response, Transnet launched a R3.4 billion port equipment overhaul programme aimed at restoring operational reliability and improving international competitiveness. Therefore, the 2021 cyberattack not only deepened existing challenges but also catalysed for reform [125].

5.3.3 The Malware: "Death Kitty" Ransomware

Although Transnet did not publicly confirm the exact strain of malware involved in the 2021 breach, subsequent cybersecurity investigations attributed the incident to the Death Kitty ransomware variant, also known as FiveHands (see Table 10).

Table 10 – Summary of Death Kitty Ransomware

Attribute	Details
Type:	Ransomware
Attacker identity	Unknown; indicators suggest HelloKitty or Death Kitty ransomware group
Attacker origin	Not officially attributed; cybercriminal group suspected (not state-sponsored)
Tactics	Encryption of critical IT systems, lateral movement, possible data exfiltration
Attack vector	Undisclosed; likely Remote Desktop Protocol (RDP) or credential compromise
Exploitation method:	Possibly Active Directory compromise and lateral movement
Destruction / Encryption	Likely symmetric file encryption via HelloKitty variant

This malware belongs to a family of financially motivated ransomware tools often deployed by criminal groups operating out of Eastern Europe or Russia [126]. The Death Kitty ransomware variant has previously been used in attacks against major corporations worldwide, typically exploiting unpatched vulnerabilities in remote access software or abusing compromised credentials to gain initial entry [117]. Death Kitty is associated with double extortion tactics: it encrypts an organisation's files while simultaneously threatening to leak stolen data if ransom demands are not met. In the case of Transnet, the

ransomware infiltrated enterprise IT systems, encrypted Active Directory servers, and rendered critical terminal platforms inoperable [120]. Transnet announced soon after the incident that no data was stolen, therefore no sensitive information compromised [117].

5.3.4 Attack timeline

The Transnet cyberattack unfolded over a two-week period during July and early August 2021, causing widespread disruption to port operations and logistics networks. As illustrated in Figure 36, the initial breach is believed to have occurred around 22 July, when Transnet began experiencing unexplained outages across its IT infrastructure [120]. On 23 July, the company publicly confirmed that it had suffered a cyberattack involving what it termed "security intrusion and sabotage" [127]. Though technical specifics were not disclosed, by 24 July, Transnet had declared force majeure at its principal container terminals (Durban, Ngqura, Port Elizabeth, and Cape Town) signalling a total halt to normal digital workflows. This legal step allowed the company to suspend contractual obligations, citing the unforeseen nature of the incident.

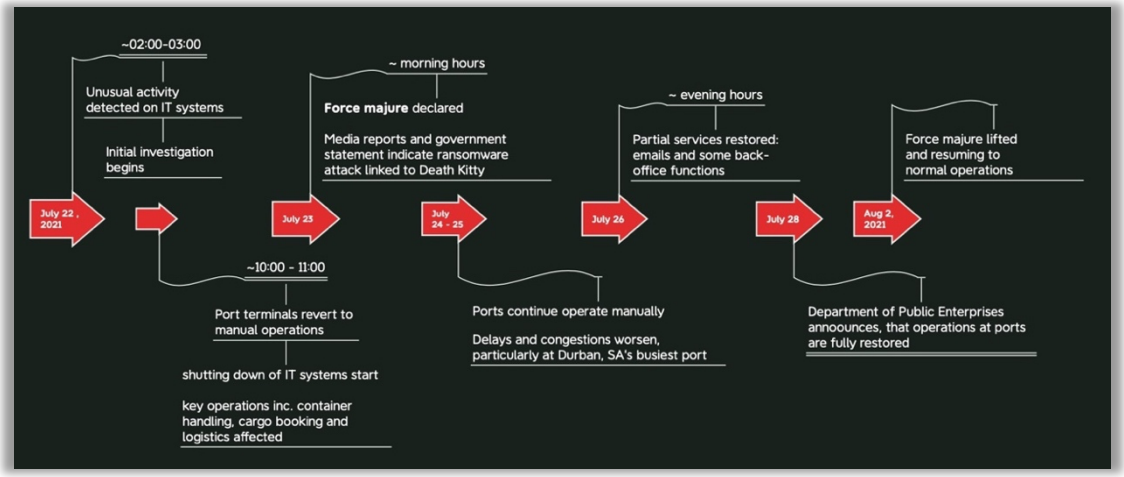


Figure 36 – Timeline of Cyberattack on Transnet 2021 [Created by the author]

With most IT systems offline, Transnet resorted to paper-based operations, which significantly slowed core logistics functions such as gate entries, truck scheduling, cargo documentation, and container handling. The Port of Durban, as South Africa's primary maritime gateway, faced immediate and severe congestion. Vessel queues lengthened, and productivity levels plummeted as port personnel were forced to process shipments manually. The company's internal IT response teams, supported by private cybersecurity firms and national authorities, began system recovery efforts in the final days of July. By

29 July, basic digital functionalities at container terminals were reportedly restored, allowing a gradual return to standard workflows. On 2 August, Transnet officially lifted the force majeure declaration, although the backlog of containers, delayed vessels, and disrupted inland freight corridors continued to affect operations well beyond that date [120]. Although no ransomware group formally claimed responsibility, and no arrests were made, the case remains notable for the speed with which an unconfirmed malware variant halted operations at one of Africa's most critical trade chokepoints

5.3.5 Operational Disruptions

The immediate impact of the ransomware attack was severe and widespread, with Transnet's container terminals rendered virtually inoperable from 22 July 2021. Critical digital platforms (e.g., vessel scheduling, gate access, and customs processing) were taken offline, forcing staff to revert to manual documentation and coordination. This sudden shift significantly reduced port throughput and delayed cargo clearance across the country [128]. At the Port of Cape Town, at least six container ships waited at anchorage due to congestion, while two vessels bypassed the port entirely. Only 2,760 containers were moved during the week of the outage, compared to an average of 2,000 containers per day. By the time digital systems were restored, more than 10,000 containers had accumulated in backlog [117]. Disruptions affected both import and export flows. Critical goods (e.g., automotive components, industrial inputs, and perishable food items) were stranded at port facilities, with refrigerated containers facing elevated spoilage risks due to delayed power connections and limited cold storage availability [129]. The inland impact was equally significant. Terminals such as City Deep in Johannesburg experienced rail and trucking delays, as containers could not be cleared or tracked from the coastal ports. These bottlenecks rippled across the national freight network, compounding logistical inefficiencies and raising costs for downstream businesses [117].

Internal communications described the disruption as "unprecedented" in Transnet's history [130], with productivity collapsing, customer frustration mounting, and the broader economy absorbing substantial indirect losses.

5.3.6 Mid- and Long-Term Impacts

Although Transnet officially restored port operations by 2 August 2021, clearing the accumulated cargo and normalising vessel schedules proved considerably more

challenging. Recovery efforts extended for a further two to three weeks, during which ports operated with extended shifts and additional staffing to address backlogs [129]. Freight forwarders and shipping lines estimated that full normalisation would take at least three additional weeks [118]. The reputational impact was tangible. South Africa's ports continued to slide in global competitiveness rankings. Notably, the Port of Durban experienced further decline on the CPPI, reinforcing perceptions of systemic vulnerability and operational fragility [124], [125].

After the attack, some international shippers considered rerouting cargoes through alternative regional ports to avoid future risk exposure. Domestically, the incident served as a pivotal moment: it propelled cyber risk at ports to the forefront of public policy and industry discourse, accelerating initiatives aimed at bolstering cybersecurity resilience, business continuity planning, and ICT modernisation [119]. In the months following the cyberattack, Transnet undertook several initiatives aimed at strengthening its digital resilience and enhancing governance around ICT management. The organisation's 2021 Integrated Report [119] outlines completed actions relating to business continuity, cybersecurity posture, disaster recovery planning, and reputational risk management. These initiatives reflect a strategic response to the vulnerabilities exposed during the cyberattack and indicate an organisational shift towards more structured digital risk oversight. An overview of the completed actions is presented in Table 11.

Table 11 – Overview of Transnet's ICT governance and cybersecurity readiness actions post-incident, as reported in the 2021 Integrated Report [119]

Planned Actions	Status Update	Narrative Statement
Delegation to management to implement, executive effective technology and information management	Complete	• The ICT delegation from the Board to management is addressed in the DOA Framework, which is approved by the Board • The Risk Committee is delegated with the responsibility of exercising ongoing oversight of ICT risk management • In particular, the Risk Committee oversees the establishment and implementation of a business continuity arrangement that allows Transnet to operate under conditions of instability and to withstand and recover from any serious risk issues
ICT integration	Complete	• There is integration of people, technologies, information and processes across the organisation. There is ethical and responsible use of technology and information, and compliance with relevant laws
ICT role in ensuring business resilience	Complete	• ICT's challenges on disaster recovery plans, tests and reports were communicated to the Board and its subcommittees
Ensuring responsiveness to cybersecurity and social media risks	Complete	• Board seeks feedback on the Transnet cybersecurity posture and plans. Transnet IT positions cybersecurity as a top priority and guards against negative publicity and reputational damage

5.3.7 Financial Implications

Despite official confirmation in mid-August 2021 that no ransom had been paid and that approximately 90% of IT systems had been restored, the cyberattack inflicted substantial

economic disruption. Although the company did not release an official estimate of direct losses, operational paralysis at its largest ports and freight corridors resulted in severe financial ripple effects [120]. The outage affected both high-value exports and time-sensitive imports. An estimated 40,000 tonnes of refrigerated cargo were exposed to spoilage risk due to cold storage bottlenecks [129]. Among the most directly impacted firms was aluminium producer Hulamin, which reported $12.6 million in losses stemming from shipment delays [131]. These figures, while significant, represent only a fraction of the broader economic impact. Sector-wide analyses suggest that South Africa lost as much as ZAR 50 billion (~ $2.8 billion) in export earnings across the mining and agricultural sectors over the 12 months following the incident [120] . Contributing factors included missed shipping windows, trade rerouting, and loss of investor and stakeholder confidence in port reliability.

The Transnet breach occurred during a fragile post-COVID economic recovery period and compounded existing weaknesses in South Africa's freight infrastructure. While systems were eventually restored, the financial consequences, both measured and unmeasured demonstrate outsized cost of cyber incidents in logistics chokepoints and the difficulties in quantifying long-tail effects.

5.3.8 Long-Term Competitiveness and Strategic Impact

Beyond immediate financial burdens, the attack raised critical concerns regarding the long-term competitiveness of South African ports. Increased insurance premiums heightened operational risk profiles, and higher shipping costs stemming from perceived cyber vulnerabilities threatening to deter future investment and divert trade routes to ports perceived as more secure. Nevertheless, the incident also served as a catalyst for reform. By late 2021, Transnet had revised its business continuity plans and initiated major cybersecurity improvements, marking important steps towards restoring operational resilience [129].

5.3.9 Insurance and Loss Recovery Considerations

The attack also exposed substantial gaps in insurance coverage and financial risk mitigation. Transnet did not publicly disclose whether it held cyber or business interruption insurance at the time of the incident. As a state-owned enterprise, it may have depended on self-insurance mechanisms, with extraordinary costs absorbed by the

government. Broader structural issues compound this vulnerability. Cyber insurance adoption in South Africa is notably low. Figure 39 shows the African cybersecurity market valued at just $0.99 billion in 2023, reflecting limited investment compared to global levels [132]. This underinvestment increases exposure not only for critical infrastructure operators like Transnet but also for businesses reliant on stable trade flows.

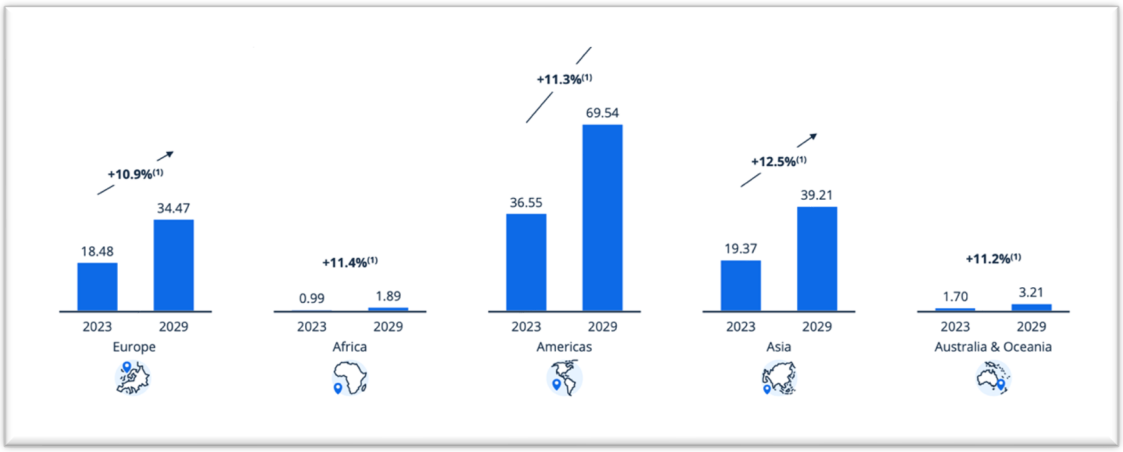


Figure 37 – Cybersecurity market size by region in 2023 and 2029 (projected) [132]

5.3.10 Broader Economic and Policy Lessons

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) noted that the "actual severity of the incident is hard to estimate" [133], particularly given the systemic and economic interdependencies involved. The attack hit South Africa at a vulnerable moment (post-COVID economic recovery) exacerbating national fragilities, and it will no doubt have long lasting damage to the country's economy. Although port operations resumed within several weeks, the incident revealed that broader economic damages (e.g., including cargo delays, missed shipping windows, and disrupted trade volumes) remained largely uninsured and absorbed by private sector stakeholders [131]. This highlights the structural gap between public infrastructure failure and private sector exposure, raising questions about risk distribution, liability and preparedness.

The attack revealed limitations in existing risk governance frameworks. Traditional incident response plans were insufficient to mitigate the cascading effects of a cyber event across national and regional trade systems. The absence of dedicated cyber insurance mechanisms magnified these losses, particularly in low-adoption environments such as sub-Saharan Africa. As shown in Figure 37, Africa's share of global cybersecurity investment remains marginal, intensifying vulnerability in an increasingly digitised trade

ecosystem [132]. At a strategic level, the incident dealt a blow to the long-term competitiveness of South African ports. Increased shipping costs, vessel delays, and perceived cyber insecurity heightened operational risk profiles. This, in turn, threatened to divert cargo flows to alternative regional ports viewed as more stable or technologically advanced. The World Bank's Container Port Performance Index reflected this decline, with Durban falling near the bottom of global rankings by 2023 [125]. Elevated insurance premiums and reputational damage further compounded competitive pressures.

5.3.11 Conclusions

Yet, the incident also functioned as a catalyst for reform. By late 2021, Transnet had revised its business continuity plans and initiated major cybersecurity improvements, including enhanced ICT governance and investment in port equipment upgrades [118], [129]. These measures signal a shift from reactive incident handling toward proactive resilience building. The Transnet case illustrates that cybersecurity in the maritime domain is no longer a purely operational concern. It is a national economic imperative, tightly interwoven with trade capacity, global positioning, and geopolitical relevance. Going forward, cybersecurity strategies must move beyond technical controls to incorporate comprehensive risk modelling, cross-sector collaboration, and economic protection mechanisms such as public-private cyber insurance schemes.

In sum, the Transnet attack highlighted that in digitally connected economies, a single cyber incident can escalate into a systemic crisis. Resilience in such contexts requires not only technical defences but institutional reform, investment in digital infrastructure, and alignment between cyber governance and national economic policy.

