Ekonomi İşletme ve Maliye Araştırmaları Dergisi
Journal of Economics, Business and Finance Research
e-ISSN: 2667-503X

Year: 2024 **Volume:** 6 **Issue:** 3 **Pages:** 268-289
Article Received Date: July 15, 2024 **Article Accepted Date:** December 31, 2024
Article Published Date: December 31, 2024 **Doi:** 10.38009/ekimad.1516613
Research Article

A Proposal for A Monte Carlo Simulation-Based Risk Framework With Optimal Cost Balance for The Maritime Industry[1]

Saim Atalay Keleştemur[*]
Süha Atatüre[**]
Güldem Elmas[***]

Abstract

The maritime industry has played a vital role in international trade since the earliest periods of human history, facilitating the movement of approximately 90% of global trade. Modern ships are increasingly equipped with sophisticated computing infrastructure to enhance navigation, communication, and operational efficiency. This technological evolution has transformed maritime operations, providing numerous advantages such as improved safety, efficiency, and communication. However, the integration of advanced computer systems also introduces significant cyber threats, which can compromise vessel operations, safety, and security. This study proposes a comprehensive cyber risk framework tailored for the maritime industry, employing Monte Carlo simulation to analyze and quantify risks for each vessel component. The risk calculation is based on the MITRE Common Attack Pattern Enumeration and Classification (CAPEC) database, providing a detailed and structured approach to identifying potential cyber threats. The study utilizes the Multiplicative Effect Approach in its cyber risk analysis methods, allowing for a nuanced understanding of how various risk factors interact and amplify the overall risk profile. The framework is designed to help maritime companies prioritize risk mitigation efforts, ensuring that available funds are allocated in a manner that maximizes risk reduction. By simulating various scenarios and their potential impacts, the framework provides actionable insights into the most effective cybersecurity measures. This approach enables maritime organizations to develop targeted strategies for enhancing their cyber resilience, ultimately contributing to the safety and reliability of global maritime trade.

Keywords: Maritime, Cybersecurity, Risk Analysis, Monte Carlo, Optimal Cost Balance

JEL Classification: *C61, C63, D81, F13*

---

[1] This article is derived from Saim Atalay Keleştemur's PhD Dissertation in Internation Trade Doctoral Program at Istanbul Gedik University.

[*] PhD Student, Istanbul Gedik University, Institute of Graduate Studies, International Trade and Finance, sakelestemur@gmail.com ORCID NO: 0009-0006-5493-2112

[**] Prof. Dr., Istanbul Gedik University, Faculty of Economics Administrative and Social Sciences, Political Science and International Relations, suha.atature@gedik.edu.tr ORCID NO: 0000-0003-1683-5224

[***] Asst. Prof., Istanbul University-Cerrahpaşa, Faculty of Engineering, Maritime Transportation Management Engineering, gelmas@iuc.edu.tr ORCID NO: 0000-0002-2585-9650

Cite: Keleştemur, S. A., Atatüre, S., & Elmas, G. (2024). A Proposal for A Monte Carlo Simulation-Based Risk Framework with Optimal Cost Balance for the Maritime Industry. Ekonomi İşletme ve Maliye Araştırmaları Dergisi, 6(3), 268-289.

Denizcilik Endüstrisi İçin Optimum Maliyet Dengesi İle Monte Carlo Simülasyonu Tabanlı Bir Risk Çerçevesi Önerisi

Öz

Denizcilik endüstrisi, insanlık tarihinin en eski dönemlerinden beri uluslararası ticarette hayati bir rol oynamış ve dünya ticaretinin yaklaşık %90'ının taşınmasını sağlamıştır. Modern gemiler, navigasyon, iletişim ve operasyonel verimliliği artırmak için giderek daha fazla sofistike bilgi işlem altyapısıyla donatılmaktadır. Bu teknolojik evrim, denizcilik operasyonlarını dönüştürmüş, gelişmiş güvenlik, verimlilik ve iletişim gibi birçok avantaj sağlamıştır. Ancak, gelişmiş bilgisayar sistemlerinin entegrasyonu, gemi operasyonlarını, güvenliğini ve emniyetini tehlikeye atabilecek önemli siber tehditleri de beraberinde getirmektedir. Bu çalışma, denizcilik endüstrisi için özel olarak tasarlanmış kapsamlı bir siber risk çerçevesi önermektedir. Her bir gemi bileşeni için riskleri analiz etmek ve nicelleştirmek amacıyla Monte Carlo simülasyonu kullanılmaktadır. Risk hesaplaması, potansiyel siber tehditleri belirlemek için ayrıntılı ve yapılandırılmış bir yaklaşım sunan MITRE Common Attack Pattern Enumeration and Classification (CAPEC) veritabanına dayanmaktadır. Çalışma, siber risk analiz yöntemlerinde Çarpan Etkisi Yaklaşımı'nı kullanarak, çeşitli risk faktörlerinin nasıl etkileşime girdiğini ve genel risk profilini nasıl artırdığını daha ince bir şekilde anlamayı sağlamaktadır. Önerilen çerçeve, denizcilik şirketlerinin risk azaltma çabalarını önceliklendirmelerine yardımcı olacak şekilde tasarlanmıştır ve mevcut bütçenin risk azaltımını maksimize edecek şekilde tahsis edilmesini sağlamaktadır. Çereve, farklı senaryoları ve bunların potansiyel etkilerini simüle ederek, en etkili siber güvenlik önlemleri hakkında uygulanabilir içgörüler sunmaktadır. Bu yaklaşım, denizcilik işletmelerinin siber dayanıklılığını artırmak için hedeflenmiş stratejiler geliştirmelerine olanak tanımakta ve küresel deniz ticaretinin güvenliği ve güvenilirliğine katkıda bulunmaktadır.

Anahtar Kelimeler: Denizcilik, Siber Güvenlik, Risk Analizi, Monte Carlo, Optimum Maliyet Dengesi

JEL Sınıflandırması: *C61, C63, D81, F13*

1. Introduction

Maritime transportation is a critical element of international trade. Approximately 90% of world trade by volume is conducted via maritime transport, highlighting its fundamental role in facilitating cross-border commerce (Cuong et al., 2020). The efficiency and development of infrastructure within the maritime sector are crucial factors in enhancing countries' competitiveness in international trade. The sustainable economic development of nations is directly linked to the indispensable role of maritime transport in supporting international trade (Xu et al., 2020).

The volume of international maritime trade has steadily increased over the last century. Autonomous ships, technological improvements on cargo handling systems, and modern shipyards and port facilities underscores the importance of maritime transport in the global movement of goods. Ports, as vital components of maritime transportation, serve as significant nodes in the international trade network, handling a substantial portion of global trade flows (Blonigen & Wilson, 2007). The strategic importance of sustainable maritime transport is accentuated by its potential to achieve global sustainability goals, such as those outlined in the 2030 Sustainable Development Agenda and the Paris Agreement.

Investments in maritime transportation infrastructure have been proven to promote exports, improve trade flows, and increase maritime trade volumes. As international goods trade grows, the role of maritime transportation becomes increasingly significant, enhancing its importance in the global trade environment (Yıldız, 2022). Maritime risks encompass various threats and challenges that pose significant dangers to the security, safety, and operations of the maritime sector.

These risks range from traditional issues like piracy and maritime terrorism to emerging concerns such as cyber threats and environmental crimes (Karamperidis et al., 2021). The extensive network of ships, ports, and supply chains in the maritime sector creates vulnerabilities that can be exploited by malicious actors aiming to disrupt and harm operations (Balduzzi et al., 2014). In the realm of cybersecurity, the increasing reliance on digital technologies in maritime operations exposes the industry to cyber threats that could compromise the security and integrity of maritime systems.