5.4 Comparative and Economic Impact Analysis

The three cyberattacks analysed in the preceding sections, 5.1 – Maersk (2017), 5.2 – CMA CGM (2020), and 5.3 – Transnet (2021), offer contrasting lenses through which the operational, economic, and institutional consequences of maritime cyberattacks can be evaluated. Each occurred within a different national context, targeted a distinct organisational structure, and exhibited varying levels of digital maturity and resilience. Taken together, these cases underscore a central thesis finding: the consequences of cyberattacks in the maritime sector are not uniform, and the severity of impact is shaped not solely by the nature of the malware, but by institutional readiness, governance models, and the surrounding economic environment. While all three incidents involved major logistics providers with global or regional significance, the variation in targeting, scale, and financial transparency complicates any standardised macroeconomic assessment. This reflects the challenge at the heart of the research: open-source data on maritime cyberattacks remains inadequate for consistent econometric modelling. Therefore, event base analysis becomes the alternative for illustrating the disproportionate and systemic implications of individual cyber events.

5.4.1 Different Targets, Shared Vulnerabilities

Despite differing motivations (state-sponsored sabotage in the case of Maersk, financially driven ransomware in the other two incidents), all three cases demonstrate the vulnerability of maritime logistics to digital disruption. The comparative attributes of the attacks are summarised in Table 12. Maersk as a collateral victim of NotPetya wiper, suffered global paralysis due to its highly centralised IT infrastructure. This revealed the strategic vulnerability of unsegmented networks in multinational operations. CMA CGM, directly targeted by the Ragnar Locker ransomware, experienced a contained disruption to booking platforms, that was mitigated by proactive communication and robust internal protocols. In contrast, Transnet, a state-owned enterprise operating within a lower digital maturity environment, experienced delayed recovery and long-term regional economic consequences after being attacked by the Death Kitty variant during a time of civil unrest and institutional fragility.

The comparison suggests the critical role of pre-attack resilience and institutional capacity. Maersk's and CMA CGM's post-attack recovery efforts included infrastructure overhauls and strategic investment in cybersecurity. Transnet, while eventually initiating

reforms, did so reactively and under economic duress. These dynamics illustrate the importance of both preparedness and structural governance in mitigating cyber risk. Table 12 presents a side-by-side view of key dimensions, including ownership, attacker type, scale of disruption, and known financial impact, offering a high-level synthesis of case characteristics.

Table 12 – Case study comparison

Dimension	**Maersk (2017)** (NotPetya)	**CMA CGM (2020)** (Ragnar Locker)	**Transnet (2021)** (Death Kitty)
Role	#2 (was #1 before MSC overtook it in 2022) largest container shipping company	#3 or #4 largest container shipping company	State-owned operator of South Africa's commercial ports and freight rail; strategic maritime chokepoint
Ownership and Structure	Private multinational corporation: publicly listed on Nasdaq Copenhagen (publicly traded with shareholder transparency)	Private multinational corporation: family-owned and not publicly traded (limited public financial disclosure)	State-owned enterprise; government-controlled with public service obligations and budgetary constraint
Attack type	Wiper (state-sponsored)	Ransomware (financially motivated)	Ransomware (likely financially motivated)
Targeting	Collateral victim	Directly targeted	Likely opportunistic targeting
Scale of disruption	Global – 600 sites, 76 ports, 49,000 systems affected,	Limited to booking systems and digital interfaces	National – Major container ports offline; manual operations activated
Response time	10 days of severe disruption weeks to full recovery	Two weeks IT outages Services restored in ~14 days	Core systems offline for ~7–10 days, full operational normalcy took 3+ weeks
Pre-attack resilience	High digital integration with known vulnerabilities unpatched on global network	Strong IT posture, robust internal response	Low digital maturity, underfunded infrastructure, recent civil unrest weakened resilience
Post-attack recovery	Full IT rebuild; improved cybersecurity and segmented network	Investments in digital platforms and resilience measures	Business continuity plan revised; equipment overhaul started post-attack
Financial impact	~$250–300 million; broader global economic impact in billions	< $50 million; strong financial year overall	No official number; indirect losses possibly > $2.8 billion in export earnings; just Hulamin lost $12.6 million
Broader Implications	Exposed vulnerabilities to fast spreading not targeted malware spurred industry wide cybersecurity upgrades	Awareness on ransomware attacks on logistics, prompting regulatory and resilience discussions	Exemplifies national infrastructure fragility, on low ICT development level economies
ISS scoring Boolean / Weighted	7 / 9	6 / 7.5	7 / 9.5

5.4.2 Cyber Incidents with Unequal Financial Metrics

The heterogeneity in cost reporting across the three cases is stark. Maersk reported direct losses between $250–300 million, amounting to around 1% of its annual revenue. These

costs included IT recovery, operational delays, and limited compensation to customers, but excluded broader economic effects. CMA CGM estimated losses below $50 million, though the full cost may have been diluted by record profitability and the absence of detailed disclosure due to its private ownership status. Transnet, meanwhile, disclosed no official figures. Yet, indirect losses across South Africa's trade economy are estimated at up to ZAR 50 billion (~$2.8 billion), with $12.6 million directly attributed to shipment delays experienced by Hulamin, just one single industrial client.

This asymmetry reflects differences not only in firm size or attack severity, but also in regulatory environments and reporting obligations. Publicly listed companies such as Maersk are required to disclose material losses. Privately held or state-owned firms, especially in emerging economies, face fewer such obligations, often limiting transparency. As a result, the broader systemic consequences, including disrupted trade, lost market confidence, and reputational damage, are underrepresented in quantitative analyses (although very important at macroeconomic level). As discussed in Section 4.4, this aligns with OECD observations on the disconnect between cybersecurity inputs (investment, controls) and outputs (measurable losses, resilience metrics) [134]. Cross-country comparisons are further made complicate by incompatible taxonomies, inconsistent terminology across datasets, and diverging national incident disclosure norms. These limitations indicate a structural opacity within maritime cyber incident reporting.

5.4.3 Implications of Macroeconomic Assessment

The comparison of these three case studies affirms broader implications of maritime cyberattacks beyond immediate financial loss. The events demonstrated the disruptiveness and cascading effects across trade flows, port operation, insurance markets and national economies. While the nature and scale of disclosure varied, each case underlined the understanding economic impact not solely through direct cost figures, but also operational downtime, reputational harm and strategic consequences. Table 13 illustrates, range of cost dimensions relevant to economic impact assessment, spanning from technical recovery costs to longer term reputational or brand damage. Customer attrition, and legal or insurance settlements are rarely disclosed or quantified systematically, not only in the closely studied three case but wider in the attack database events. For instance, Maersk's losses are among the few well-documented examples of a

corporate disclosure following the major cyberattack. Conversely, both CMA CGM and Transnet leave substantial data gaps, either by not reporting losses or failing to differentiate between direct and indirect consequences. This undermines the possibility of constructing sector-wide economic models based on open-source data, especially when attempts at aggregation are distorted by survivor bias, underreporting, and political factors. Although public reporting remains inconsistent, patterns across the studied cases reinforce importance of structured data for identifying systematic risk.

Table 13 – Cost dimensions and availability in case study data

Cost Type	Example Case	Estimated Ranges	Publicly Disclosed	Detailed
Direct IT recovery	Maersk, CMA CGM	$10M-$300M	Yes	Typically included in post-incident reports or earnings calls, especially for public companies
Operational downtime	Maersk, Transnet	7-14 days, global delays	Yes / no	Described in days, not quantified
Ransom payment	-	unknown	no	Even if demands were made, organisations typically avoid disclosing if payment occurred
Supply chain disruption	Transnet, Hulamin	12,6M-$2.8B (estimated)	Secondarily	These impacts are sometimes estimated by third parties, not included in attack report
Insurance, legal costs	-	Not disclosed	No	These costs are typically not disclosed publicly and often settled privately or absorbed internally
Reputational damage	All	Not quantified	No	This is intangible property, e.g. infered from share prices
Customer attrition	-	No clear data	No	Commercially sensitive data, rarely publicised
Productivity loss	All	Not standardised	No	Percentages were mentioned, but unquantifiable

5.4.4 Conclusion: Lessons from the Case Studies

The three case studies demonstrate that even almost identical attack types can yield vastly different outcomes, deepening on the institutional and economic context of the victims. Moreover, cyber incidents when they affect critical nodes within the global supply chain almost certainly produce cascading effects that remain invisible in official financial statements (could be to some extent be traced and researched manually). While Maersk's experience triggered industry-wide transformation, Transnet's case highlighted the fragility of under-resourced infrastructure in the face of digital threats. A clear pattern can be seen, that organisations with stronger governance and higher digital maturity tend to recover faster and report more transparently, supporting sectoral learning. In contrast,

entities with weaker structures and limited cyber insurance face prolonged disruption and often provide little public information. This imbalance hinders shared understanding of risk across the industry.

The findings reflect the need for better cyber practices, and better systems to record and report cyber incidents. The absence of standardised categories, mandatory reporting, and inconsistent attack attribution makes it difficult to compare incidents or assess their economic impacts. Without common frameworks and transparent data, it is nearly impossible to measure the wider consequences of maritime cyberattacks. Improving reporting standards and data sharing is not just a technical goal but a component for economic planning and risk management.

5.5 Cybersecurity Investment and Cost-Benefit Reflection

Investment in cybersecurity within the maritime sector constitutes a financial decision made under conditions of uncertainty. While the costs of cyber incidents are difficult to measure precisely, they are known to be substantial. Therefore, cybersecurity expenditure, although often intangible in its returns, can be considered cost-effective, providing critical preventive value rather than representing a sunk cost. Even though the benefits of this preventative measures, to avoiding losses remain difficult to quantify and rarely appear explicitly in financial statements.

5.5.1 Is prevention cost-effective?

Findings from the case studies demonstrate that early investment in cybersecurity and resilience measures can significantly mitigate operational and financial damage. Organisations such as Maersk and CMA CGM, which invested in strengthening digital resilience following major incidents, experienced comparatively faster recovery. Conversely, Transnet's experience illustrates how structural underinvestment can amplify the scale and duration of disruption. At the sectoral level, the merged database reveals that cyberattacks affect a diverse range of maritime entities, with no segment consistently insulated from cyber threats. While larger companies appear more frequently among reported victims, likely due to their greater visibility and digital footprint, smaller firms are also affected. However, the current database lacks consistent parameters on company size, cybersecurity maturity, or digital dependency, limiting more granular assessments of vulnerability patterns.

Digitalisation and automation in the maritime sector are often driven by competitive incentives, including the pursuit of decarbonisation targets, optimisation of routes, and overall cost reduction. Innovation solves problems. Cybersecurity, by contrast, lacks this internal momentum, it is not inherently rewarded by efficiency gains or regulatory mandates in many regions. As a result, it is frequently treated as a reactive expense rather than a proactive investment, even though, cybersecurity investments are cost-effective not only at the firm level but also essential for preserving sector-wide stability. The broader implications are including recommendations for policy, regulation, and future research, are addressed in Chapter 6.

5.6 Synthesis of Case Study Findings

The case studies presented in this chapter illustrated how maritime cyberattacks can lead to serious operational disruption and financial harm across diverse organisational contexts. While the scope and visibility of each incident varied, common patterns emerged: delayed recovery in the absence of preparedness, fragmented reporting, and a lack of consistent cost disclosure. These cases confirm that cyber risk is a shared challenge across the maritime sector, affecting both global corporations and state-owned enterprises, with impacts cascading over the maritime domain. Taken together, the analyses underscore the sector's exposure to complex, multidimensional threats that are often underestimated or poorly captured by existing data. Although quantification challenges persist, the qualitative evidence supports a clear conclusion: maritime cybersecurity must be addressed as a strategic and systemic priority. The following chapter explores the broader implications of these findings for policy, investment, and future research.

6 Discussion of Key Findings and Implications

This chapter consolidates the findings presented in Chapter 4 and 5 and situates them in their broader strategic, policy and economic contexts. It considers how the observed patterns of cyberattacks, their consequences, and the limitations in current data and governance structures inform the maritime sector's overall cyber resilience and economic exposure.

6.1 Introduction

Over recent decades, cyberattacks targeting maritime infrastructure have become more frequent, sophisticated, and impactful. What sets apart the maritime cyber threat landscape from other domains is its unique hybridity. The sector must now confront emerging digital threats, and also the convergence of cyber risks with traditional maritime hazards (natural, physical and man-made) ranging from piracy and smuggling to espionage and physical sabotage, many of which are being reconfigured or amplified in cyberspace. This evolving hybrid threat landscape is particularly challenging due to the defining characteristics of cyberspace: anonymity, asymmetry, and amplification. Threat actors can operate remotely, obscure their identities, and use relatively inexpensive tools to inflict disproportionate damage. Even modestly resourced attackers can now leverage advanced technologies, accelerating the reach and severity of incidents. However, the evidence suggests that many of the most disruptive actors in the maritime domain are, in fact, well-resourced and embedded in broader geopolitical agendas.

Notably, the analysis presented in Chapter 4 is based on data compiled prior to the major geopolitical escalations of the past three years. Even in that earlier period, state-linked actors were active in using cyber means to exert influence and disrupt maritime infrastructure. The maritime domain is increasingly being drawn into the broader cyber theatre, whether through deliberate targeting or from untargeted cyber operations. This reinforces the view that the maritime sector is not only the backbone of global trade but also a strategic asset and potential vulnerability in the context of geopolitical competition.

The following sections address how these insights map onto the research questions, the challenges of economic quantification, the role of taxonomy, and the broader implications for regulation, investment, and strategic policy development

6.2 Reflection on Research Questions

This section evaluates the extent to which the research has addressed the main research question and its four supporting sub-questions. Drawing on both the quantitative dataset analysis and the qualitative case studies presented in Chapters 4 and 5, it offers a structured response to each question. While it was not possible to construct a robust macroeconomic model due to the limitations of available data (RQ2), the documented incidents and case study findings offer valuable insights into economic disruption (RQ1), the practical value of case-based analysis (RQ3), and the challenges surrounding cybersecurity investment in a rapidly evolving sector (RQ4). Together, these reflections reinforce the study's core argument: that existing evidence although incomplete is sufficient to demonstrate the maritime sector's vulnerability and to support targeted policy and investment responses.

6.2.1 RQ1: Economic Disruption at Organisational, Sectoral, and Macroeconomic Levels

The evidence confirms that maritime cyberattacks can result in significant economic and operational disruption, at both organisational and sectoral levels. While precise macroeconomic quantification was not achievable, the examined incidents, especially the ones demonstrated in the case studies, showed that even isolated attacks can cascade through global supply chains, affecting customers, cargo flows, and pricing. For example, the Transnet ransomware attack in 2021 resulted in port closures and shipment delays, yet its broader economic impact was entangled with concurrent challenges, such as the COVID-19 pandemic and pre-existing governance gaps. This illustrates the difficulty of attributing specific economic effects to isolated cyber incidents, particularly when they coincide with other disruptions.

6.2.2 RQ2: Challenges in Quantifying the Economic Impact

Efforts to collect meaningful data on the number of maritime cyberattacks encountered substantial obstacles. Underreporting, inconsistent definitions, and lack of disclosure

across jurisdictions make reliable data collection difficult or impossible. While some estimates exist for average ransom payments and breach frequency, these are typically derived from non-public sources, rendering them unsuitable for open-source economic analysis. As explained in Section 3.9, the original plan to adapt the Thomas Murray model for sectoral cost estimation was abandoned. The absence of accessible raw data and the inability to isolate maritime-specific data and indicators from generalised national-level inputs made this approach unworkable. Open-source datasets rarely provide standardised financial metrics, particularly for privately held or smaller firms, whose reporting practices are inconsistent at best. While finding financial statements of public companies is possible, accessing precise financial data or even response plans of smaller, private organisations is seldom and random. This reflects a structural challenge: the maritime sector lacks harmonised reporting protocols that would enable longitudinal tracking, sector-specific cost aggregation, or international benchmarking.