International Security Management Systems (ISMS), the Ship Security Plan (SSP), and the International Ship and Port Facility Security (ISPS) Code are critical components for ensuring the security and safety of maritime operations on a global scale. Established by the International Maritime Organization (IMO) in 2004, the ISPS Code aims to enhance security in response to global threats of piracy and terrorism. This code promotes international cooperation among governments, shipping companies, and port facilities to identify, assess, and respond to security threats to ships and ports (Radonja & Glujić, 2020).

According to the ISPS Code, each ship is required to have a Ship Security Plan (SSP). The SSP outlines the security procedures and measures to be implemented on board to prevent security incidents affecting ships engaged in international trade (Grapa & Lemoncito, 2021). Furthermore, the ISPS Code mandates collaboration among governments, shipping companies, ship personnel, and port facility personnel to detect security threats and take preventive measures against security incidents. Emerging cyber threats in the maritime sector highlight the necessity for a Ship Cyber Security Plan, which can be developed through the implementation of cyber risk frameworks tailored for ships.

This study aims to highlight the importance of cyber risks on vessels. By expanding and applying a cyber risk assessment methodology using a catalogue of common attack patterns from MITRE CAPEC, we aim to contribute for the creation of an SSP. Each attack pattern is classified according to the Maritime Cyber Risk Management Guidelines published by the IMO. That way, we aim for the framework to be used globally.

2. Literature Review

Maritime transportation, as a significant component of the global economy, is a critical element of international trade. The efficiency and development of infrastructure within the maritime sector are crucial factors in enhancing countries' competitiveness in international trade. The sustainable economic development of nations is directly linked to the indispensable role of maritime transport in supporting international trade.

The volume of international maritime trade has steadily increased over the last century, with the technological enhancements and growing numbers of modern vessels. This underscores the critical importance of maritime transport in the global movement of goods. Ports, as vital components of maritime transportation, serve as significant nodes in the international trade network, handling a substantial portion of global trade flows (Blonigen & Wilson, 2007).

The strategic importance of sustainable maritime transport is accentuated by its potential to achieve global sustainability goals, such as those outlined in the 2030 Sustainable Development Agenda and the Paris Agreement. Investments in maritime transportation infrastructure have been proven to promote exports, improve trade flows, and increase maritime trade volumes. As international goods trade grows, the role of maritime transportation becomes increasingly significant, enhancing its importance in the global trade environment (Yıldız, 2022).

Maritime risks encompass various threats and challenges that pose significant dangers to the security, safety, and operations of the maritime sector. These risks range from traditional issues like piracy and maritime terrorism to emerging concerns such as cyber threats and environmental crimes (Karamperidis et al., 2021). The extensive network of ships, ports, and supply chains in the maritime sector creates vulnerabilities that can be exploited by malicious actors aiming to disrupt and harm operations (Balduzzi et al., 2014).

The increasing reliance on digital technologies in maritime operations exposes the industry to cyber threats that could compromise the security and integrity of maritime systems. Vulnerabilities in ship computer aided components such as the Automatic Identification System (AIS) and potential cyber-

attacks on autonomous ships underscore the need for robust cybersecurity measures to protect against data breaches and operational disruptions.

International Security Management Systems (ISMS), the Ship Security Plan (SSP), and the International Ship and Port Facility Security (ISPS) Code are critical components for ensuring the security and safety of maritime operations on a global scale. Established by the International Maritime Organization (IMO) in 2004, the ISPS Code aims to enhance security in response to global threats of piracy and terrorism. This code promotes international cooperation among governments, shipping companies, and port facilities to identify, assess, and respond to security threats to ships and ports (Radonja & Glujić, 2020).

According to the ISPS Code, each ship is required to have a Ship Security Plan (SSP). The SSP outlines the security procedures and measures to be implemented on board to prevent security incidents affecting ships engaged in international trade (Grapa & Lemoncito, 2021). Furthermore, the ISPS Code mandates collaboration among governments, shipping companies, ship personnel, and port facility personnel to detect security threats and take preventive measures against security incidents. Emerging cyber threats in the maritime sector highlight the necessity for a Ship Cyber Security Plan, which can be developed through the implementation of cyber risk frameworks tailored for ships.

2.1. Previous Cyber Incidents on Maritime Industry

2.1.1. Antwerp Port Cyber Attack

In 2009, a cyberattack in Belgium's Port of Antwerp severely disrupted port operations. Cybercriminals infiltrated the port's container tracking system, altering container locations to facilitate drug smuggling. This attack posed significant security risks and caused serious disruptions in operational processes. Authorities launched a comprehensive investigation to identify security vulnerabilities and prevent similar incidents.

The attackers tracked containers to identify and steal valuable cargo, posing a major threat to port security and damaging the port's reputation. This cyber incident highlighted the need for port administrations to be prepared not only for physical security but also for cybersecurity. Following the attack, port officials enhanced security measures and developed new protocols to secure operational processes (Seatrade Maritime, 2013).

2.1.2. South Korea Drill Platform Ransomware Attack

In 2010, a drilling rig traveling from a construction site in South Korea to South America fell victim to a malware attack. The attack infected the rig's critical control systems with a virus, severely disrupting operational processes. The malware specifically targeted computers controlling the Blowout Preventer (BOP) system, hindering the rig's ability to operate safely and efficiently.

As a result of the attack, operations were halted for 19 days to clean the system, leading to an estimated daily cost of $700,000, totaling $13.3 million in losses. This incident highlighted the critical importance of cybersecurity in the maritime sector and the need to protect control systems. In response, the company implemented enhanced cybersecurity measures and launched a comprehensive cybersecurity training program for its employees (Drilling Contractor, 2015).

2.1.3. Greek Maritime Company Wi-Fi Network Attack

In 2011, a Greek shipping company fell victim to a cyberattack conducted via the Wi-Fi network at its headquarters. Attackers infiltrated the company's IT systems, obtaining information about ships and navigation routes. This data was used to plan and execute physical pirate attacks in the Gulf of Aden. Local pirates exploited this information to identify the most vulnerable moments and routes, making their attacks more effective.

As a result, the company suffered significant financial losses and was forced to take extensive measures to address security vulnerabilities. Cybercriminals escalated attacks on ships, disrupting maritime operations and damaging the company's reputation. Following the incident, the company developed a comprehensive security strategy to strengthen cybersecurity measures and prevent similar events. This case underscored the critical importance of cybersecurity in the maritime sector and prompted other companies to review their security protocols (Safety4Sea, 2019).

2.1.4. Iran's Offshore Platform in the Persian Gulf Targeted by a Cyberattack

In 2012, Iranian officials reported a cyberattack targeting the communication networks of an offshore oil platform in the Persian Gulf. This attack underscored the seriousness of cybersecurity threats to Iran's oil sector. Following the attack, the websites of Iran's Ministry of Petroleum and the National Iranian Oil Company (NIOC), along with other related official sites, were taken offline. This disruption temporarily affected the country's oil production and export activities.

In response, Iran established a "cyber crisis committee" to address such threats and implemented urgent measures. Officials acknowledged that the attack had erased some user data but stated that production and exports were not impacted. This incident highlighted Iran's emphasis on cybersecurity following the Stuxnet attack and demonstrated its efforts to enhance defense capabilities against such threats. Iran's proactive response emphasized the importance of protecting critical infrastructure with robust security measures (The Jerusalem Post, 2012).

2.1.5. Insider Attack on a US Nuclear Aircraft Carrier

In 2014, a system administrator launched an insider cyberattack on a U.S. nuclear aircraft carrier. The attacker infiltrated the ship's IT systems, gaining access to critical data and jeopardizing operational processes. This incident highlighted the significant threat posed by insider risks in the maritime sector. Authorities reviewed security protocols and implemented necessary updates to prevent similar occurrences.

Following the attack, aircraft carrier officials undertook not only procedural and policy changes for IT systems but also technical enhancements. Additionally, the incident raised awareness of the human factor's importance in cybersecurity. Comprehensive cybersecurity training programs were initiated for employees to increase awareness and prevent future threats (Data Breach Today, 2014).

2.1.6. GPS Blackout Affecting 280 Ships in South Korea

In 2016, hundreds of airplanes and ships in South Korea were forced to return to port due to issues with their navigation systems. These problems were alleged to have been caused by GPS jamming attacks carried out by North Korea. It was discovered that North Korea had transmitted widespread GPS jamming signals during joint military exercises between South Korea and the United States.

These attacks affected not only ships but also airplanes and land vehicles, disrupting the safe navigation of vessels and causing significant operational delays. Following these incidents, South Korean authorities implemented various measures to detect and prevent GPS jamming signals. However, no definitive evidence directly implicating North Korea in these attacks was found, and thus no official accusations were made (BBC, 2016).

2.1.7. MAERSK NoPetya Ransomware Attack

The 2017 NotPetya cyberattack affected several major maritime companies, including Maersk Line. This ransomware attack caused significant operational disruptions and financial losses. Maersk allocated substantial resources to mitigate the impact and implemented serious updates to its security protocols. The NotPetya attack underscored the critical importance of cybersecurity in the maritime industry.

The attack temporarily halted Maersk's global operations. In response, the company developed a comprehensive strategy to rebuild its systems and protect against similar incidents. Maersk collaborated with cybersecurity experts to review its security protocols and launched training programs for its employees. Following the attack, Maersk established a stronger cybersecurity infrastructure and resumed its operational activities (Los Angeles Times, 2017).

2.1.8. COSCO Shipping Lines Ransomware Attack

In 2018, COSCO Shipping Lines' U.S. network was hit by a ransomware attack, temporarily halting the company's North American operations and compromising customer data. Following the attack, COSCO took extensive security measures to rebuild its systems and prevent similar incidents. The company also strengthened its IT infrastructure and updated its cybersecurity protocols.

In response, COSCO reviewed its operational processes and security measures. It launched cybersecurity training programs for employees to prevent recurrence and updated its security software, developing new protocols to build a system resilient to ransomware attacks. This incident highlighted the seriousness of ransomware threats in the maritime sector and the critical need for preparedness against such threats (Maritime Executive, 2018).

2.1.9. Naantali Port Tanker Ship Ransomware Attack

In 2019, a ransomware infection targeted the management server of an oil tanker near Finland's Port of Naantali. The attack also erased the backup disk, making it impossible for the vessel to restore its operational data. The infection was believed to have entered through various vectors such as the Remote Desktop Protocol (RDP), a USB device, or an email attachment.

This incident highlighted the severe threat ransomware poses to the maritime sector and caused significant operational disruptions. The same tanker was infected again four months later near the same port, indicating that attackers regained access and re-targeted the ship's systems. Following the attacks, the vessel operators implemented extensive security measures to prevent recurrence (Soner et., 2024).

2.1.10. Mediterranean Shipping Company (MSC) Cyber Attack

In 2020, Mediterranean Shipping Company (MSC), one of the world's largest shipping companies, suffered a significant cyberattack. The attackers infiltrated the company's IT systems, gaining access to critical data and disrupting operational processes. This attack severely impacted MSC's global operations, causing substantial disruptions to its commercial activities.

Following the attack, MSC took extensive measures to rebuild its systems and prevent similar incidents. The company strengthened its IT infrastructure and updated its cybersecurity protocols. It also launched cybersecurity training programs for employees to raise awareness and preparedness against cyber threats (SeaTrade Maritime, 2020).

2.1.11. Rotterdam Port Cyber Attack

In 2021, the Port of Rotterdam, Europe's largest port, suffered a major cyberattack. The attackers infiltrated the port's IT systems, gaining access to critical data and severely disrupting operational processes. This attack brought port operations to a standstill, significantly impacting commercial activities.

After the incident, port authorities undertook extensive measures to rebuild systems and prevent similar incidents. They strengthened the IT infrastructure and updated cybersecurity protocols. Additionally, cybersecurity training programs were launched to raise employee awareness and preparedness against such threats (Port Technology, 2022).

2.1.11. Nagoya Port LockBit RansomwareAttack

In 2023, Nagoya Port, Japan's largest port, suffered a LockBit ransomware attack. The attackers infiltrated the port's IT systems, significantly disrupting operational processes. This attack halted port operations and suspended Toyota's import-export lines.

Nagoya Port authorities implemented extensive measures to rebuild systems and prevent similar incidents. They launched cybersecurity training programs to enhance employee awareness and preparedness against cyber threats (Security Week, 2023).

This study aims to highlight the importance of cyber risks on vessels. By expanding and applying cyber risk assessment methodology using a catalogue of common attack patterns from MITRE CAPEC, we contribute to the literature. Each attack pattern is classified according to the Maritime Cyber Risk Management Guidelines published by the IMO. The study also employs the Multiplicative Effect Approach in its cyber risk analysis methods, enabling a detailed comprehension of how various risk factors interact and intensify the overall risk profile. The framework is specifically designed to assist maritime companies in prioritizing risk mitigation efforts, ensuring that available funds are allocated in a way that maximizes risk reduction.

3. Methodology

This study aims to identify cyber risks targeting computer-aided systems on ships by analyzing past cyber incidents in the maritime sector and to develop a mathematical risk analysis model using Monte Carlo simulation based on MITRE CAPEC IDs. The study employs a research design that formulates the potential impacts of cyber threats likely to be encountered by modern commercial vessels, using the MITRE CAPEC framework's attack vectors and the Multiplier Effect Approach. Subsequently, these risks are processed through Monte Carlo simulation to obtain mathematical results.

Monte Carlo simulation is a statistical technique that employs random sampling to solve complex problems that may be deterministic in nature. This method is particularly useful in scenarios where traditional analytical methods are impractical. The name "Monte Carlo" itself is derived from the famous casino in Monaco, reflecting the method's reliance on randomness and probability (Wu & Pan, 2018). The fundamental principle of Monte Carlo simulation involves generating a large number of random samples to approximate the behavior of a system or process.

In finance, Monte Carlo methods are extensively used for option pricing and risk assessment, allowing analysts to model the uncertainty and variability inherent in financial markets (Bakar, 2019). Advancements in computational power have significantly enhanced the capabilities of Monte Carlo simulations, allowing for more complex and detailed analyses. This evolution has expanded the scope of Monte Carlo applications, enabling researchers and practitioners to tackle increasingly sophisticated problems across diverse domains, including machine learning and quantum processes (Liu, 2024).

The MITRE Common Attack Pattern Enumeration and Classification (CAPEC) is a comprehensive framework designed to catalog and classify various attack patterns that adversaries may employ in cyber operations. Developed by the MITRE Corporation, CAPEC serves as a valuable resource for cybersecurity professionals, providing detailed descriptions of attack methods and techniques that can be utilized to enhance security measures across different systems and applications (Dimitrov, 2023). CAPEC is structured in a hierarchical taxonomy, allowing users to navigate through various attack patterns based on their characteristics and methodologies.

Each entry in the CAPEC database includes specific details about the attack, such as its purpose, the techniques involved, and potential mitigations. This structured approach enables organizations to better understand the nature of threats they face and to develop more effective defense strategies (Seid, 2024). CAPEC is frequently used in conjunction with other MITRE frameworks, such as the

ATT&CK framework, which focuses on the tactics, techniques, and procedures (TTPs) used by attackers. This integration allows for a more holistic view of the threat landscape, enabling security professionals to correlate attack patterns with specific vulnerabilities and to prioritize their response efforts accordingly (Al-Sada, 2024).