6.2.3 RQ3: Reliability and Value of Case Studies

Despite data limitations, the selected case studies offered robust insight into the financial and operational impacts of cyberattacks. While not generalisable for statistical modelling, they revealed recurring patterns of disruption, including system outages, cargo delays, reputational damage, and recovery challenges. A key observation across the case studies is the critical role of human resilience. In all three incidents, technological restoration was important, but it was the adaptability of personnel, through manual workarounds, crisis coordination, and improvisation, that ultimately enabled timely recovery. This suggest the need to invest not only in cybersecurity infrastructure but also in organisational awareness, training, and response capacity, Ultimately the human workforce remains the most dependable fallback mechanism when digital systems fail

6.2.4 RQ4: Cost-Benefit Reflections and Sectoral Readiness

The findings suggest that while awareness of cyber threats is growing, the maritime sector still lags in terms of proactive investment. Regulatory developments such as IMO MSC.428(98), BIMCO guidelines, and IACS URs E26/E27 are gradually improving baseline resilience, but adoption remains uneven, particularly among smaller firms facing resource constraints It is also important to recognise that the sector is still undergoing digital transformations. Estimates suggest the maritime digitalisation market will grow at roughly 10% annually [130], [135]. Yet, as of 2021, only 20% of the world's 4 900 ports

had adopted or planned to adopt digital capabilities [136]. This indicates that current cyber exposure is limited to a specific, albeit expanding, segment of maritime operations.

This transitional state presents both risks and opportunities. While the continued use of manual systems and offline procedures may currently insulate certain operations from cyber threats, the sector's overall trajectory is increasingly defined by automation and digital integration. This trend introduces new vulnerabilities and will require proportionate investment in cybersecurity to mitigate the heightened exposure it creates. Most investment decisions currently prioritise efficiency gains over systemic risk mitigation, which can leave supply chains exposed to high-consequence disruptions. Coordinated public–private frameworks, mandatory incident disclosure, and improved threat intelligence sharing will be essential for better understanding and managing these emerging risks.

6.3 Barriers to Macroeconomic Modelling in the Maritime Sector

Early in the research. process a macroeconomic modelling approach was considered to estimate the economic cost cyberattacks affecting the maritime sector. This would have involved applying measurable indicators, such as the number of cyberattacks, sectoral GDP contribution, and level of digital integration to estimate economic disruption at a national or regional levels. However, as discussed in Chapter 3, the approach proved unfeasible due to limited access to source data and the absence of a suitable open-source equivalent that would allow for maritime sector-specific calculations.

The goal was to isolate the maritime sector’s role in the overall cyber-related losses and demonstrate its disproportionate exposure due to its critical infrastructure status and rising digitalisation. Efforts to identify consistent baseline data, to estimate the number of maritime cyber incidents, quickly revealed significant limitations. Open-access databases such as MCAD and ADMIRAL displayed inconsistent classifications, incomplete records, and conflicting information for identical events. Key details such as attacker identity, attack method, or cost implications were frequently missing, and incident dating and categorisation varied across sources. Cost estimates, where provided, were sparse and typically restricted to direct IT recovery, with little information on supply chain disruption, reputational damage, or productivity loss. These inconsistencies made aggregation across time periods, geographies, or incident types unreliable.

As a result, the research approach shifted to two complementary strategies: (1) conducting a structured analysis of documented maritime cyber incidents using a custom-built taxonomy and merged dataset; and (2) selecting and reconstructing high-impact case studies through cross-verification of company disclosures, academic and industry reports, and public statements. The taxonomy was developed to standardise fields across fragmented datasets and enable structured comparisons of incident characteristics, while the case studies served to ground the analysis in concrete, well-documented events where financial and operational consequences could be traced in greater depth. This dual-track approach improved analytical clarity and exposed structural limitations in current reporting practices. While the taxonomy and its incident severity scoring (ISS) enabled more systematic comparison of recorded incidents, even this method was constrained by missing or inconsistent data. The case study method, by contrast, provided richer contextual detail but remained limited in scalability. These methods, however, together offered complementary insights, but neither was capable of supporting macroeconomic extrapolation with statistical confidence.

The implications of these modelling barriers are relevant beyond academic research. In the absence of harmonised classifications and consistent financial reporting, policymakers and regulators lack enough evidence base needed to assess systemic exposure or prioritise sector-wide investment. Insurers similarly face uncertainty in pricing cyber risk, particularly when data on losses is unverifiable or unavailable. Smaller maritime operators are disproportionately affected, as the lack of comparative benchmarks weakens the case for proactive cybersecurity investment in organisations with limited financial or technical resources. This contributes to a negative feedback loop: weak reporting deters policy development, which in turn fails to create incentives for transparency or investment. Although the case studies and structured dataset analysis offer valuable insights, neither can yet capture the full scale of cyber risk facing maritime economies. Until standardised taxonomies, mandatory incident disclosure, and interoperable databases are implemented, macroeconomic impact modelling in this sector will remain speculative, and strategic decision-making will continue to rely on fragmented evidence.

6.4 Maritime Cyberattack Taxonomy: Purpose and Strategic Value

6.4.1 Development of the Taxonomy

The maritime cyberattack taxonomy was developed in direct response to the inconsistencies and fragmentation observed in existing datasets. During the merger of the MCAD and ADMIRAL databases, it became clear that only around half of the recorded incidents overlapped. Even among these, discrepancies in dates, attack classifications, and impact descriptions were frequent. It includes standardised fields for incident characteristics such as attack method, access vector, sectoral and geographical impact, and operational technology involvement. Additional dimensions capture attacker identity, motivation, human safety implications, and supply chain disruption. This supports the structured analysis of the fragmented data. To assess incident severity in a comparative manner, a complementary Incident Severity Score (ISS) model was introduced. Together, the taxonomy and ISS framework enabled structured classification, facilitated trend analysis, and improved consistency across disjointed data sources.

6.4.2 Application and Future Use

The taxonomy provides a foundational structure for future data collection, incident classification, and impact assessment in the maritime cyber domain. Its value lies in improving analytical clarity, and in supporting operational decision-making, sectoral benchmarking, and policy formulation. For practitioners and insurers, it offers a way to identify high-risk patterns and better estimate exposure. For policymakers, it reveals where reporting gaps persist and where standardisation efforts should be prioritised. Unlike generic cyber taxonomies, this structure accounts for the hybrid character of maritime systems (where IT breaches can lead to physical consequences) and enables contextual analysis across vessel operations, shore-based systems, and supply chain components.

Further development of the taxonomy, through stakeholder input, regulatory alignment, or integration with industry-specific platforms could enable its adoption as a standard for maritime cybersecurity reporting. It also offers a scalable framework for comparative incident tracking and a basis for future sector-specific risk modelling, once data quality and completeness improve.

6.5 Implications for Practice, Policy, and Future Research

6.5.1 Underinvestment and Risk Misalignment

Recurring insight throughout this research is the significant underinvestment in maritime cybersecurity relative to the sector's exposure. Despite increasing awareness of digital threats, many organisations, mostly small and medium-sized enterprises continue to allocate minimal budgets to cybersecurity, often below $100,000 annually [137]. Which is in stark contrast to the estimated average financial impact of a single cyber incident, that can exceed $550,000 (and increasing) [2]. The mismatch suggests that cybersecurity is still frequently viewed as a technical overhead rather than a core component of operational resilience. One of the main challenges in justifying increased cybersecurity investment is in the difficulty of quantifying avoided losses, to convince C level executives. Since successful attacks are easier to document than prevented ones, internal business cases for proactive investment often lack persuasive evidence. This is compounded by the absence of reliable sectoral benchmarks and limited reporting of post-incident costs. Larger firms may rely on contingency funding or insurance, while smaller actors often operate without meaningful protection. This asymmetry exacerbates systemic risk, given the sector's high interdependence: even a disruption at a low-profile logistics firm or regional terminal can trigger ripple effects across global supply chains.

Addressing this misalignment requires clearer economic justifications, and also mechanisms such as benchmarking tools or scenario-based modelling to support investment decisions. Until cybersecurity is fully recognised as a strategic necessity, underinvestment will continue to expose the sector to avoidable operational and financial disruption.

6.5.2 Incentivising Smaller Operators and Enabling Inclusion

SMEs play a vital role in the maritime ecosystem but face significant challenges in adopting comprehensive cybersecurity measures. These firms often operate with limited budgets, minimal in-house IT expertise, and competing operational demands that relegate cybersecurity to a secondary priority. Nevertheless, their operational role is critical. Disruptions affecting even modest terminals, service providers, or vessel operators can produce cascading consequences across larger supply chains. The cybersecurity readiness gap between large firms and smaller operators creates systemic vulnerabilities. While

major shipping companies may have access to advanced detection tools, dedicated response teams, and insurance mechanisms, SMEs are more likely to rely on ad hoc, reactive responses. This disparity not only weakens overall sectoral resilience but also undermines collective risk management efforts.

To address this, public and private stakeholders should consider targeted support mechanisms. These may include subsidies, cost-sharing schemes, access to shared cybersecurity services, or simplified regulatory pathways tailored to SME constraints. What is easily applicable for a large enterprise might be a burden or impossible challenge for an SME. Emerging policy frameworks such as NIS2 already acknowledge the disproportionate burden borne by smaller organisations and call for more inclusive approaches to compliance. Financial incentives can reduce the barrier to entry for adopting baseline security measures, while also encouraging participation in coordinated response networks and reporting systems. Ensuring that all maritime actors regardless of size can meaningfully contribute to and benefit from cybersecurity frameworks is essential for building a resilience and trusted interoperability.

6.5.3 Strengthening Public–Private Partnerships (PPP)

Effective maritime cybersecurity depends on sustained cooperation between public authorities and private sector stakeholders. Given the sector's complexity and global interdependence, no single actor can manage cyber risk in isolation. Port authorities, shipping companies, classification societies, regulators, and emergency responders must align their efforts through structured public–private partnerships. While coordination challenges persist, encouraging signs of progress are visible. International bodies, particularly the IMO have taken a leading role in shaping guidelines, facilitating stakeholder dialogue, and promoting awareness. Panels, advisory groups, and cross-sector initiatives are increasingly involving both industry representatives and policymakers to define shared objectives and foster trust.

Although the tangible impact of these efforts remains difficult to quantify in the short term, the foundational structures for durable cooperation are gradually taking shape. What is now required is sustained commitment. The sector must move toward a governance model where cybersecurity is embedded within corporate culture, rather than treated as an external compliance obligation. True resilience will not emerge from regulation or technical solutions alone. It depends on collective responsibility where public and private

actors, regardless of size or jurisdiction, recognise their shared role in securing the maritime domain.

6.6 Regulatory Gaps and Policy Barriers

Past decade has witnessed steady progress in global maritime cybersecurity governance, spanning shipping, logistics, and port operations. The IMO has led several initiatives, including integrating cyber risk management into the International Safety Management (ISM) Code's framework. IMO Resolution MSC.428(98) (2017) urges all shipping companies to incorporate cyber risk controls into their Safety Management Systems, effectively making cybersecurity part of mandatory ship safety certification since 2021. Complementing this, IMO issued industry guidelines (MSC-FAL.1/Circ.3) and worked with stakeholders to promote best practices. Industry groups have also rallied to improve resilience: the Baltic and International Maritime Council (BIMCO) and other bodies jointly published the Guidelines on Cyber Security Onboard Ships to help standardise defences in line with IMO's recommendations [29], [36], [138].

Beyond shipping, regional and national regulatory frameworks have evolved to strengthen cyber resilience across port and logistics infrastructure. The European Union's Network and Information Systems (NIS) directives now impose baseline cybersecurity obligations on critical maritime operations, supported by sector-specific guidance from ENISA. Similarly, leading maritime nations have updated national legislation (e.g., U.S. Maritime Transportation Security Act) to account for digital threats to port facilities. At the international level, cooperation has also improved. Organisations like INTERPOL and Europol have developed cyber threat intelligence channels, and regional initiatives such as the European Maritime Security Network facilitate cross-border incident coordination and emergency response. These developments represent important steps toward a more secure digital maritime ecosystem [139].

Nevertheless, the global regulatory framework remains fragmented and incomplete. A foremost issue is the lack of a unified international legal instrument dedicated to maritime cyber threats. Most IMO measures are largely guidance-based or appended to existing safety codes, rather than a binding convention [139]. This leads to inconsistent implementation: while IMO's ISM Code amendment addresses shipboard cyber risk, there is no equivalent enforceable standard covering shore-based port systems and the

wider maritime supply chain, leaving major part of logistics infrastructure under-protected in many jurisdictions.

Enforcement mechanisms are also uneven and often reliant on decentralised oversight. IMO's cyber risk management resolution relies on flag states and port state control for enforcement, resulting in variable compliance across different regions [140]. Many provisions remain essentially voluntary or subject to interpretation; for instance, classification societies have introduced cybersecure ship design rules for new vessels, but these do not apply retroactively to the vast number of existing ships, creating a protection gap in the global fleet [141]. Incident reporting practices are similarly inconsistent. There is no global requirement for disclosing maritime cyber incidents, nor any standardised registry or information-sharing protocol. As a result, opportunities to learn from incidents are frequently lost, and emerging threats may go undetected at the system level. This uneven regulatory landscape results in "weak links" across the maritime supply chain. While some nations and major operators have implemented advanced cyber protocols, others continue to lack even basic protections. The diversity of actors in the sector translates into widely varying levels of awareness, funding, and preparedness. Smaller shipping companies and port operators often operate without dedicated IT or cybersecurity staff, and studies continue to highlight low levels of cybersecurity training among maritime personnel [139]. The skills gap and limited capacity mean that even where guidelines exist, they may not be effectively implemented by all stakeholders.

Economic pressures further complicate adoption. In a competitive and cost-sensitive industry, companies may defer cybersecurity upgrades unless they are explicitly required. In parallel, the prevailing culture of secrecy around incidents discourages transparency. Operators often fear reputational damage, regulatory scrutiny, or legal liability, and therefore underreport breaches. This obstructs industry-wide learning and hinders the development of a shared understanding of evolving threats [141]. The rapid evolution of cyber threats outpaces traditional regulatory cycles, not only in the maritime domain, but across many sectors. Technologies used in navigation, cargo management, and communications are advancing quickly, and attackers adapt just as fast. The IMO has acknowledged the fast-changing digital risks are difficult to manage through static technical standards alone. Meaning that even where policies are in place, they must be continually updated and coordinated globally. As a response, it has launched the Strategy on Maritime Digitalization, which seeks to coordinate global efforts around digital

infrastructure, including cybersecurity [142].[142] This initiative This strategy invites participation from member states and industry stakeholders and aims to establish a more cohesive digital governance model. However, longstanding obstacles as jurisdictional complexity, unequal national capacities, limited data sharing, and the accelerating speed of technological innovation continue to limit implementation.

Closing these regulatory gaps will require a shift from voluntary guidelines to enforceable, harmonised frameworks. Maritime cybersecurity must evolve beyond technical compliance toward integrated, cross-sector governance mechanisms. Until then, the sector will remain vulnerable to fragmented oversight, misaligned incentives, and under-preparedness in the face of increasingly complex threats.

6.6.1 Standardisation and Framework Harmonisation

One of the most effective ways to improve maritime cybersecurity at scale is through the adoption and harmonisation of structured cybersecurity frameworks. Existing initiatives as BIMCO's *Guidelines on Cyber Security Onboard Ships*, and the IACS *Unified Requirements E26 and E27* offer outcome-based approaches tailored to the unique IT-OT convergence found in maritime operations. These frameworks provide valuable guidance on governance, risk controls, asset protection, and recovery planning. However, the implementation of these remains uneven. While major operators may have the capacity to integrate these frameworks, many smaller firms lack the technical expertise or financial resources to do so effectively. Compounding this challenge is the absence of global enforcement. Most frameworks remain non-binding, and without formal regulatory backing, their uptake is left to voluntary compliance, leading to fragmented levels of preparedness across the sector.

The trend toward stronger regulatory coordination is gaining momentum. The European Union's NIS2 Directive, for example, expands the scope of cybersecurity obligations to include key maritime infrastructure and enforces stricter requirements for risk management and incident response. While similar legislation is not yet uniformly adopted worldwide, this movement signals a growing consensus that cybersecurity frameworks must shift from being optional guidance to enforceable standards. To support the broader uptake, frameworks must be accompanied by targeted implementation support. This includes training, awareness campaigns, and technical toolkits tailored to different organisational capacities. Regional harmonisation efforts, especially when supported by

port authorities and flag states will also reduce regulatory fragmentation and promote cross-border operational consistency.

6.6.2 Mandatory Reporting and Threat Intelligence Sharing

Mandatory cyber incident reporting is the enabler for improving collective maritime cybersecurity. It improves visibility into emerging threats, facilitates intelligence sharing, and supports, sector-wide learning from both successful defences and failures. However, current reporting practices across the maritime sector are highly inconsistent. Many organisations, especially the ones outside regulated jurisdictions such as the EU face no binding obligation to disclose incidents. As a result, underreporting remains widespread. Even when incidents are disclosed, the level of detail varies widely, and post-incident assessments often omit financial losses, system vulnerabilities, or lessons learned. This limits the maritime sector's collective ability to detect patterns, anticipate emerging threats, and prevent repeat incidents.

Regulatory developments (e.g., NIS2 Directive) mark a shift toward enforced reporting for operators of essential services, including ports and shipping firms. Early effects of these mandates are visible in improved data availability in maritime-focused databases. However, challenges remain. Smaller operators may hesitate to report incidents due to concerns over reputational damage or legal consequences. Inconsistent definitions of what constitutes a reportable cyber event further complicate compliance. To address these gaps, reporting mechanisms should be formalised, standardised, and made proportional to organisational capacity. Anonymised or confidential reporting channels may help overcome reluctance by protecting commercially sensitive information. Clear safeguards should be embedded into reporting frameworks to protect companies from undue liability or competitive disadvantage.

A culture of trusted information sharing supported by policy, industry associations, and regulators would not only improve maritime cybersecurity but also contribute to broader situational awareness across critical infrastructure sectors. Cross-sectoral and cross-border data exchange has increasing importance in a threat environment where attackers exploit interdependencies and jurisdictional blind spots. In the long term, establishing an international, centralised maritime cyber incident registry could be a major step forward. Until then, stronger national mandates and regional cooperation can help closing the sector's intelligence gaps and aligning response capabilities with evolving risks.

6.6.3 Embedding Cyber Resilience into Maritime Governance

For maritime cybersecurity to be effective in the long term, it must be fully integrated into the sector's broader governance structures, risk management practices, and operational planning. Cyber risk should not be treated as a niche concern managed solely by IT departments but must be embedded into safety management systems, port operations protocols, continuity planning, and regulatory compliance frameworks. The IMO's Resolution MSC.428(98) was a step in this direction. It requires shipping companies to include cyber risk in their Safety Management Systems, linking cybersecurity to core safety responsibilities. Similar changes are being made at national and EU levels to better protect critical infrastructure

However, as this study's analysis of the merged dataset shows, practical implementation of these requirements remains inconsistent. In some cases, cyber preparedness exists only on paper, with limited operational translation. Embedding resilience means creating a culture in which cybersecurity is viewed not as a one-time compliance task but as a dynamic, evolving responsibility. This includes regular training, scenario testing, and alignment with physical safety protocols. As digitalisation expands across port infrastructure and vessel operations, building cyber preparedness into the DNA of maritime governance will be essential to maintaining continuity, safeguarding human life, and protecting global trade.

7 Limitations and Challenges

This study encountered several limitations that constrain the generalisability and scope of its findings. The most significant challenge was the limited availability of structured, verified, and financially detailed cyber incident data in the maritime sector. Both datasets used only contain publicly disclosed incidents and display inconsistencies in classification, attribution, and depth of reporting. As a result, the initial scope and direction of the thesis were changed.

Despite careful refinement, extension and categorisation, the merged dataset remained insufficient in volume and consistency to support robust quantitative or macroeconomic modelling. The methodological differences between the source databases introduced further analytical constraints (hence the development of the taxonomy) and turning towards a primarily qualitative approach. Consequently, the original aim to estimate the macroeconomic cost of maritime cyberattacks was reframed to investigate whether such estimation is even feasible.

While selected case studies are valuable for illustrating real-world impact, they are inherently limited in statistical generalisability. The analysis was further constrained by the absence of post-incident financial disclosure standards and the limited availability of long-term economic follow-up data. While incorporating more case studies or interviews or primary data collection from affected companies could have enhanced the granularity and representativeness of case studies, or enhancing the merged database, this was deemed beyond the feasible scope of the current research. The thesis relied on publicly verifiable, secondary sources to maintain transparency and reproducibility. Future studies could build on this foundation through fieldwork or industry surveys.

Language bias in open-source data (English and French predominating in the two main source dataset), differences in regulatory reporting obligations across jurisdictions, and the absence of standardised impact metrics also restricted the comprehensiveness of the study. These limitations point to a broader issue: the maritime sector lacks data infrastructure incentives required for systematic economic impact assessment.

8 Conclusion, Recommendations and Future Work

8.1 Conclusion

This thesis set out to examine whether the macroeconomic consequences of cyberattacks on the maritime sector can be calculated using existing data, and whether current open-source incident records are sufficient to support such analysis. Based on the findings the answer is clear: while the economic impact of maritime cyberattacks is undeniably substantial, current data infrastructure is too fragmented, inconsistent, and incomplete to support reliable macroeconomic modelling. The original plan to apply econometric methods was therefore abandoned in favour of a case-based and taxonomy-driven analysis is more appropriate for the available data. In response to the limitations, the thesis introduced a structured maritime cyberattack taxonomy, designed to address inconsistencies in incident classification and improve comparability across records. This taxonomy, combined with an Incident Severity Score model, enabled a more systematic assessment of impact at the organisational and sectoral levels. While generalisable financial quantification proved unfeasible, the structured analysis revealed recurring patterns of disruption, particularly in cases involving operational technology and supply chain dependencies.

Ultimately, this research contributes to the emerging field of maritime cybersecurity by offering a practical classification framework, highlighting the sector's data shortcomings, and proposing actionable directions for improving future risk assessment. The findings suggest the need for standardised reporting and coordinated response strategies, not only for research purposes, but for informed policymaking and strategic investment across the maritime domain.

8.2 Recommendations for Future Work

Future research should prioritise improving the quality, availability, and consistency of maritime cyber incident data. A key step toward this goal is the development of interoperable and open-access databases that include not only technical characteristics of

incidents but also financial metrics, long-term impacts, and organisational responses, supply chain interdependencies. Such datasets should adopt standardised taxonomies for comparability across jurisdictions and over time.

Sector-specific economic models are also needed to capture the cascading and systemic effects of cyberattacks. These models should account for supply chain interdependencies, temporal disruptions, and cross-sectoral spillovers that are typically absent from firm-level impact assessments. In addition, future studies should explore underreported or blended threat types, particularly those involving cyber-physical convergence, and refine attribution techniques to better understand the role of state-sponsored actors, organised crime, and insider threats. Threat actors of the maritime moving towards the cyberspace will heighten the number of cyber assisted incidents. Also, threats that are not cyber but preventable through cyber means are optionally area to investigate.

Another important direction is to study the "silent" segment of the maritime sector, organisations that have neither experienced nor reported cyber incidents. Understanding their exposure levels, security practices, and reasons for non-disclosure could offer valuable insights into unquantified risks and barriers to reporting. As maritime digitalisation accelerates, further work should track the evolution of cyber exposure across the sector. This includes relationship between ICT maturity, maritime digital transformation, and national economic dependency on maritime trade. Only a small fraction of the world's ports has reached high levels of digital maturity, but this is changing rapidly [136]. Forecasting how increasing interconnectivity affects systemic risk for designing pre-emptive cybersecurity policies. Anticipating future risks will be essential for shaping proactive, evidence-based maritime cybersecurity strategies.

Additionally, the use of AI and large language models (LLMs) to support in maritime cyber incident analysis should be further explored. However, effective use of these technologies requires well-structured, standardised, and categorised input data. At present, the inconsistent terminology and incomplete documentation limit the potential of AI tools. Developing harmonised data taxonomies and comprehensive lifecycle documentation for each incident would allow for automated trend detection, severity forecasting, and correlation mapping between cyber events and geopolitical dynamics.

Finally, future research could also focus on mapping systemic vulnerabilities across the global maritime economy, particularly in regions with low ICT maturity and poor regulatory coverage. This includes approximating the types of maritime assets most frequently targeted and evaluating the resilience of digital infrastructure across varied operational contexts. Finally, studies should explore the organisations characteristics that enable effective cyber governance, particularly among entities that successfully withstood or mitigated severe cyberattacks. These examples may offer transferable lessons for broader resilience-building and informed regulatory design

9 Summary

This thesis set out to investigate whether the macroeconomic consequences of cyberattacks on the maritime sector can be meaningfully assessed using currently available data. Motivated by the sector's increasing digitalisation and critical role in global trade, the research aimed to quantify economic impact through a structured, data-driven approach. However, the lack of accessible, standardised, and financially detailed cyber incident records necessitated a shift in methodology. In response, the study developed a custom taxonomy for maritime cyberattacks and introduced an Incident Severity Score (ISS) model to support structured analysis of publicly documented incidents. These tools enabled the identification of recurring attack patterns and sector-specific vulnerabilities, especially in cases involving operational technology, supply chain disruption, and underprepared organisational responses. Complementing this, in-depth case studies provided concrete illustrations of economic and operational impact, although their limited generalisability precluded robust macroeconomic modelling.

The research concludes that while the economic effects of maritime cyberattacks are substantial, current open-source data is insufficient for reliable quantitative estimation at a global level. Fragmentation, underreporting, and the absence of standardised cost metrics hinders the transparency and strategic risk assessment. Nevertheless, the tools developed in this study offer a practical foundation for improved data classification, cross-case comparison, and future sectoral risk modelling. Beyond academic insight, this thesis highlights the need for regulatory harmonisation, mandatory incident reporting, and inclusive cybersecurity investment strategies. It also points to key directions for future research, including the development of interoperable databases, sector-specific economic models, and AI-assisted analytics. As maritime digital transformation accelerates, addressing these gaps will be increasingly important to enhancing global cyber resilience, protecting critical infrastructure, and ensuring the continuity of maritime trade in an increasingly contested digital landscape.

References

[1] World Economic Forum, “These are the world’s most vital waterways for global trade”, Feb. 15, 2024. Available: https://www.weforum.org/stories/2024/02/worlds-busiest-ocean-shipping-routes-trade/. [Accessed: Nov. 03, 2024]

[2] CyberOwl, HFW, and Thetius, “Shifting Tides, Rising Ransoms: The State of Cyber Security in the Maritime Industry”, Oct. 2023. Available: https://cyberowl.io/wp-content/uploads/2023/10/CyberOwl_HFW_Thetius-Cyber-Security-Report-2023-Shifting-Tides-Rising-Ransoms.pdf. [Accessed: Aug. 06, 2024]

[3] I. N. Putra, A. Octavian, A. K. Susilo, and Y. N. Santosa, “Assessment of Cyber Resilience in the Maritime Domain Using System Dynamics and Analytical Hierarchy Process (AHP)”, *Trans. Marit. Sci.*, vol. 13, no. 2, Jun. 2024, doi: 10.7225/toms.v13.n02.w06. Available: https://www.toms.com.hr/index.php/toms/article/view/642. [Accessed: Apr. 17, 2025]

[4] C. Senarak, “Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases”, *Marit. Econ. Logist.*, vol. 26, no. 1, pp. 105–130, Mar. 2024, doi: 10.1057/s41278-023-00276-8

[5] A. Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History”, *Wired*. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [Accessed: Mar. 21, 2025]

[6] Thomas Murray, “Calculating the cost of cyber attacks: an economic analysis of the worldwide impact”, Feb. 2024. [Online]. Available: https://thomasmurray.com/insights/calculating-cost-cyber-attacks. [Accessed: Apr. 13, 2024]

[7] R. Dieye, A. Bounfour, A. Ozaygen, and N. Kammoun, “Estimates of the macroeconomic costs of cyber-attacks”, *Risk Manag. Insur. Rev.*, vol. 23, no. 2, pp. 183–208, Jun. 2020, doi: 10.1111/rmir.12151.

[8] J. M. Lane and M. Pretes, “Maritime dependency and economic prosperity: Why access to oceanic trade matters”, *Mar. Policy*, vol. 121, p. 104180, Nov. 2020, doi: 10.1016/j.marpol.2020.104180

[9] M. Herrera Dappe, C. Jooste, and A. Suárez-Alemán, *How Does Port Efficiency Affect Maritime Transport Costs and Trade? Evidence from Indian and Western Pacific Ocean Countries*. in Transport and ICT Global Practice Group. Washington, DC: World Bank, 2017. doi: 10.1596/1813-9450-8204. Available: https://hdl.handle.net/10986/28447. [Accessed: Mar. 12, 2025]

[10] PricewaterhouseCoopers (PwC), “Transportation & Logistics 2030 Volume 4: Securing the Supply Chain”, 2011. [Online]. Available: https://www.pwc.com/gx/en/transportation-logistics/pdf/supply-chain-security-2030.pdf. [Accessed: Mar. 07, 2025].