For the literature review, academic databases were researched, and cyber-attacks, countermeasures, and threats specific to the maritime sector were examined. Additionally, the Maritime Cyber Attack Database (MCAD) from NHL Stenden University of Applied Sciences was used to analyze past cyber incidents. All attack methods targeting computer-aided systems on ships were examined, and for each component, the CAPEC attack vector, risk probability, risk severity, and risk impact were processed.

After calculating the risk impact using the Multiplier Effect Approach, a Risk Score based on CVSS 3.0 was obtained, categorizing risks as Low, Medium, High, and Very High. Based on all analyses and calculations, CAPECs and their results, which can be used as an attack model for ship components, are presented in a table. By examining the attack vectors of past cyber incidents in the maritime sector, data was obtained.

Software and hardware vulnerabilities of ship components (assets) that were subjected to cyber attacks were also examined, forming the final dataset for the study's components and CAPEC attack vectors. Attack vectors and components were treated as variables, and protective security measures applicable to these variables were also proposed as solutions. The obtained variables and assessments are presented in Table 1.

Table 1. Definitions of MITRE CAPEC IDs

CAPEC-2: **Inducing Account Lockout**	**An attacker takes advantage of a security feature, like a password throttling mechanism that locks accounts after several failed attempts, to execute a DoS attack. This results in legitimate users being locked out of their accounts.**
CAPEC-28: **Fuzzing**	An attacker utilizes fuzzing to identify system vulnerabilities. Fuzzing tests software security by providing random inputs to the system, uncovering failures without any preconceived notions or assumptions about the system.
CAPEC-70: **Try Common or Default Credentials**	An attacker might attempt to gain unauthorized access by leveraging common or default usernames and passwords. This technique often involves exploiting several well-known weaknesses in account security practices.
CAPEC-74: **Manipulating State**	An attacker alters the state information kept by the target software or induces a state change in hardware. If successful, the compromised state causes the target system to operate in unintended ways.
CAPEC-94: **Adversary in the Middle (AiTM)**	An attacker intercepts communication between two components, such as a client and server, to modify or steal transaction data. This often involves placing themselves within the communication channel between the components.
CAPEC-114: **Authentication Abuse**	An attacker exploits weaknesses in the authentication mechanism or its implementation to gain unauthorized access to an application, service, or device. A specific series of events can result in granting the attacker access.
CAPEC-115: **Authentication Bypass**	An attacker circumvents an authentication mechanism to access an application, service, or device with authorized user privileges, allowing access to protected data without authentication process.

Table 1 (Continued). Definitions of MITRE CAPEC IDs

CAPEC-117: Interception	**An attacker monitors data streams to or from the target to collect sensitive information or support further attacks, which can include sniffing network traffic and other data streams like radio communications.**
CAPEC-122: Privilege Abuse	An attacker takes advantage of features intended for privileged users that are accessible to non-privileged accounts. Controlling access to sensitive information and functionality is vital to ensure only authorized users can access these resources.
CAPEC-124: Shared Resource Manipulation	An attacker manipulates shared resources, such as application pools or hardware pin multiplexing, to influence behavior. This can compromise other applications or threads depending on the shared resource.
CAPEC-125: Flooding	An attacker depletes a target's resources by rapidly initiating numerous interactions, exploiting rate limiting weaknesses. This flooding attack prevents legitimate access and can cause crashes, relying on request volume rather than operational manipulation.
CAPEC-148: Content Spoofing	An attacker modifies content to differ from the original while keeping the apparent source unchanged. This includes web pages, emails, and file transfers, leading to financial fraud, privacy violations, and other negative consequences.
CAPEC-151: Identity Spoofing	An attacker engages in identity spoofing by assuming another entity's identity to achieve a goal. They may craft messages that appear to come from a different source or use stolen or spoofed authentication credentials to perform malicious activities.
CAPEC-153: Input Data Manipulation	An attacker takes advantage of input validation weaknesses by manipulating the data format, structure, and composition sent to an input-processing interface. By providing non-standard input, the attacker can compromise the security of the target system.
CAPEC-161: Infrastructure Manipulation	An attacker manipulates network routing to redirect messages to their server. Unaware of the redirection, victims unknowingly share sensitive information, such as bank login credentials, believing they are connecting securely.
CAPEC-184: Software Integrity Attack	An attacker triggers events that cause a user, program, server, or device to perform actions compromising software code, data structures, or firmware. This modification undermines the target's integrity, creating an insecure state.
CAPEC-212: Functionality Misuse	An attacker exploits a legitimate application capability to cause harm by using system functionality in unintended ways. This often involves overusing a feature or leveraging design flaws to access unauthorized, sensitive data.
CAPEC-216: Communication Channel Manipulation	An attacker manipulates settings or parameters on a communication channel to compromise its security, potentially causing information exposure, data insertion or removal from the communication stream, and overall system compromise.
CAPEC-231: Oversized Serialized Data Payloads	An attacker injects oversized serialized data payloads into a parser during data processing, leading to adverse effects such as exhausting system resources and enabling arbitrary code execution. This exploitation can cause system crashes.
CAPEC-240: Resource Injection	An attacker takes advantage of input validation flaws by altering resource identifiers, resulting in unintended resource modification or specification. This can cause unauthorized access, data corruption, or other security breaches in the target system.

Table 1 (Continued). Definitions of MITRE CAPEC IDs

CAPEC-272: Protocol Manipulation	**An attacker undermines a communications protocol to carry out attacks such as impersonation, data theft, session control, or other exploits. These attacks exploit invalid assumptions, incorrect implementations, or inherent vulnerabilities within the protocol itself.**
CAPEC-390: Bypassing Physical Security	An attacker can bypass facilities that employ layered physical security models, such as locks, electronic card entry systems, and alarms. Although these measures reduce random breaches, planned attacks can focus on evading security, surveillance, and bypassing locks.
CAPEC-438: Modification During Manufacture	An attacker alters a component during the manufacturing process to compromise the supply chain. They can modify software, hardware, firmware, or design. The most significant risk is intentional design manipulation to create malicious hardware or devices.
CAPEC-439: Manipulation During Distribution	An attacker compromises the integrity of a product, software, or technology during its distribution. The threat can emerge at multiple stages, with tampering potentially occurring during integration or packaging as products pass through various suppliers and integrators.
CAPEC-440: Hardware Integrity Attack	An attacker exploits vulnerabilities in the system maintenance process to implement changes or new installations in technology, products, or components at the victim's location, intending to launch an attack during their operational use.
CAPEC-441: Malicious Logic Insertion	An attacker embeds hidden malicious logic (malware) into a benign component of a deployed system, exploiting new attack vectors such as digital storage, Bluetooth, and Wi-Fi in devices like greeting cards, picture frames, and projectors.
CAPEC-476: Signature Spoofing by Misrepresentation	An attacker takes advantage of vulnerabilities in parsing or display code to create a data blob that appears to have a valid signature but contains a false identity. This manipulation can cause the recipient software or user to perform compromising actions.
CAPEC-490: Amplification	An attacker carries out an amplification attack by sending requests to a third-party service using a spoofed source address. This causes large responses to flood the target server, leveraging minimal resources to create significant traffic.
CAPEC-536: Data Injected During Configuration	An attacker injects malicious data into critical operational files during the configuration or recalibration of a victim's system. This manipulation causes the system to perform suboptimally, benefiting the attacker and compromising the system's efficiency.
CAPEC-547: Physical Destruction of Device or Component	An attacker physically damages a device or component, rendering it nonfunctional. This destruction prevents the device from operating as intended, disrupting its normal function and potentially causing significant operational impact.
CAPEC-578: Disable Security Software	An attacker exploits a weakness in access control to disable security tools, ensuring they are not detected. This can involve terminating processes, deleting registry keys to prevent tools from starting at runtime, deleting log files, or using other methods.
CAPEC-582: Route Disabling	An attacker disrupts the network route between two targets, severing their communication channel. Unlike typical obstruction attacks, this approach targets the route itself rather than the data. It can result from significant errors or manipulation of infrastructure control.