[11] R. Ottis and P. Lorents, “Cyberspace: Definition and Implications”, Cooperative Cyber Defence Centre of Excellence, Reading, UK, 2010. [Online]. Available:

https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/. [Accessed: Mar. 10, 2025].
[12] eMSP NBSR Consortium, “Addressing the Fragmentation of Ocean Governance Across Borders”, eMSP NBSR Project, Policy Brief, Jan. 2024. Available: https://www.emspproject.eu/wp-content/uploads/2024/01/Ocean-Governance-Policy-Brief-eMSP-NBSR-January-2024.pdf. [Accessed: Mar. 08, 2025]
[13] R. Sen, “Cyber and Information Threats to Seaports and Ships”, Elsevier, 2016, pp. 281–302. doi: 10.1016/B978-0-12-803672-3.00009-1. Available: https://linkinghub.elsevier.com/retrieve/pii/B9780128036723000091. [Accessed: Apr. 14, 2024]
[14] DNV, “*Maritime Cyber Priority 2023: Staying Secure in an Era of Connectivity*”, DNV, Jun. 2023. Available: https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023/. [Accessed: May 01, 2024]
[15] GTA NSW, “Mapping the World’s Key Maritime Choke Points”, Geography Teachers’ Association of New South Wales, New South Wales, Australia, Educational Map Brief, Sep. 2021. Available: https://www.gtansw.org.au/wp-content/uploads/2021/09/Mapping-the-Worlds-Key-Maritime-Choke-Points.pdf. [Accessed: Mar. 10, 2025]
[16] S. Editor, “Ever Given: The grounding that changed the world’s view of shipping”, *SAFETY4SEA*, Mar. 28, 2023. Available: https://safety4sea.com/cm-ever-given-the-grounding-that-changed-the-worlds-view-of-shipping/. [Accessed: Dec. 10, 2024]
[17] M. Li, J. Zhou, S. Chattopadhyay, and M. Goh, “Maritime Cybersecurity: A Comprehensive Review”. arXiv, Sep. 09, 2024. Available: http://arxiv.org/abs/2409.11417. [Accessed: Oct. 22, 2024]
[18] Maritime Reporter TV, *Cyber Security in the Maritime Sector - What You Need to Know Now*, YouTube, Jan. 09, 2025. Available: https://www.youtube.com/watch?v=TowS1G-kmPQ. [Accessed: May 08, 2025]
[19] D. Heering, O. M. Maennel, and A. N. Venables, “Shortcomings in cybersecurity education for seafarers”, in *Developments in Maritime Technology and Engineering*, 1st ed.London: CRC Press, 2021, pp. 49–61. doi: 10.1201/9781003216582-06. Available: https://www.taylorfrancis.com/books/9781003216582/chapters/10.1201/9781003216582-06. [Accessed: Mar. 13, 2025]
[20] D. C. Chupkemi and K. Mersinas, “Challenges in Maritime Cybersecurity Training and Compliance”, *J. Mar. Sci. Eng.*, vol. 12, no. 10, p. 1844, Oct. 2024, doi: 10.3390/jmse12101844
[21] “2024 Cybersecurity Skills Gap Global Research Report”, *Fortinet*. Available: https://www.fortinet.com/resources/reports/cybersecurity-skills-gap. [Accessed: Mar. 13, 2025]
[22] A. Oruc, N. Chowdhury, V. Gkioulos, and S. Katsikas, “Evaluation of Maritime Cyber Security (MarCy) Training Programme”, *TransNav Int. J. Mar. Navig. Saf. Sea Transp.*, vol. 18, no. 4, pp. 743–763, 2024, doi: 10.12716/1001.18.04.01
[23] International Maritime Organization (IMO), “International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)”. Available: https://www.imo.org/en/ourwork/humanelement/pages/stcw-conv-link.aspx. [Accessed: Mar. 13, 2025]
[24] International Maritime Organization (IMO), “Maritime Cyber Risk”, *IMO*. Available: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx. [Accessed: Mar. 13, 2025]

[25] DNV, “Maritime Cyber Security Awareness E-learning”, *DNV*. Available: https://www.dnv.com/maritime/maritime-academy/cyber-security-elearning/. [Accessed: Mar. 13, 2025]
[26] Maritime Institute of Technology and Graduate Studies (MITAGS), “Maritime Cybersecurity Training”, *MITAGS*. Available: https://www.mitags.org/maritime-cybersecurity-courses/. [Accessed: Mar. 13, 2025]
[27] Cyber Risk GmbH, “Maritime Cybersecurity Trained Professional (MarCybTPro) Program”. Available: https://www.maritime-cybersecurity.com/MarCybTPro_Training.html. [Accessed: Mar. 13, 2025]
[28] Tallinn University of Technology, “Estonian Maritime Academy”, *TalTech*. Available: https://taltech.ee/en/estonian-maritime-academy. [Accessed: Mar. 13, 2025]
[29] BIMCO, “The Guidelines on Cyber Security Onboard Ships”, BIMCO, Lyngby, Denmark, 4th ed, 2017. Available: http://www.icsshipping.org/docs/defaultsource/resources/safety-security-and-operations/guidelineson-cybersecurity-onboard-ships.pdf
[30] C. Sungbaek, O. Erwin, V. Gabor, and Vasco PRATES, “Cybersecurity Considerations in Autonomous Ships”, Sep. 2022. [Online]. Available: Cybersecurity_Considerations_in_Autonomous_Ships.pdf. [Accessed: Mar. 07, 2025]
[31] G. Visky, A. Rohl, R. Vaarandi, S. Katsikas, and O. M. Maennel, “Hacking on the High Seas: How Automated Reverse-Engineering Can Assist Vulnerability Discovery of a Proprietary Communication Protocol”, presented at the 2024 IEEE 49th Conference on Local Computer Networks (LCN), IEEE Computer Society, Oct. 2024, pp. 1–7. doi: 10.1109/LCN60385.2024.10639746. Available: https://www.computer.org/csdl/proceedings-article/lcn/2024/10639746/2067mnN8WSk. [Accessed: Oct. 09, 2024]
[32] W. Loomis, V. V. Singh, G. C. Kessler, and X. Bellekens, “Signaling for Cooperation on Maritime Cybersecurity” [Online]. Available: https://www.garykessler.net/maritimecyber.html. [Accessed: March 18, 2025].
[33] M. Schwarz, M. Marx, and H. Federrath, “A Structured Analysis of Information Security Incidents in the Maritime Sector”. arXiv, Dec. 13, 2021. doi: 10.48550/arXiv.2112.06545. Available: http://arxiv.org/abs/2112.06545. [Accessed: Feb. 05, 2025]
[34] M. Usman, A. Khan, and S. Amjad, “Implications of Transnational Crime on Maritime Jurisdiction and Enforcement”, *Int. Rev. Soc. Sci.*, vol. 9, no.4 pp. 456-467, Apr. 2021, [Online]. Available: https://www.researchgate.net/publication/376406492_Implications_of_Transnational_Crime_on_Maritime_Jurisdiction_and_Enforcement. [Accessed: March 18, 2025]
[35] International Maritime Organization (IMO), “Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems”, International Maritime Organization, MSC.428(98), Jun. 2017. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. [Accessed: Mar. 09, 2025]
[36] IMO, “The International Safety Management (ISM) Code”. Available: https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx. [Accessed: Apr. 17, 2025]
[37] “NIS2 Directive | Prepare Your Organization Now”, *The NIS2 Directive*.[Online]. Available: https://nis2directive.eu/. [Accessed: Apr. 17, 2025]

[38] IACS, “Addressing cyber resilience of ships - Press - IACS”, *Safer and Cleaner Shipping - IACS*. Available: https://iacs.flumeserver.co.za/news/iacs-ur-e26-and-e27-press-release/. [Accessed: May 06, 2025]
[39] DNV, “Tackling a Growing Cybersecurity Threat in an Increasingly Connected Industry”, *DNV - Maritime Impact*, Dec. 12, 2024. Available: https://www.dnv.com/expert-story/maritime-impact/tackling-a-growing-cybersecurity-threat-in-an-increasingly-connected-industry/. [Accessed: Mar. 14, 2025]
[40] J. Welch, “Understanding Cybersecurity in the Barge Transport Industry”, *BargeOps*, May 10, 2024. Available: https://bargeops.com/understanding-cybersecurity-in-the-barge-transport-industry/. [Accessed: Mar. 13, 2025]
[41] A. Oruc, G. Kavallieratos, V. Gkioulos, and S. Katsikas, “Cyber Risk Assessment for SHips (CRASH)”, *TransNav Int. J. Mar. Navig. Saf. Sea Transp.*, vol. 18, no. 1, pp. 115–124, Mar. 2024, doi: 10.12716/1001.18.01.10
[42] I. Progoulakis, I. K. Dagkinis, A. Dimakopoulou, T. Lilas, N. Nikitakos, and P. M. Psomas, “Cyber–Physical Security Assessment for Maritime Vessels: Study on Drillship DP System Using American Petroleum Institute Security Risk Analysis and Bow-Tie Analysis”, *J. Mar. Sci. Eng.*, vol. 12, no. 10, p. 1757, Oct. 2024, doi: 10.3390/jmse12101757
[43] Fortune Business Insights, “Cybersecurity Market Size, Share, Analysis | Global Report 2032”, Fortune Business Insights, Apr. 2025. Available: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165. [Accessed: Mar. 20, 2025]
[44] DNV, “Maritime appetite for cyber risk notably higher than other key industries, new report reveals”, *DNV*, Nov. 13, 2024. Available: https://www.dnv.com/news/maritime-appetite-for-cyber-risk-notably-higher-than-other-key-industries-new-report-reveals/. [Accessed: Feb. 09, 2025]
[45] F. Macdonald, “The Challenging Relationship of Cyber Security and Insurance”, *Thetius*, Dec. 06, 2023. Available: https://thetius.com/the-challenging-relationship-of-cyber-security-and-insurance/. [Accessed: Mar. 20, 2025]
[46] “From strategy to implementation: a short guide to the Identity Governance and Administration (IGA) roadmap”, *DNV*. Available: https://www.dnv.com/cyber/insights/articles/From-strategy-to-implementation-a-short-guide-to-the-identity-governance-and-administration-iga-roadmap/. [Accessed: Mar. 20, 2025]
[47] European Union Agency for Cybersecurity., *ENISA threat landscape: transport sector (January 2021 to October 2022) : March 2023*. LU: Publications Office, 2023. Available: https://data.europa.eu/doi/10.2824/553997. [Accessed: Mar. 26, 2025]
[48] P. Há. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, “A Retrospective Analysis of Maritime Cyber Security Incidents”, *TransNav Int. J. Mar. Navig. Saf. Sea Transp.*, vol. 15, no. 3, pp. 519–530, 2021, doi: 10.12716/1001.15.03.04
[49] 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, p. 119078, Nov. 2024, doi: 10.1016/j.oceaneng.2024.119078
[50] M. V. Clavijo Mesa, C. E. Patino-Rodriguez, and F. J. Guevara Carazas, “Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and

Defenses in Maritime Supply Chains", *Information*, vol. 15, no. 11, p. 710, Nov. 2024, doi: 10.3390/info15110710
[51] A. Oruc, "Claims of State-Sponsored Cyberattack in the Maritime Industry," in P*roc. 15th Int. Naval Eng. Conf. Exhib*. (INEC 2020), Delft, The Netherlands, Oct. 2020. [Online]. Available: https://www.researchgate.net/publication/344570028_Claims_of_State-Sponsored_Cyberattack_in_the_Maritime_Industry. [Accessed: March 7, 2025]. doi: 10.24868/issn.2515-818X.2020.021
[52] E. F. Horsley, "State-Sponsored Ransomware Through the Lens of Maritime Piracy," Ga. J. Int'l & Comp. L., vol. 47, no. 3, pp. 669–681, 2019. [Online]. Available: https://digitalcommons.law.uga.edu/gjicl/vol47/iss3/8/. [Accessed: March 7, 2025].
[53] N. Shereikis, "Above Us Only Stars", *C4ADS*, Mar. 26, 2019. Available: https://c4ads.org/reports/above-us-only-stars/. [Accessed: Mar. 20, 2025]
[54] "EASA updates advisory on navigation interference", *GPS World*, Jul. 09, 2024. Available: https://www.gpsworld.com/easa-updates-advisory-on-navigation-interference/. [Accessed: Apr. 17, 2025]
[55] GPS jamming, "GPS jamming 27.2.2025". Available: https://gpsjam.org/?lat=45.00000&lon=35.00000&z=3.0&date=2025-02-27
[56] John Wiseman (@lemonodor), "GPS interference". Available: https://gpsjam.org/faq#what-exactly-does-this-map-show
[57] "International - U.S. Energy Information Administration (EIA)". Available: https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints. [Accessed: Mar. 20, 2025]
[58] C. Pownall, "The Context and Impact of Maersk's NotPetya Cyber Attack", Jun. 2019. Available: https://www.researchgate.net/publication/346080185_The_Context_and_Impact_of_Maersk's_NotPetya_cyber_attack
[59] NHL Stenden University of Applied Sciences, "Maritime Cyber Attack Database (MCAD)", *Maritime Cybersecurity*, May 06, 2025. Available: https://maritimecybersecurity.nl/. [Accessed: Mar. 06, 2025]
[60] M. P. Fischerkeller and R. J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation".
[61] "MTS-ISAC | maritime cybersecurity", *MTS-ISAC*. Available: https://www.mtsisac.org. [Accessed: May 09, 2025]
[62] "CSO Alliance - North". Available: https://www.nepia.com/articles/cso-alliance/. [Accessed: May 09, 2025]
[63] "Coast Guard Maritime Industry Cybersecurity Resource Website". Available: https://www.uscg.mil/MaritimeCyber/. [Accessed: May 07, 2025]
[64] Maritime Computer Emergency Response Team (M-CERT), "ADMIRAL: Advanced Dataset of Maritime Cyber Incidents Released for Literature". Oct. 29, 2024. Available: https://www.m-cert.fr/admiral/. [Accessed: Feb. 04, 2025]
[65] J. Pijpker, S. McCombie, S. Johnson, R. Loves, and G. M. Makrakis, "An Open-Source Database of Cyberattacks on the Maritime Transportation System". Oct. 25, 2024. doi: 10.20944/preprints202410.1996.v1. Available: https://www.preprints.org/manuscript/202410.1996/v1. [Accessed: Mar. 07, 2025]
[66] P. Dreyer, B. R. Jackson, D. K. Boudreaux, P. S. Steinberg, and J. Oberholtzer, *Estimating the Global Cost of Cyber Risk,* RAND Corporation, Santa Monica, CA, USA, Research Report RR-2299-WFHF, 2018. [Online]. Available:

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2299/RAND_RR2299.pdf. [Accessed: Apr. 11, 2024].
[67] P. J. Fell, N. de Vette, S. Gardó, B. Klaus, and J. Wendelborn, "Towards a framework for assessing systemic cyber risk", European Central Bank, Financial Stability Review – Special Feature, Nov. 2022. Available: https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html
[68] G. A. Weaver, B. Feddersen, L. Marla, D. Wei, A. Rose, and M. Van Moer, "Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach", *Transp. Res. Part C Emerg. Technol.*, vol. 137, p. 103423, Apr. 2022, doi: 10.1016/j.trc.2021.103423
[69] K. Tam, B. Chang, R. Hopcraft, K. Moara-Nkwe, and K. Jones, "Quantifying the econometric loss of a cyber-physical attack on a seaport", *Front. Comput. Sci.*, vol. 4, Jan. 2023, doi: 10.3389/fcomp.2022.1057507. Available: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2022.1057507/full. [Accessed: Oct. 22, 2024]
[70] O. Soner, G. Kayisoglu, P. Bolat, and K. Tam, "An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors", *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, p. 1748006X241283093, Oct. 2024, doi: 10.1177/1748006X241283093
[71] A. Turner, S. J. McCombie, and A. J. Uhlmann, "Editorial: The impacts of cyber threat in the maritime ecosystem", *Front. Comput. Sci.*, vol. 6, p. 1378160, Feb. 2024, doi: 10.3389/fcomp.2024.1378160
[72] R. Ottis, "Conflict in Cyberspace", in *Routledge Handbook of the Future of Warfare*, 1st ed.London: Routledge, 2023, pp. 411–420. doi: 10.4324/9781003299011-43. Available: https://www.taylorfrancis.com/books/9781003299011/chapters/10.4324/9781003299011-43. [Accessed: Mar. 11, 2025]
[73] "Fleet of approximately 100 Chinese flagged 'Squid jiggers' fishing vessels going dark in Argentina's EEZ", *MCAD*. Available: https://maritimecybersecurity.nl/incident/eP5ox1L63y. [Accessed: Feb. 15, 2025]
[74] "Global number of cyberattacks 2023", *Statista*. Available: https://www.statista.com/forecasts/1485031/cyberattacks-annual-worldwide. [Accessed: Apr. 03, 2025]
[75] S. LaGrone, "U.S. Pays Philippines $1.97 million for Reef Damage from Guardian Grounding", *USNI News*, Feb. 18, 2015. Available: https://news.usni.org/2015/02/18/u-s-pays-philippines-1-97-million-reef-damage-guardian-grounding. [Accessed: Apr. 18, 2025]
[76] "CNA Financial Paid $40 Million in Ransom After March Cyberattack", *Bloomberg.com*, May 20, 2021. Available: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack. [Accessed: Apr. 18, 2025]
[77] J. Burt, "Carnival Cruises agrees to pay $6m+ after cyberattacks". Available: https://www.theregister.com/2022/06/28/carnival-cybersecurity-fines/. [Accessed: Apr. 18, 2025]
[78] S. Steinberg, A. Stephan, and K. Neary, "*NotPetya: A Columbia University Case Study*", Columbia University School of International and Public Affairs (SIPA), 2021. Available: https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf#. [Accessed: Mar. 21, 2025]