Table 1 (Continued). Definitions of MITRE CAPEC IDs

CAPEC-593: **Session Hijacking**	**This type of attack involves an adversary exploiting weaknesses in an application's session management for authentication. The attacker can steal or manipulate an active session to gain unauthorized access to the application.**
CAPEC-594: **Traffic Injection**	An attacker injects traffic into a target's network connection to degrade or disrupt it and potentially alter its content. This targeted attack uses specific input to affect the system, rather than overwhelming resources through flooding.
CAPEC-600: **Credential Stuffing**	An attacker employs known credentials across various systems to gain access. Credential stuffing exploits the common practice of credential reuse, increasing the chances of unauthorized access.
CAPEC-601: **Jamming**	An adversary uses radio noise or signals to interfere with communications. By deliberately flooding system resources with illegitimate traffic, they prevent authorized users' legitimate traffic from getting through.
CAPEC-603: **Blockage**	An attacker obstructs the delivery of a critical system resource, causing the system to fail or stop functioning. This disruption can halt operations, resulting in significant downtime and potential damage to the system's integrity.
CAPEC-624: **Hardware Fault Injection**	An attacker employs disruptive signals or environmental changes, such as electromagnetic pulses, laser pulses, and temperature extremes, to cause device malfunctions. These methods can exploit cryptographic operations to obtain secret key information.
CAPEC-627: **Counterfeit GPS Signals**	An attacker tricks a GPS receiver by broadcasting fake GPS signals that imitate normal ones. These spoofed signals mislead the receiver, causing it to estimate its location incorrectly or register an inaccurate time. This deception can lead to significant navigation errors.
CAPEC-634: **Probe Audio and Video Peripherals**	The attacker leverages audio and video functionalities through malware or scheduled tasks to capture sensitive information via microphones, webcams, or applications with audio and video capabilities, aiming for financial, personal, or political gain.
CAPEC-699: **Eavesdropping on a Monitor**	An attacker eavesdrops on the content of an external monitor by capturing signals emitted from cables or video ports. This method impacts data confidentiality without altering the cables or installing software, thus evading detection by traditional security tools.

Each MITRE CAPEC attack vector was re-examined and the metrics were recalculated according to the vulnerabilities and weaknesses of the vessel components and cyber-attack vectors in the maritime sector. MITRE CAPEC serves as a reference for understanding the potential risks associated with each component and helps prioritize security measures based on the calculated risk levels.

Understanding CAPEC IDs is crucial for accurately identifying and categorizing various cyber threats that can affect maritime systems. Each CAPEC ID corresponds to a specific attack pattern and provides detailed descriptions and methodologies used by adversaries. This information is crucial for security experts in designing and implementing effective mitigation strategies for specific threats.

Our risk calculation model involves defining metrics for probability, severity, and impact, and then converting these metrics into a risk score according to each CAPED ID in the list. Below the factor affecting the risk score can be listed as below:

- **Probability:** refers to the likelihood of an attack occurring.

- **Attack Surface:** Refers to how exposed and vulnerable the network is.
- **Enemy Skill Level:** Indicates the technical expertise required for the attack.
- **Defensive Measures:** Refers to the existing security controls that can prevent or detect the attack.
- **Prevalence:** Indicates how common such attacks are in similar contexts.
- **Severity:** Refers to the extent of damage or disruption that the attack could cause.

To calculate the impact, we can use either the Weighted Sum Approach or the Multiplier Effect Approach. In our framework, we use the Multiplier Effect Approach to calculate the impact more precisely.

$$I = \sqrt{LxS} \quad (1)$$

For each component considered, the probability, severity, and impact values were determined based on CAPEC IDs that could serve as potential attack models for the components, as well as personal observations and assessments in the field of cybersecurity. After calculating the risk impact, it is possible to calculate the Risk Score (RS) by multiplying Likelihood, Severity, and Impact. Risk Score can be calculated by the formula below:

$$RS = L \; x \; S \; x \; I \quad (2)$$

The probability, severity, and impact values for each component were determined based on CAPEC IDs that could serve as potential attack models for the components, as well as personal observations and assessments in the field of cybersecurity. Even the CAPEC ID's give the Likelihood, Severity, and Impact scores, our risk analysis model provides a different approach by adding the mitigations and the maritime technology, especially vessel ICTs.

Table 2. Rate Scores and Definitions

Likelihood (L)	Severity (S)	Impact (I)	Risk Score (RS)
1 (Rare)	1 (Negligible)	1 (Insignificant)	*RS = L x S x I*
2 (Unlikely)	2 (Minor)	2 (Low)	*RS = L x S x I*
3 (Possible)	3 (Moderate)	3 (Medium)	*RS = L x S x I*
4 (Likely)	4 (Major)	4 (High)	*RS = L x S x I*
5 (Almost Certain)	5 (Catastrophic)	5 (Critical)	*RS = L x S x I*

We created a risk scoring table that consists of four risk levels: Low, Medium, High, and Critical. It is possible to find the Risk Level for each potential risk by matching the calculated RS value with the RS Range on Table 3. Risk mitigation is essential for protecting the operational integrity, safety, and efficiency of maritime vessels.

By identifying, assessing, and implementing strategies to reduce risks, organizations can prevent potential disasters, financial losses, and operational disruptions. Effective risk mitigation ensures compliance with international maritime regulations, maintaining the vessel's certification and avoiding legal repercussions. Additionally, it enhances the resilience of ship operations, ensuring that critical systems remain functional even in adverse conditions or cyber threats.

We also used Monte Carlo simulation for adding a mathematical calculation for each risk on vessel components. Monte Carlo simulation is a technique used to solve mathematical problems by

employing a large number of samples of random variables. This method is particularly useful for risk assessment in situations where uncertainties and variables are complex. To incorporate Monte Carlo Simulation into our developed cyber risk analysis model, the following steps can be applied:

- **Defining Probability Distributions:** Probability distributions for the probability, severity, and impact values are defined for each component. These distributions are determined based on historical data and expert opinions.
- **Generating Random Samples:** Random samples (sample sets) are generated from the defined probability distributions. Each sample represents the likelihood, probability, severity, and impact values for a specific scenario.
- **Calculating Risk Scores:** A risk score is calculated for each sample. These calculations are repeated thousands of times over a specific period to obtain the distribution of risk scores.
- **Analyzing Results:** The obtained distribution of risk scores is analyzed. This analysis includes key statistical measures such as the mean value of the risk, variance, and the probability of exceeding a certain threshold.
- **Decision Making:** Based on the analysis results, the most critical components and the measures that need to be taken for them are identified.

For each component within the system or framework under analysis, probability distributions are carefully defined based on the nature and characteristics of the data. Common distributions such as normal, log-normal, beta, or other appropriate models are selected to best represent the underlying behavior and uncertainty associated with each component. These distributions are chosen to accurately capture variability and provide a realistic basis for subsequent calculations.

Once the probability distributions are defined, the Risk Score for each component is calculated. This involves evaluating the potential impact and likelihood of risks associated with the component, often by integrating the selected probability distributions into a risk model. These Risk Scores serve as quantitative measures of the risks posed by individual components.

Following the calculation of individual Risk Scores, a comprehensive analysis is conducted to determine the overall Mean Risk Score. This is achieved by averaging the Risk Scores across all components, providing an aggregated view of the system's risk profile. Additionally, the Variance of the Risk Scores is calculated to assess the level of dispersion or variability in the risk data, offering insights into the consistency of risk levels across components.