[79] A.P. Moller - Maersk A/S, “Annual Report 2017”, A.P. Moller - Maersk A/S, Copenhagen, Denmark, Feb. 2018. Available: https://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf. [Accessed: Oct. 15, 2024]
[80] Graham Cluley, “The inside story of the Maersk NotPetya ransomware attack, from someone who was there”, *GrahamCluley.com*, Jun. 25, 2020. Available: https://grahamcluley.com/the-inside-story-of-the-maersk-notpetya-ransomware-attack/. [Accessed: Mar. 24, 2025]
[81] N. Antonov, *Ports Europe,* “Alphaliner Top 100 container market ranking”, Jun. 23, 2024. Available: https://www.portseurope.com/alphaliner-top-100-container-market-ranking/. [Accessed: Mar. 21, 2025]
[82] Carly Burdova, “What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?”, *Avast*, Jun. 18, 2020. Available: https://www.avast.com/c-eternalblue. [Accessed: Mar. 21, 2025]
[83] Aurelija Einorytė, “Mimikatz: everything you need to know | NordVPN”, *NordVPN Blog*, May 08, 2023. Available: https://nordvpn.com/blog/what-is-mimikatz/. [Accessed: Mar. 21, 2025]
[84] Endrin Musa, "*Maersk - The Ransomware Survivors", YouTube,* May 12, 2023. [Online Video] Available: https://www.youtube.com/watch?v=bKWXcOWzZSY. [Accessed: Mar. 24, 2025]
[85] T. Clarkson, “Maersk Cyber Attack: How NotPetya Crippled Global Shipping”, *OxygenIT Blog*, Jun. 26, 2024. Available: https://www.oxygenit.co.nz/blog/maersk-cyber-attack? [Accessed: Mar. 22, 2025]
[86] Nate Lord, “The Cost of a Malware Infection? For Maersk, $300 Million”, *Fortra’s Digital Guardian*, Aug. 17, 2017. Available: https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million. [Accessed: Mar. 24, 2025]
[87] enteringmode, “Responding to “the Most Destructive and Costly Cyberattack in History””, *ICDS*, Feb. 22, 2018. Available: https://icds.ee/en/responding-to-the-most-destructive-and-costly-cyberattack-in-history/. [Accessed: Mar. 24, 2025]
[88] P. Roberts, “FedEx: NotPetya Cost $300m, Wrecked Q1 Earnings”, *The Security Ledger with Paul F. Roberts*, Sep. 20, 2017. Available: https://securityledger.com/2017/09/fedex-notpetya-cost-300m-wrecked-q1-earnings/. [Accessed: Mar. 24, 2025]
[89] Kevin Townsend, “Court Rules in Favor of Merck in $1.4 Billion Insurance Claim Over NotPetya Cyberattack”, *SecurityWeek*, May 03, 2023. Available: https://www.securityweek.com/court-rules-in-favor-of-merck-in-1-4-billion-insurance-claim-over-notpetya-cyberattack/. [Accessed: Mar. 24, 2025]
[90] BBC News, “NotPetya cyber-attack cost TNT at least $300m”, *BBC News*, Sep. 20, 2017. Available: https://www.bbc.com/news/technology-41336086. [Accessed: Mar. 24, 2025]
[91] The Council of Insurance Agents & Brokers, “NotPetya: A War-Like Exclusion?”, The Council of Insurance Agents & Brokers, May 2019. Available: https://www.ciab.com/resources/notpetya-a-war-like-exclusion/. [Accessed: Mar. 24, 2025]
[92] M. Crosignani, M. Macchiavelli, and A. F. Silva, “Pirates without Borders: The Propagation of Cyberattacks through Firms’ Supply Chains”, Federal Reserve

Bank of New York, 937, Jul. 2020. Available: https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf . [Accessed: Mar. 24, 2025]
[93] Yiannis Kotoulas, "Cadbury owner settles legal battle with Zurich over $100m NotPetya cyber claim", *Insurance Times*, Nov. 10, 2022. Available: https://www.insurancetimes.co.uk/news/cadbury-owner-settles-legal-battle-with-zurich-over-100m-notpetya-cyber-claim/1442951.article. [Accessed: Mar. 24, 2025]
[94] S. Ragan, "Nuance says NotPetya attack led to $92 million in lost revenue", *CSO Online*, Feb. 28, 2018. Available: https://www.csoonline.com/article/564713/nuance-says-notpetya-attack-led-to-92-million-in-lost-revenue.html. [Accessed: Mar. 24, 2025]
[95] N. Dwyer, "The Staggering Cost of NotPetya Infection: DLA Piper and TNT Still Counting the Cost", *Computer One Australia*, Jun. 13, 2018. Available: https://computerone.com.au/dla-piper-tnt-notpetya/. [Accessed: Mar. 24, 2025]
[96] M. K. M. July 2 and 2024, "Feds Hit Health Entity With $950K Fine in NotPetya Attack". Available: https://www.bankinfosecurity.com/feds-hit-health-entity-950k-fine-in-notpetya-attack-a-25677. [Accessed: Mar. 24, 2025]
[97] Jack Rhysider, "NotPetya". Available: https://darknetdiaries.com/transcript/54/. [Accessed: Mar. 24, 2025]
[98] Yahoo Finance, "A.P. Møller - Mærsk A/S (DP4B.DU) Stock Price, News, Quote & History", *Yahoo Finance*. Available: https://finance.yahoo.com/chart/DP4B.DU/. [Accessed: Mar. 24, 2025]
[99] James Reddick, "Merck settles with insurers who denied $700 million NotPetya claim", *The Record*, Jan. 05, 2024. Available: https://therecord.media/merck-insurance-settlement-notpetya. [Accessed: Mar. 24, 2025]
[100] TSIB Team, "Claims Update: NotPetya Cyber Attack Settled", *TSIB Blog*, Jan. 12, 2024. Available: https://blog.tsibinc.com/claims-update-notpetya-cyber-attack-settled. [Accessed: Mar. 24, 2025]
[101] E. Blosfield, "Cyber Lessons for the Insurance Industry Continue Three Years After NotPetya", *Insurance Journal*, Aug. 12, 2020. Available: https://www.insurancejournal.com/news/national/2020/08/12/578788.htm. [Accessed: Mar. 24, 2025]
[102] P. He and E. M. Gold, "Lloyd's of London Requires Insurers to Add Exclusions to Limit Coverage for State-Backed Cyberattacks", *Policyholder Pulse*, May 09, 2023. Available: https://www.policyholderpulse.com/lloyds-london-state-backed-cyberattacks/. [Accessed: Mar. 24, 2025]
[103] L. Harris, "Threat of state-sponsored cyber attacks could make UK terror insurer obsolete", *Financial Times*, Apr. 24, 2025. Available: https://archive.ph/Whqwv. [Accessed: Mar. 24, 2025]
[104] M. Białas, "Maritime Cyber Attacks", *Vessel Automation*, Aug. 25, 2021. Available: https://vesselautomation.com/maritime-cyber-attacks/. [Accessed: Mar. 26, 2025]
[105] The Maritime Executive, "*CMA CGM Group Latest to Suffer Cyber Attack*", The Maritime Executive, Sep. 28, 2020. Available: https://maritime-executive.com/index.php/article/cma-cgm-group-latest-to-suffer-cyber-attack. [Accessed: Mar. 24, 2025]
[106] "*French shipping giant CMA CGM targeted in Ragnar Locker ransomware attack*", SiliconANGLE, Sep. 29, 2020. Available:

https://siliconangle.com/2020/09/29/french-shipping-giant-cma-cgm-targeted-ragnar-locker-ransomware-attack/. [Accessed: Mar. 26, 2025]
[107] "*[Security Weekly] Shipping Giant CMA CGM Goes Offline Following Ragnar Locker Ransomware Attack*", Penta Security Inc., Oct. 01, 2020. Available: https://www.pentasecurity.com/blog/security-weekly-shipping-giant-cma-cgm-ransomware/. [Accessed: Mar. 26, 2025]
[108] "*Cyberattack Update: 10/11/2020*". Available: https://www.cmacgm-group.com/en/news-media/global-it-update-09-29-2020. [Accessed: Mar. 26, 2025]
[109] "CMA CGM | The Group CMA CGM". Available: https://www.cma-cgm.com/about/the-group. [Accessed: Mar. 26, 2025]
[110] D. Fainsilber, "CMA CGM encaisse de nouveaux profits record au deuxième trimestre", *Les Échos*, Sep. 02, 2022. Available: https://www.lesechos.fr/industrie-services/tourisme-transport/cma-cgm-encaisse-de-nouveaux-profits-records-au-deuxieme-trimestre-1785494. [Accessed: Mar. 25, 2025]
[111] David, "Ragnar Locker Ransomware: Targeting Critical Infrastructure", *Data Stack Hub*, Oct. 25, 2024. Available: https://www.datastackhub.com/security/ragnar-locker-ransomware/. [Accessed: Mar. 27, 2025]
[112] G. Trompiz, "Shipping line CMA CGM suspects data breach from cyber attack", *Reuters*, Sep. 30, 2020. Available: https://www.reuters.com/article/business/shipping-line-cma-cgm-suspects-data-breach-from-cyber-attack-idUSKBN26L2MZ/. [Accessed: Mar. 27, 2025]
[113] *CMA CGM, "2020 Consolidated Financial Statements"*, Mar. 2021. Available: https://www.cmacgm-group.com/api/sites/default/files/2021-03/2020%20-%20Consolidated%20Accounts_1.pdf? [Accessed: Mar. 27, 2025]
[114] Lloyd's List News Desk, "CMA CGM confirms ransomware attack", *Lloyd's List*, Sep. 29, 2020. Available: https://www.lloydslist.com/-/media/lloyds-list/daily-pdf/2020/09-september/dailypdf290920.pdf? [Accessed: Mar. 26, 2025]
[115] Varuna Marine, "The Future and Maritime Cybersecurity: Are we really prepared?", *Varuna Marine Services*, Aug. 27, 2021. Available: https://varunamarine.eu/the-future-and-maritime-cybersecurity-are-we-really-prepared/. [Accessed: Apr. 18, 2025]
[116] CMA CGM, "2021 Consolidated Financial Statements", CMA CGM, Mar. 2022. Available: https://www.cmacgm-group.com/api/sites/default/files/2022-04/2021%20-%20Consolidated%20Accounts.pdf. [Accessed: Mar. 27, 2025]
[117] "South Africa Will Lift Force Majeure at Ports as Operations Resume", *The Maritime Executive*. Available: https://maritime-executive.com/article/south-africa-will-lift-force-majeure-at-ports-as-operations-resume. [Accessed: Mar. 28, 2025]
[118] Transnet SOC Ltd., Integrated Report 2021. Johannesburg, South Africa: Transnet SOC Ltd., 2021. [Online]. Available: https://static.pmg.org.za/Transnet_Integrated_Report_2021.pdf. [Accessed: March 28, 2025].
[119] Transnet SOC Ltd, "Transnet SOC Ltd Integrated Report 2022/23", Transnet SOC Ltd, 2023. Available: https://nationalgovernment.co.za/entity_annual/3440/2023-transnet-soc-ltd-annual-report.pdf. [Accessed: Mar. 28, 2025]

[120] S. Timcke, M. Gaffley, and A. Rens, “The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa’s Transnet”, *Afr. J. Inf. Commun.*, vol. 32, pp. 1–28, 2023, doi: 10.23962/ajic.i32.16949
[121] N. Ebrahim, “Transnet ramps up operations to clear three-month backlog at Durban port”, *Business*. Available: https://www.news24.com/fin24/economy/transnet-ramps-up-operations-to-clear-three-month-backlog-at-durban-port-20231202. [Accessed: Mar. 28, 2025]
[122] L. Omarjee, “Cyberattack, civil unrest, cable theft and Covid-19: Transnet turns corner on a tough 6 months”, *Business*. Available: https://www.news24.com/fin24/cyberattack-civil-unrest-cable-theft-and-covid-19-transnet-turns-corner-on-a-tough-6-months-20211112. [Accessed: Mar. 28, 2025]
[123] TBY, “Port Series: Durban, South Africa - The Business Year”, Nov. 11, 2024. Available: https://thebusinessyear.com/article/port-series-durban-south-africa/. [Accessed: Mar. 28, 2025]
[124] “Navigating troubled waters: Unpacking South Africa’s port challenges and charting a course for trans : Clyde & Co”. Available: https://www.clydeco.com:443/insights/2024/01/navigating-troubled-waters-unpacking-aouth-africa. [Accessed: Mar. 28, 2025]
[125] J. Maggs, “Durban to get lion’s share of R3.4bn Transnet port equipment overhaul”, *Moneyweb*, Feb. 28, 2025. Available: https://www.moneyweb.co.za/moneyweb-podcasts/moneyweb-midday/durban-to-get-lions-share-of-r3-4bn-transnet-port-equipment-overhaul/. [Accessed: Mar. 28, 2025]
[126] R. G. & P. Burkhardt, “‘Death Kitty’ ransomware linked to attack on South African ports”, *Business*. Available: https://www.news24.com/fin24/death-kitty-ransomware-linked-to-attack-on-south-african-ports-20210729. [Accessed: Mar. 28, 2025]
[127] “South Africa’s logistics company Transnet SOC hit by a ransomware attack - RedPacket Security”, Jul. 27, 2021. Available: https://www.redpacketsecurity.com/south-africas-logistics-company-transnet-soc-hit-by-a-ransomware-attack/. [Accessed: Mar. 28, 2025]
[128] M. Toyana, “Transnet cyberattack puts employees’ salaries at risk while backlogs at ports mount”, *Daily Maverick*, Jul. 26, 2021. Available: https://www.dailymaverick.co.za/article/2021-07-26-transnet-cyberattack-puts-employees-salaries-at-risk-while-backlogs-at-ports-mount/. [Accessed: Mar. 28, 2025]
[129] United Nations Conference on Trade and Development (UNCTAD), “Case Study 17: Port of Durban, South Africa”, UNCTAD, 2021. Available: https://resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa#. [Accessed: Mar. 24, 2025]
[130] KBV Research, “Maritime Digitization Market Size, Share & Analysis, 2028”, KBV Research, KBV-13961, Feb. 2023. Available: https://www.kbvresearch.com/maritime-digitization-market/. [Accessed: May 07, 2025]
[131] H. K. P. January 06 and 2022, “Insuring against cyberattacks”, *Recycling Today*. Available: https://www.recyclingtoday.com/article/insuring-against-cyberattacks-metals-industry/. [Accessed: Mar. 31, 2025]