The results of these calculations form the foundation for the Simulation Results Analysis. This analysis leverages the calculated Mean Risk Score and Variance to evaluate system-wide risk trends, identify outliers, and prioritize areas requiring intervention or mitigation. By systematically combining probability distributions with statistical measures, the approach ensures a robust and detailed understanding of risks, enabling informed decision-making and effective risk management strategies.

$$P(L) = f(L), P(S) = g(S), P(I) = h(I) \quad (3)$$

$$\mathrm{RSi} = \mathrm{Li} \times \mathrm{Si} \times \mathrm{Ii}(\mathrm{i} = 1, 2, \ldots, \mathrm{N}) \quad (4)$$

$$\mu RS = \frac{1}{N} \sum_{i=1}^{N} RS_i \quad (5)$$

$$\sigma_{RS}^2 = \frac{1}{N} \sum_{i=1}^{N} (RS_i - \mu RS)^2 \quad (6)$$

After the Initial Risk Score (IRS) has been determined for each identified risk, targeted mitigation efforts are subsequently undertaken. These efforts are critical in managing and reducing the overall risk exposure. The process involves several key steps, including the identification and implementation

of preventive actions, the assessment of associated costs, the calculation of the proportion of the risk mitigated, and the evaluation of the residual impact. Once the IRS is calculated, specific mitigation strategies are developed and implemented to address the identified risks. These strategies are tailored to reduce the likelihood, severity, and impact of each risk. Preventive actions may include technological upgrades, process improvements, training programs, policy changes, or other relevant interventions designed to mitigate the risk.

Each preventive action incurs a certain cost, which needs to be assessed and documented. This includes direct costs, such as the purchase of new technology or the implementation of new processes, and indirect costs, such as training personnel or potential downtime during the implementation phase. A thorough cost-benefit analysis is conducted to ensure that the benefits of the mitigation efforts outweigh the costs involved. The proportion of the risk that has been mitigated as a result of the preventive actions is calculated. This is typically expressed as a percentage, indicating how much of the initial risk has been effectively reduced.

$$PRM = \frac{Percentage\ of\ Risk\ Mitigated}{100} \qquad (7)$$

Mitigated risk refers to the level of risk that remains after preventive measures and mitigation strategies have been implemented to reduce the initial risk. Essentially, it is the portion of the initial risk that has been addressed and minimized through various risk management activities. Mitigation efforts aim to lower the likelihood of the risk event occurring, decrease the severity of its consequences, or lessen its overall impact on the organization.

$$MRS(i) = IRS(i)\ x\ PRM(i) \quad (8)$$

The residual impact, or the risk that remains after the preventive actions have been implemented, is then evaluated. Residual impact refers to the level of risk that remains after all possible mitigation measures have been implemented. It is the potential effect or damage that could still occur despite the efforts to reduce or control the initial risk.

$$RRS(i) = IRS(i) - MRS(i) \quad (9)$$

The Residual Risk Score helps in understanding the remaining risk that the organization needs to manage and monitor continuously. Finally, the total cost of mitigation is determined, which includes both the costs of the preventive actions and the potential costs associated with the residual risk. The Total Cost (TC) is calculated as:

$$C_{total} = \sum_{i-1}^{n}(Cost(i) + C_{RI}(i)\ x\ RRS(i)) \quad (10)$$

This comprehensive evaluation ensures that the mitigation strategies are not only effective in reducing risk but also cost-efficient. By continuously assessing and refining these strategies, organizations can enhance their risk management framework and ensure a robust approach to mitigating potential threats. After defining the Cost of Preventive Measures, it is important to calculate the Total Cost. The last step is to create a risk inventory and define a budget for mitigating. Then the risks are prioritized according to the budget, initial risk score, initial cost, mitigation cost, and mitigation rate. Optimal Cost Balance algorithm is used to minimize the cybersecurity risk by selecting the most cost-effective measures within a predefined budget.

$$M_i = \frac{R_i}{C_i}\ for\ i = 1,2,...,N \quad (11)$$

$$Sort\ (M_i, i)\ in\ decending\ order\ by\ Mi$$

$$Initialize\ P = 0,\ Budget\ remaining = B$$

$$For\ each\ measure\ (M_i, i)\ in\ sorted\ order:$$

$$if\ C_i \leq Budget\ remaining:$$

$$P = P \cup \{i\}$$

$$Budget\ remaining = Budget\ remaining - C_i$$

This loop iteratively selects measures as long as their cost does not exceed the remaining budget. The algorithmic representation of the proposed methodology delineates a systematic approach to maritime cybersecurity risk assessment and mitigation. This comprehensive framework encompasses multiple interconnected phases, beginning with data acquisition and culminating in optimized risk management strategies. The methodology integrates both deterministic and probabilistic components, incorporating Monte Carlo simulation techniques for uncertainty quantification and an optimal cost balance algorithm for resource allocation optimization.

Here is the flowchart of the methodology in Mermaid syntax:

```
flowchart TD
    A[Start] --> B[Data Collection]
    B --> B1[Academic Database Research]
    B --> B2[Maritime Cyber Attack Database]
    B --> B3[CAPEC Attack Vectors]

    B1 & B2 & B3 --> C[Initial Risk Assessment]
    C --> C1[Define Metrics]
    C1 --> C2[Calculate Initial Risk Score]
    C2 --> |RS = L × S × I| C3[Risk Level Classification]

    C3 --> D[Monte Carlo Simulation]
    D --> D1[Define Probability Distributions]
    D1 --> D2[Generate Random Samples]
    D2 --> D3[Calculate Risk Scores]
    D3 --> D4[Analyze Results]

    D4 --> E[Risk Mitigation]
    E --> E1[Calculate Mitigated Risk Score]
    E1 --> |MRS = IRS × PRM| E2[Calculate Residual Risk]
    E2 --> |RRS = IRS − MRS| E3[Calculate Total Cost]

    E3 --> F[Optimal Cost Balance Algorithm]
    F --> F1[Sort Measures by Effectiveness]
    F1 --> F2[Initialize Budget]
    F2 --> F3[Select Cost-Effective Measures]
    F3 --> G[End]
```

4. Results

This section presents the findings obtained using our Monte Carlo simulation-based risk analysis model. The scenario involves assessing cyber risks for a specific ship component in the maritime sector. The simulation results demonstrate the level of risk carried by the ship's navigation system under certain scenarios and the factors influencing this risk.

According to the Monte Carlo simulation results, the impact magnitude indicates how certain security measures can alter the risk scores. It is essential to determine the severity of the risk using the mean risk score and variance. Even the CVSS scoring system is suitable, we have created our Risk Score Range for our model. Initially, the risk scores need to be categorized into specific ranges:

Table 3. Risk Levels and Descriptions

Risk Score Range	Risk Level	Description
0.00 – 0.20	Low	Minimal risk, manageable with standard controls.
0.21 – 0.40	Medium	Moderate risk, needs targeted controls.
0.41 – 0.60	High	Significant risk, requires immediate action.
0.61 – 1.00	Very High	Severe risk, demands urgent comprehensive action.

A specialized software is developed using the Python programming language to integrate Monte Carlo simulation for risk analysis. The software leverages the powerful *numpy* package for statistical data analysis and the *matplotlib* package for creating histograms. This software aims to assess the risk associated with various components of a system, in this case, a ship component. By utilizing Monte Carlo simulation, the software provides a probabilistic analysis that accounts for the inherent uncertainties in risk assessment parameters.

For each of these parameters, estimated standard deviation values are used to account for the uncertainties in their estimation. The Monte Carlo simulation generates numerous scenarios by sampling from the probability distributions defined by these standard deviations, providing a comprehensive view of the potential outcomes.