[132] Statista, “Cybersecurity: Market Data & Analysis”, Statista, Aug. 2024. Available: https://www.statista.com/outlook/tmo/cybersecurity/worldwide. [Accessed: Mar. 28, 2025]
[133] H. Beckvard, S. Cho, A. Ertan, B. Valk, A. Väljataga, and J. Wünsche, “Recent Cyber Events: Considerations for Military and National Security Decision Makers”, *CCDCOE*, Sep. 2021. Available: https://ccdcoe.org/uploads/2021/09/Report_The_Global_Threat_A4-1.pdf#. [Accessed: Mar. 28, 2025]
[134] Organisation for Economic Co-operation and Development (OECD), “New Perspectives on Measuring Cybersecurity”, OECD Publishing, OECD Digital Economy Papers 366, Jun. 2024. doi: 10.1787/b1e31997-en. Available: https://www.oecd.org/en/publications/new-perspectives-on-measuring-cybersecurity_b1e31997-en.html. [Accessed: Mar. 27, 2025]
[135] Allied Market Research, “Maritime Digitization Market Statistics | Industry Forecast - 2031”. Available: https://www.alliedmarketresearch.com/maritime-digitization-market-A47395. [Accessed: May 07, 2025]
[136] M. Lind, S. Haraldson, K. Lind, W. Lehmacher, M. Svan, M. Renz, J. Gardeitchik, S. Singh, and P. Zuesongdham, “Ports of Tomorrow: Measuring Digital Maturity to Empower Sustainable Port Operations and Business Ecosystems,” *UNCTAD Transport and Trade Facilitation Newsletter,* no. 92, Article No. 80, Nov. 2021. [Online]. Available: https://unctad.org/news/ports-tomorrow-measuring-digital-maturity-empower-sustainable-port-operations-and-business. [Accessed: March 4, 2025].
[137] P. McGillivary, “Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed”, *Mar. Technol. Soc. J.*, vol. 52, no. 5, pp. 44–57, Sep. 2018, doi: 10.4031/MTSJ.52.5.11
[138] DNV, “Maritime Cyber Security Regulations”, *DNV*. Available: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/. [Accessed: Aug. 30, 2024]
[139] O. Melnyk, O. Drozdov, and S. Kuznichenko, “Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures”, *Lex Portus*, vol. 11, no. 1, Mar. 2025, doi: 10.62821/lp11101. Available: https://lexportus.net.ua/en/arkhiv-2/216-uncategories/ctati-vypuska-1-2025/554-melnyk-1111. [Accessed: Apr. 05, 2025]
[140] “Port State Control”, *International Maritime Organization (IMO)*. Available: https://www.imo.org/en/OurWork/IIIS/Pages/Port%20State%20Control.aspx. [Accessed: Apr. 05, 2025]
[141] S. Editor, “Preparing for the Digital Age: Shipping needs cybersecurity on its priority list”, *SAFETY4SEA*, Mar. 24, 2025. Available: https://safety4sea.com/cm-preparing-for-the-digital-age-shipping-needs-cybersecurity-on-its-priority-list/. [Accessed: Apr. 05, 2025]
[142] International Maritime Organization (IMO), “IMO to develop global strategy for maritime digitalization”, *IMO Press Briefings*, Mar. 18, 2025. Available: https://www.imo.org/en/MediaCentre/PressBriefings/pages/IMO-global-strategy-maritime-digitalization.aspx. [Accessed: Apr. 05, 2025]
[143] Council of the European Union, “Council Conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan”, Council of the European Union, Oct. 2023. Available: https://www.consilium.europa.eu/media/67499/st14280-en23.pdf. [Accessed: Mar. 09, 2025]

[144] European Union Agency for Cybersecurity (ENISA), “Port Cybersecurity - Good practices for cybersecurity in the maritime sector”, ENISA, Nov. 2019. Available: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector. [Accessed: Mar. 09, 2025]
[145] European Union Agency for Cybersecurity (ENISA), “Maritime Sector Sails through rough ‘Cybersecurity’ Seas | ENISA”, *ENISA*, Oct. 21, 2022. Available: https://www.enisa.europa.eu/news/maritime-sector-sails-through-rough-cybersecurity-seas. [Accessed: Mar. 09, 2025]
[146] European Maritime Safety Agency (EMSA), *European Maritime Safety Agency (EMSA)* - Quality Shipping, Safer Seas, Cleaner Oceans”. Available: https://www.emsa.europa.eu/. [Accessed: Apr. 05, 2025]
[147] S. Gandhi, “Frontex as a hub for surveillance and data sharing: Challenges for data protection and privacy rights”, *Comput. Law Secur. Rev.*, vol. 53, p. 105963, Jul. 2024, doi: 10.1016/j.clsr.2024.105963
[148] “Common information sharing environment (CISE) - European Commission”. Available: https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en. [Accessed: May 07, 2025]
[149] Danish Maritime Authority, “Danish Maritime Cybersecurity Unit”, *Danish Maritime Authority*. Available: https://www.dma.dk/safety-at-sea/danish-maritime-cybersecurity-unit. [Accessed: Mar. 09, 2025]
[150] “Maritime and Port Authority of Singapore”, *Maritime & Port Authority of Singapore (MPA)*, May 07, 2025. Available: https://www.mpa.gov.sg/home. [Accessed: May 07, 2025]
[151] “National maritime security strategy”, *GOV.UK*. Available: https://www.gov.uk/government/publications/national-maritime-security-strategy. [Accessed: May 07, 2025]
[152] Department for Transport, Code of Practice: Cyber Security for Ships, London, UK, Jul. 2023. [Online]. Available: https://assets.publishing.service.gov.uk/media/64c929c0d8b1a71bd8b05e80/code-of-practice-cyber-security-for-ships.pdf. [Accessed: April 7, 2025].
[153] University of Plymouth, “Cyber-SHIP Lab - University of Plymouth.” [Online]. Available: https://www.plymouth.ac.uk/research/cyber-ship-lab. [Accessed: May 07, 2025].
[154] NORMA Cyber, “Home,” NORMA Cyber. [Online]. Available: https://www.normacyber.no/. [Accessed: Feb. 03, 2025]
[155] Lloyd’s Register, “Lloyd’s Register”, *Lloyd’s Register*. Available: https://www.lr.org/en/. [Accessed: Mar. 09, 2025]
[156] DNV, “Cyber Secure class notation”, *DNV*. Available: https://www.dnv.com/services/cyber-secure-class-notation-124600/. [Accessed: Mar. 09, 2025]
[157] Bureau Veritas, “Rules on Cyber Security for the Classification of Marine Units”, Bureau Veritas, Courbevoie, France, Jul. 2024. Available: https://erules.veristar.com/dy/data/bv/pdf/659-NR_2024-07.pdf. [Accessed: Mar. 09, 2025]
[158] Nippon Kaiji Kyokai (ClassNK), “Guidelines for Cyber Resilience of Ships”, ClassNK, Edition 1.0, Jul. 2024. Available: https://www.classnk.or.jp/hp/pdf/activities/cybersecurity/gl_CyberResilienceofShips_202407e.pdf. [Accessed: Mar. 09, 2025]

[159] American Bureau of Shipping, “Guide for Cybersecurity Implementation for the Marine and Offshore Industries”, American Bureau of Shipping, Spring, TX, USA, Aug. 2023. Available: https://ww2.eagle.org/en.html. [Accessed: Mar. 09, 2025].

Appendix I – Roles of Regulatory and Classification Bodies in Maritime Cybersecurity

This appendix outlines a non-exhaustive list of principal regulatory, advisory, and technical bodies involved in shaping maritime cybersecurity policy and practice at the international, regional, and national levels. These organisations are governmental, intergovernmental, classification-based, and industry-led, all play various roles, from issuing guidelines and enforcing regulations to coordinating incident response and developing industry-specific standards.

1. International Regulatory Bodies

1.1. International Maritime Organization (IMO)

The IMO is a specialised UN agency responsible for regulating global shipping. It has recognised cyber threats as a safety issue and responded with:

- Resolution MSC.428(98) [35], requiring shipowners to incorporate cyber risk management into their Safety Management Systems (ISM Code) by 2021 [36].
- Guidelines on Maritime Cyber Risk Management, offering voluntary high-level advice on identifying and mitigating cyber risks.

Limitations: Implementation is delegated to Flag States, and enforcement remains uneven. The guidelines lack technical specificity and auditing mechanisms.

2. Regional and Supranational Bodies

2.1. European Union Maritime Security Strategy (EUMSS)

The EUMSS provides a framework to address EU-wide maritime security challenges. The 2023 revision prioritised [143]:

- Hybrid and cyber threats targeting critical maritime infrastructure.
- Alignment with EU-level legislation such as the Critical Entities Resilience Directive and NIS2 Directive.

2.2. European Union Agency for Cybersecurity (ENISA)

ENISA enhances cybersecurity resilience across EU member states, including maritime [144], [145]:

- Develops sector-specific guidelines and threat intelligence.
- Collaborates with port authorities and infrastructure operators on cyber defence.

- Supports risk mitigation for undersea cable networks and port-based OT/IT systems.

2.3. European Maritime Safety Agency (EMSA)

EMSA assists EU institutions and Member States in maritime safety and cybersecurity [146]:

- Issues technical guidance and operational support for maritime cyber risk management.
- Conducts tabletop exercises, training, and simulation workshops for ports and Flag States.
- Bridges maritime and cybersecurity policy through EU-level coordination.

2.4. European Border and Coast Guard Agency (Frontex)

Frontex is responsible for EU border control and maritime surveillance [147]:

- Uses the EUROSUR framework to detect maritime threats, including unauthorised intrusions.
- Shares intelligence on maritime incidents with cyber relevance among member states

securing maritime borders indirectly supports cybersecurity efforts by preventing unauthorised access and potential cyber threats originating from maritime routes

2.5. Common Information Sharing Environment (CISE)

CISE facilitates information exchange across EU and national maritime authorities [148]:

- Improves situational awareness by ensuring secure, real-time access to maritime surveillance data.
- Supports inter-agency cooperation in responding to cyber-enabled maritime incidents.

3. National Maritime Authorities

3.1. Danish Maritime Authority (DMA)

The DMA oversees maritime regulation in Denmark and has taken a proactive role in cybersecurity (established in 2019) [149]:

- Acts as a hub for cyber and information security for Danish maritime stakeholders.
- Provides national guidance and collaborates with public and private actors.

3.2. United States Coast Guard (USCG)

The USCG integrates cybersecurity within its maritime safety and infrastructure protection mission [63]:

- Issues cyber frameworks and policies for U.S. ports and vessels.
- Coordinates with CISA and the maritime sector on critical threat response.

3.3. Maritime and Port Authority of Singapore (MPA)

MPA leads maritime regulation and innovation in Singapore [150]:

- Implements port cybersecurity initiatives under its “Smart Port” digital strategy.
- Organises cyber drills and offers grants for cybersecurity investment in port infrastructure.

3.4. United Kingdom Maritime Cybersecurity Initiatives

The United Kingdom has developed a multifaceted approach to maritime cybersecurity, integrating national strategies, regulatory frameworks, and collaborative efforts:

- National Strategy for Maritime Security (2022) [151]: This strategy emphasizes enhancing capabilities in technology, innovation, and cybersecurity to protect maritime interests. It outlines objectives to support the maritime sector in building resilience against cyber threats, including providing advice and guidance on cyber best practices.
- Cybersecurity Code of Practice for Ships (2023) [152]: Published by the UK government, this code assists organizations in producing cybersecurity assessments and plans, serving as annexes to the ship security plan required under the ISPS Code.
- Cyber-SHIP Lab at the University of Plymouth [153]: This research facility focuses on addressing cybersecurity threats in the maritime industry by creating realistic simulations of shipping networks to test for vulnerabilities in maritime control systems.

3.5. Norwegian Maritime Cybersecurity Initiatives

Norway has adopted a proactive and coordinated approach to strengthening maritime cybersecurity through national and institutional collaboration:

- National Strategy for Maritime Cybersecurity (2020): Developed by the Norwegian Maritime Authority and the Norwegian Coastal Administration, this strategy focuses on preventive measures, response capabilities, and legal frameworks to create a resilient cybersecurity posture for Norway's maritime sector.
- NORMA Cyber: The Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) collaborates with authorities to enhance cybersecurity in the maritime industry. It plays a crucial role in producing and distributing warnings, sharing information on vulnerabilities, and analysing cyber incidents within the maritime sector [154].

4. National Cybersecurity Authorities and CERTs

4.1. Cybersecurity and Infrastructure Security Agency (CISA, USA)

CISA is the lead U.S. federal agency for critical infrastructure protection, including maritime:

- Publishes Maritime Cyber Risk Profiles, alerts, and sectoral guidance.
- Supports coordination with USCG, port authorities, and shipping firms.
- Coordinates with the US Coast Guard for maritime-specific threats.
- Offers technical assistance and incident response for port and shipping operators.

4.2. Australian Cyber Security Centre (ACSC)

ACSC provides Australia’s national cyber threat intelligence and incident response:

- Works closely with maritime transport operators as part of critical infrastructure defence.
- Publishes advisories and promotes cyber maturity among maritime stakeholders.

4.3. M-CERT / France Cyber Maritime

M-CERT is France's dedicated maritime cybersecurity coordination centre:

- Maintains the ADMIRAL cyberattack database.
- Provides intelligence sharing, incident response coordination, and cyber resilience promotion within the French maritime sector.

5. Industry Associations and Non-Governmental Organisations

5.1. International Chamber of Shipping (ICS)

ICS represents around 80% of the world's merchant fleet across ~40 countries:

- Collaborates with BIMCO to produce cyber risk management resources such as the Cyber Security Workbook for Onboard Ship Use.
- Advocates for workable global cybersecurity standards and policies through the IMO.

5.2. Baltic and International Maritime Council (BIMCO)

BIMCO is one of the largest global shipowner associations:

- Published Guidelines on Cyber Security Onboard Ships with partners like ICS.
- Developed the BIMCO Cyber Security Clause for contracts.
- Co-authored the practical Cyber Security Workbook with Witherby Publishing and ICS.

6. Classification Societies

Classification societies are independent non-governmental organisations that establish and maintain technical standards for the construction and operation of ships and offshore structures. Many now offer cyber-specific notations, frameworks and advisory services. Their guidelines align with IMO regulations, particularly the ISM Code, which mandates the integration of cyber risk management into maritime safety systems.

6.1. International Umbrella Organisation

6.1.1. International Association of Classification Societies (IACS)

IACS is a collective of leading classification societies that work together to develop unified requirements and guidelines. It coordinates harmonised cybersecurity standards and supports integration of cyber risk into class certification systems. It has recently introduced two mandatory cyber resilience standards mandatory for all IACS-member classed newbuilds from January 2024 and represent a significant regulatory advancement in embedding cybersecurity into the maritime lifecycle.

- UR E26: Cyber Resilience of Ships – Focuses on risk management and design-stage cybersecurity integration across ship systems [38].
- UR E27: Cyber Resilience of Onboard Systems and Equipment – Defines technical requirements and security controls for onboard equipment and control systems [38].

6.2. Individual Classification Societies

6.2.1. Lloyd's Register (LR)

LR Introduced the Cyber Secure class notation, which provides a framework for assessing the cybersecurity readiness of shipboard systems. It also provides cybersecurity assurance and risk frameworks. This notation helps shipowners implement appropriate cyber risk management practices [155].

6.2.2. DNV (Det Norske Veritas)

DNV, the Norwegian Classification Society developed the Cyber Secure class notation, offering a structured approach to evaluating and mitigating cyber risks in maritime operations. DNV's guidelines assist in integrating cybersecurity into existing safety management systems. Offers "Cyber Secure" class notations and training [156].

6.2.3. Bureau Veritas (BV)

BV has launched the Cyber Managed Prepared (CMP) notation, focusing on ensuring that vessels have robust cybersecurity measures in place. This notation covers aspects such as risk assessment, implementation of security controls, and continuous monitoring. Developed "CYBER MANAGED" notations [157].

6.2.4. ClassNK (Nippon Kaiji Kyokai)

ClassNK has introduced Guidelines for Designing Cyber Resilient Ships, which define cybersecurity verification for onboard IT/OT systems in accordance with IMO regulations. (ClassNK, 2023) [158].

6.2.5. American Bureau of Shipping (ABS)

ABS published a set of CyberSafety® Notations, covering CyberSafety Management Systems (CMS) and cyber resilience for operational networks. ABS emphasizes securing shipboard industrial control systems and integrating cybersecurity into vessel safety plans (ABS, 2023) [159].

Appendix II – Maritime Cyberattack Taxonomy

This appendix presents the custom taxonomy developed during the course of this research for classifying and analysing maritime cyber incidents. The visual structure of the taxonomy is shown in Figure 38, and the section for impact assessment in Figure 39. Table 14 further details how the fields are structured in the taxonomy. This is the fundamental framework behind the merged dataset.

1. Taxonomy Structure

The taxonomy has eight interlinked dimensions (field categories), collecting key attributes of a maritime cyber incidents. Each dimension includes structured and defined fields to tag and sort events consistently. It is designed to keep already existing references and links of the source databases, additional new fields are introduced to add additional sources and relevant information to them for easier cross referencing and for future research. Figures 38 is a simple visualisation the arrangement of categories within the taxonomy, and Table 14 shows how the fields and types of format data can be collected under each. Some fields have predefined parameters, some are Boolean or scale (such as the mitigation effectiveness, or the incident impact scoring parameters).

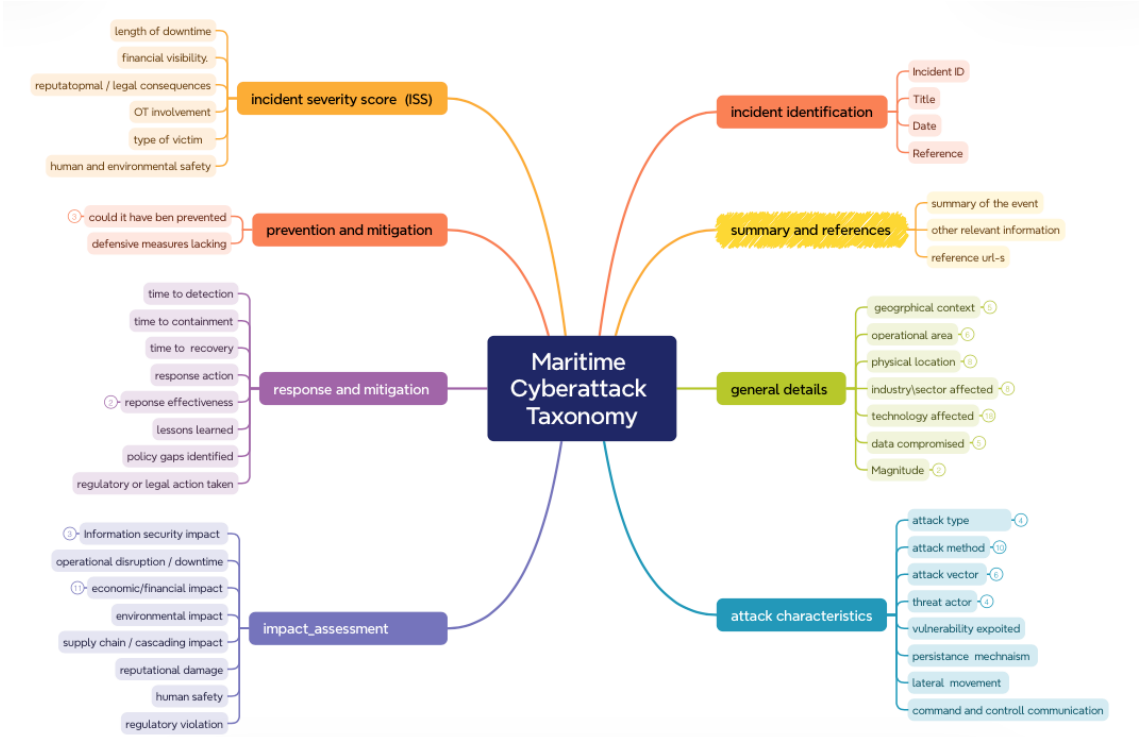


Figure 38 – Maritime Cyberattack Taxonomy [visualisation created by the author]

All field categories are further structured

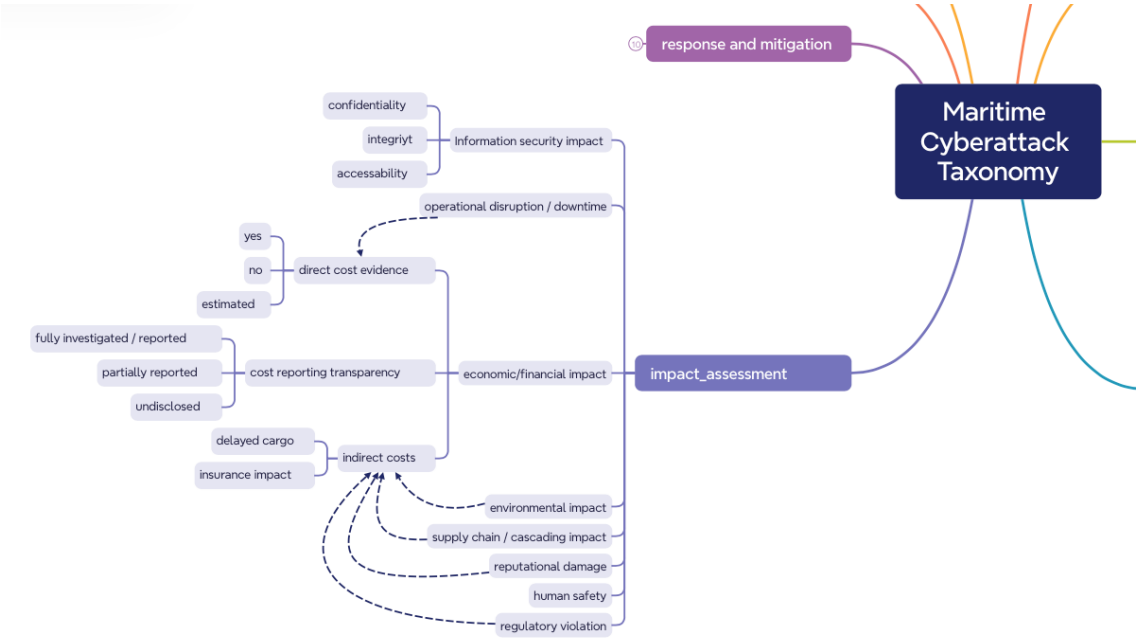


Figure 39- Impact assessment segment according to the Maritime Cyberattack Taxonomy

Table 14 – Structure of Taxonomy

	Field Category	Fields Names	Format / Type
1	Incident Identification	Unique ID	Alphanumeric / Unique Key
		Title	Free text
		Date	
		Source ID(s)	
		Reporter Entity	
		Sources	
2	General Details	Geographical Context	Predefined
		Impact Area	Free text
		Incident Location	Free text
		Incident Country	Enum / ISO Country List
		Incident Region	Enum / Region List
		Victim Country	Enum / ISO Country List
		Victim Region	Enum / Region List
		Victim Identity	Free text
		Victim Type	Free text
		Industry Sector Affected	Free text
		Technology Affected	Free text
		Data Compromised	Free text
		Magnitude	Levels/ predefined list / Free text
3	Attack Characteristics	Nature of Attack	Enum / Predefined List

		Attack Method	Free text
		Attack Vector	Free text
		Threat Actor Type	Enum / predefined list
		Threat Actor Identity	Free text
		Threat Actor Country Origin	Enum / ISO Country List
		Motivation	Enum / predefined list
		Vulnerability Exploited	Free text
		Persistence Mechanism	Free text
		Lateral Movement	Boolean / Free text
		C2 Communication	Boolean / Free text
4	Impact Assessment	C-I-A Impact	Enum / predefined list
		Operational Downtime	Numeric / free text
		Economic Impact	Numeric / Free text
		Environmental Impact	Free text
		Spillover Effect	Free text
		Reputational Damage	Free text
		Human Safety Impacts	Free text
		Regulatory Violations	Free text
5	Response and Policy insight	Response Actions	Free text
		Response Effectiveness	Levels / predefined list
		Time to Detection	Numeric (Hours / Days)
		Time to Containment	Numeric (Hours / Days)
		Lessons Learned	Free text
		Policy Gaps Identified	Free text
		Regulatory and Legal Actions	Free text
6	Prevention and Future Mitigation	Could it have been prevented?	Boolean / Free text
		Defence Measures Lacking	Free text
		Industry Recommendations	Free text
7	Summary and References	Event Summary	Free text
		Other Information	Free text
		Reference URL fields	Free text
8	Incident Severity Scoring	Victim Type	Boolean / numeric value
		Operational Technology (OT)	Boolean / numeric value
		Sensitive Data Involvement	Boolean / numeric value
		Operational Downtime	Boolean / numeric value
		Financial Impact	Boolean / numeric value
		Environmental Impact	Boolean / numeric value
		Supply Chain / Cascading Effects	Boolean / numeric value
		Reputational Damage	Boolean / numeric value
		Human Safety	Boolean / numeric value
		Legal and Regulatory Action	Boolean / numeric value

2. Hybrid Incident Severity Scoring (ISS) Model

The ISS was developed to systematically assess event severity through two metrics: a Boolean Impact Score (b-ISS: 0–10), indicating how many impact domains were affected, and a Weighted ISS (w-ISS: 0–14), capturing the intensity of each impact based on predefined weightings. Together, they produce a cumulative score that enables comparative analysis across incidents and enables filtering through the dataset. The scoring parameters are detailed in Table 15.

Table 15 – ISS scoring

Impact Factor	b-ISS Value (1/0)	w-ISS Range	Criteria
Victim Type	1 if victim is critical (e.g., port, navy)	0–1	1 = critical infrastructure, 0.5 = mid-tier, 0 = low value
Operational Technology (OT)	1 if OT systems were affected	0–1	1 = confirmed OT system compromise
Sensitive Data Involvement	1 if data was exfiltrated or leaked	0–1	1 = confirmed data breach involving PII, manifests, credentials etc.
Operational Downtime	1 if any disruption occurred	0–2	2 = prolonged (over week) or critical downtime, 1.5 = 4-7 days, 1 = 1-3 days, 0.5 = < 24h, 0 = <1h disruption
Financial Impact	1 if economic costs were observed	0–2	2 = significant financial impact (e.g., >$10M) 1 = moderate loss,
Environmental Impact	1 if maritime environment affected	0–1	1 = confirmed damage or pollution 0.5 = potential damage
Supply Chain / Cascading Effects	1 if third-party or global operations impacted	0–1	1 = disruption extended beyond primary victim
Reputational Damage	1 if public image was affected	0–1	1 = negative media coverage, public response, or reputational harm
Human Safety	1 if any safety risk present	0–3	3 = injury or loss of life 1 = minor safety threat,
Legal and Regulatory Action	1 if fines, lawsuits, or investigations followed	0–1	1 = confirmed legal or regulatory consequence

Appendix III – Top 30 Most Severe Incidents of 2001-2020

This appendix presents a curated selection of the 30 most severe maritime cyber incidents identified within the merged dataset, covering the period from 2001 to 2020. The incidents were ranked using the Incident Severity Score (ISS), which combines a Boolean score (b-ISS) reflecting the breadth of impact and a Weighted score (w-ISS) capturing the intensity of disruption across affected domains. Table 16 summarises each incident by key parameters, including the year, nature of attack, attacker identity or origin, underlying motivation, targeted technology, and a brief event summary. Due to space constraints, not all taxonomy fields are displayed; instead, this selection prioritises the most critical indicators of impact and severity. The full incident details remain available within the complete database.

Table 16 – Top 30 most severe cyberattacks from merged database sub dataset (2001-2020)

	Incident	Year	Nature of Attack	Attacker Identity / Origin	Motivation	Technology affected	Event Summary / Impacts	b-ISS (0-10)	w-ISS (0-14)
1	MT Kerala Hijacking	2014	Cyber-Assisted	Unidentified **pirate group**	Financial	AIS, Satellite Communication	$10 million fuel stolen, crew harmed	8	11
2	Stena Impero Seizure	2019	Cyber-Physical	Iran's Revolutionary Guards	Geopolitical	GPS, AIS	British tanker seized, 19 crew held	8	11
3	Venezuela Oil Sabotage	2002	Cyber-Physical	Unidentified	Political	SCADA, Industrial Ethernet	Production halted, economic damage	9	10,5
4	NotPetya on Maersk	2017	Cyber-only	Sandworm Team (Russia)	Geopolitical	Enterprise IT Systems	$250–$300M loss, 45K PCs affected	7	9

5	Pacific Energy SCADA Tampering	2008	Cyber-Physical	Ricky Joe Mitchell	Sabotage	SCADA, ICS	Leak detection disabled, shutdown	7	8,5
6	Iranian Offshore Platforms	2012	Cyber-Physical	Unidentified	Geopolitical	SCADA, IT	Disruption via malware	7	8,5
7	Drilling Rig Malware	2010	Cyber-Physical	Somali **Pirates**	Sabotage	ICS, Safety Systems	19-day downtime	7	8,5
8	Illicit Transfer - East China Sea	2018	Cyber-Assisted	Russia & DPRK	Sanctions evasion	AIS	AIS dark activity, illegal cargo	9	8
9	Illicit Transfer - Ningbo/Nampo	2019	Cyber-Enabled	North Korean vessels	Sanctions evasion	AIS	Coordinated AIS blackout	9	8
10	Shamoon on Aramco	2012	Cyber-only	Cutting Sword of Justice	Geopolitical	MS Windows, Networks	30,000 PCs wiped, oil halted	6	8
11	Kharg Island Malware	2012	Cyber-Physical	Unidentified	Geopolitical	SCADA, IT	Oil terminal damage	7	8
12	SK GPS Jamming (11 days)	2011	Cyber-only	Unidentified	Geopolitical	GPS	145 towers, 106 planes, 10 ships affected	5	8
13	Aus Defence Breach	2016	Cyber-only	Chinese APT	Espionage	Corporate IT	30GB military data stolen	7	7,5
14	US Navy-HPES Breach	2016	Cyber-only	Unidentified	Espionage	IT Systems	134,386 records leaked	7	7,5
15	Putin GPS Spoofing	2018	Cyber-only	Russian State	Security/Protection	GNSS, GPS	24 ships spoofed	8	7
16	Diamond 8 AIS Evasion	2019	Cyber-Enabled	DPRK-linked Vessel	Sanctions evasion	AIS	Multiple blackouts, fuel transfer	8	7
17	Illegal Fishing - West Africa	2014	Cyber-Assisted	Releixo & Egaluze	Financial	AIS, VMS	Repetitive dark activity	7	7
18	Aus Customs Hack	2012	Cyber-only	Unidentified	Smuggling	IT Systems	Criminals evaded flagged cargo	6	7
19	CMA CGM Ransomware	2020	Cyber-only	Ragnar Locker	Financial	IT Systems	Booking and logistics disrupted	7	7
20	SK GPS Jamming (16 days)	2012	Cyber-only	North Korea	Geopolitical	GPS	254 ships, 1,016 planes disrupted	6	7

21	Greek Shipping Hacked by Pirates	2010	Cyber-only	Unidentified	Financial	IT Systems, Wi-Fi	Hackers leaked ship routes for pirate attacks	5	7
22	Anchor Panda APT14 Espionage	2013	Cyber-only	APT14 (China)	Espionage	Satellite Comms, IT Networks	Years-long spying on maritime firms	7	6,5
23	Houston/Gulf Oil Platforms Malware	2013	Cyber-Physical	Unidentified	Sabotage	ICS, SCADA	Rig lost navigation, environmental damage	7	6,5
24	Shahid Rajaee Port Attack	2020	Cyber-only	Unconfirmed (possibly Israel)	Retaliation	IT Systems	Port operations halted, major delays	7	6,5
25	Vessels Spoofed in Quanzhou, China	2019	Cyber-only	Unidentified	Geopolitical	GPS, IT Systems	Spoofing disrupted oil terminal ops	8	6
26	GPS Jamming - 280 Fishing Ships	2016	Cyber-only	North Korea	Geopolitical	GPS	Fishing disrupted, ships forced back	7	6
27	Ryuk on US Maritime Facility	2019	Cyber-Physical	Unattributed	Financial	IT Systems, OT	30+ hour port shutdown from phishing	7	6
28	NK GPS Jam on Ships & Planes	2016	Cyber-only	North Korea	Provocation	GPS	700 ships & planes affected	7	6
29	Toll Group Ransomware	2020	Cyber-only	Nefilim	Financial	IT Systems	220GB data encrypted, logistics halted	7	6
30	Marseille Port Ransomware	2020	Cyber-only	Unknown	Financial	Municipal/Port IT	Smart Port systems exposed	7	6

Appendix IV – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Júlia Anna Grosschmid

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Assessing the Economic Impact of Cyberattacks in the Maritime Sector: A Taxonomy-Driven Case Study and Data Analysis” supervised by professor Sanja Bauk
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

18.05.2025

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.