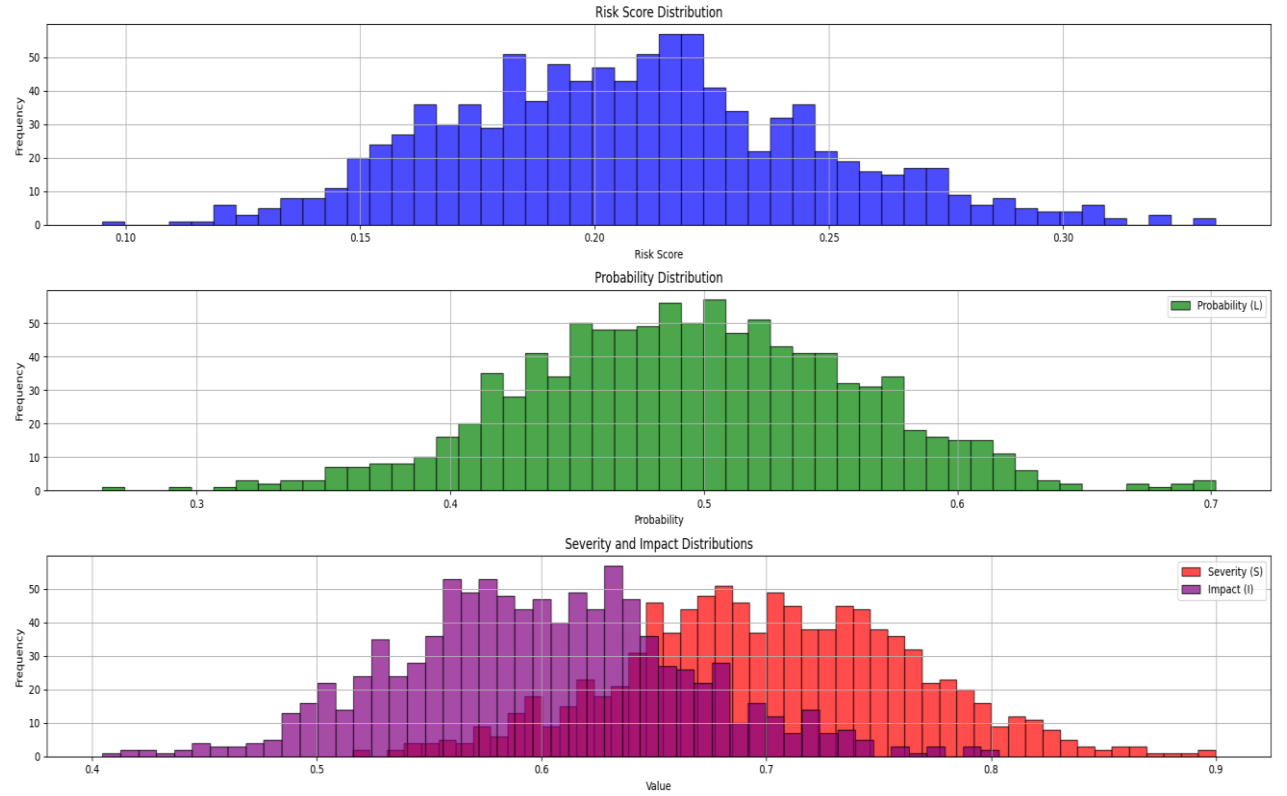
After the simulation, the software calculates the following statistical measures from the generated risk scores. The results of the risk analysis are visualized using histograms, which provide a graphical representation of the distribution of risk scores. This visualization helps in understanding the risk metrics. The simulation results for a selected ship component are as follows:

- **Mean Risk Score (μ_{RS}):** 0.20801597849455428
- **Risk Score Variance (σ^2_{RS}):** 0.0015108564402906298
- **Risk Severity:** Very High
- **Risk Probability (L_{mean}):** 0.5
- **Risk Severity (S_{mean}):** 0.7
- **Risk Impact (I_{mean}):** 0.6000000000000001

To accurately determine the overall risk score of the entire system and assess the company's security posture, it is essential to calculate each individual risk through a systematic, iterative process. This involves executing a loop that methodically evaluates all components or risk factors within the system, utilizing Monte Carlo simulation for each. The iterative loop ensures that the simulation captures the complex interactions and dependencies among various risk factors.

As the simulation runs, it aggregates the individual risk scores to provide a comprehensive, holistic view of the system's risk landscape. This aggregated risk profile is instrumental in enabling decision-makers to make well-informed, strategic decisions regarding risk mitigation and management. By understanding the cumulative risk, organizations can prioritize their efforts and allocate resources effectively to address the most significant vulnerabilities. This approach not only enhances the overall cybersecurity resilience but also ensures that the available budget is used in a manner that maximizes risk reduction, thereby strengthening the company's defensive posture against potential cyber threats.

Figure 1. Risk Severity and Impact Distribution Histogram



The tool utilizes a systematic approach to optimize the selection of cybersecurity measures based on a given budget. It performs a risk and cost analysis, prioritizes the measures, and outputs the most cost-effective solutions to mitigate the risks within the available budget. The tool also employs an Optimal Cost Balance Algorithm to assess and prioritize cybersecurity measures. The key steps involved in the process are:

1. **Risk and Cost Data Input:** The user provides the necessary data, including the costs, risk reductions, initial risk scores, and initial risk costs for various cybersecurity measures. Additionally, a total budget is specified.
2. **Calculation of Efficiency Ratios:** The tool calculates the efficiency ratio for each measure, defined as the risk reduction per unit cost. This ratio helps in determining the cost-effectiveness of each measure.
3. **Sorting of Measures:** The measures are sorted in descending order based on their efficiency ratios, ensuring that the most effective measures are considered first.
4. **Budget-Constrained Selection:** The tool iterates through the sorted list and selects the measures that can be implemented within the provided budget. It keeps track of the remaining budget and stops once no further measures can be accommodated.

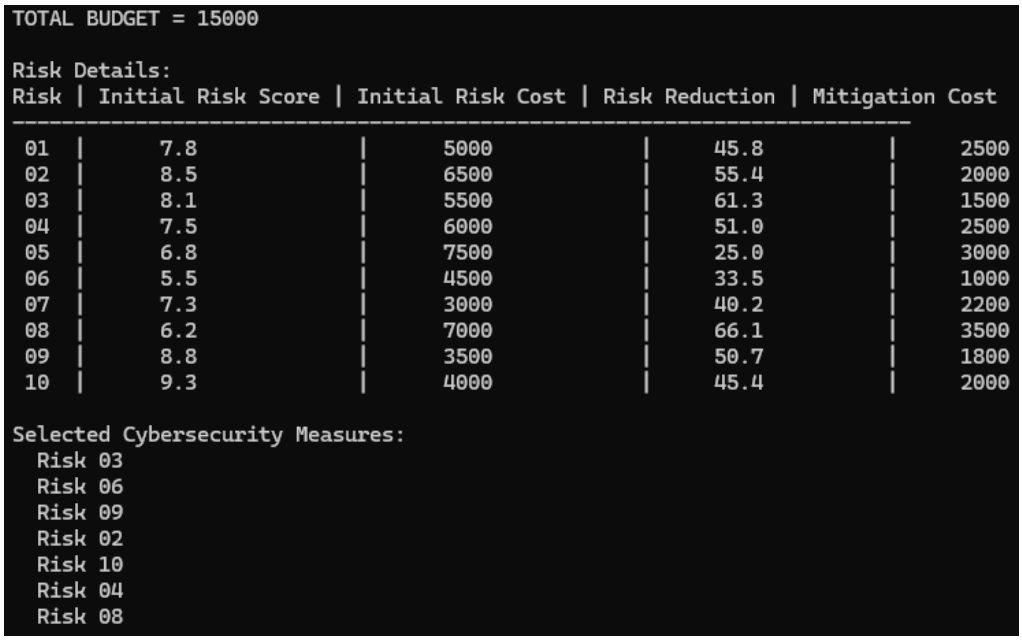
The tool documents the details of each risk, including the initial risk score, initial risk cost, risk mitigation, and mitigation cost. This comprehensive information is crucial for understanding the baseline conditions and evaluating the potential impact of each mitigation measure. In addition to detailed documentation, the tool also generates a visual representation of the mitigation costs and initial risk costs for each risk in the form of a chart. This visual aid is instrumental in illustrating the cost distribution and the relative impact of each measure. By clearly displaying the financial aspects of risk management, the chart helps decision makers to quickly compare and contrast different risks and their associated costs, facilitating a deeper understanding of where resources can be most effectively allocated to maximize risk mitigation.

Table 4. Risk Reduction Rates and Mitigation Costs (Total Budget = $15k)

Risk ID	Initial RS	Initial RC ($k)	Risk Reduction (%)	Mitigation Cost ($k)
01	7.8	5000	45.8	2500
02	8.5	6500	55.4	2000
03	8.1	5500	61.3	1500
04	7.5	6000	51.6	2500
05	6.8	7500	25.2	3000
06	5.5	4500	33.5	1000
07	7.3	3000	40.7	2200
08	6.2	7000	66.1	3500
09	8.8	3500	50.4	1800
10	9.3	4000	46.9	2000

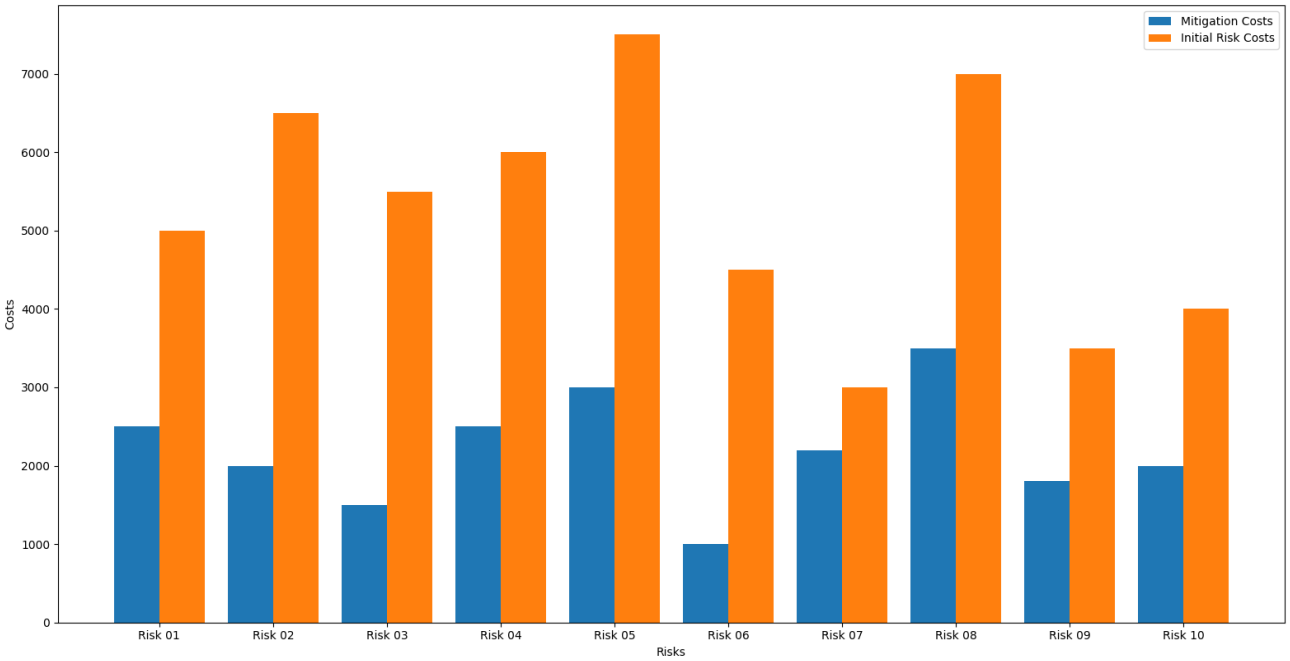
The tool effectively prioritizes and selects cybersecurity measures that provide the highest risk reduction within a specified budget. By combining quantitative analysis with visualization, it aids decision-makers in understanding and addressing the most critical risks efficiently. The selected measures represent a strategic approach to enhancing the company's security posture, ensuring that the available resources are utilized in the most impactful way. Based on the budget constraints and the efficiency ratios, the tool selects the cybersecurity measures.

Figure 2. Selected Cybersecurity Measures



As seen in the list, there are only 7 (seven) risks that can be mitigated within the budget of $15,000. These selected measures collectively offer a significant improvement in the security posture of the company by addressing the most critical and cost-effective risks first. These measures were selected because they provide the highest risk reduction per unit cost and fit within the specified budget. The selection process ensures that the maximum possible risk reduction is achieved with the available budget.

Figure 3. Initial Risk Costs and Mitigation Costs



5. Discussion

The maritime sector comprises many different stakeholders, each potentially bringing its own risks depending on the nature of its IT infrastructure. For instance, the information systems on a ship within a maritime company differ from those in the IT department onshore. Therefore, there is a need for a universal and interconnected risk assessment framework specific to the maritime sector.

The Monte Carlo simulation-based risk analysis model used in this study allows for a more accurate and reliable assessment of cyber risks for specific components in the maritime sector. With the increasing digitalization in the maritime industry, it highlights the rise in cybersecurity threats and the necessity for more proactive measures against these threats. Specifically, critical components such as ship navigation systems should implement stricter security controls and continuous monitoring systems.

Optimal Cost Balance Algorithm provides companies with a systematic method to prioritize risk mitigation within a given budget. The Python-based tool developed for this case study can be extended into a visual, user-friendly interface. By incorporating this tool into a professional web-based platform, it can be delivered as a software-as-a-service (SaaS) solution specifically for the maritime industry. This approach not only enhances the usability and accessibility of the tool but also enables real-time risk assessment and decision-making.

Future research should test the applicability of this model across different types of ships and operational scenarios to enhance its accuracy and reliability with the data obtained. Moreover, integrating dynamic risk assessment models and real-time threat intelligence can further improve the effectiveness of cybersecurity strategies in the maritime sector.

6. Conclusion

The integration of a cyber risk framework based on MITRE CAPEC into the maritime industry is crucial for protecting modern ships against emerging cyber threats. This comprehensive framework, designed to assess and mitigate risks associated with each ship component, offers a robust methodology that includes both qualitative and quantitative analysis. By employing the Multiplier Effect Approach and traditional risk management methods, our research provides a detailed risk calculation model that prioritizes the security of critical maritime assets.

The maritime sector, with its complex network of ships, ports, and supply chains, is particularly vulnerable to cyber threats due to its increasing reliance on digital technologies. Our study emphasizes the importance of understanding and addressing these vulnerabilities through systematic risk assessment and proactive cybersecurity measures.

The risk calculation table we developed allows for precise evaluation of the impact of cyber threats, ensuring that security efforts are focused on the most critical areas. By identifying specific attack patterns and corresponding mitigation strategies, maritime organizations can enhance their cybersecurity posture and resilience against potential disruptions. Decision making on risk mitigation is also very important for maritime organizations. It may be difficult to prioritize risk mitigation within a specific budget. Our framework helps decision makers by calculating the risk impacts and mitigation costs by using the Optimal Cost Balance Algorithm.

Future research can further develop our cyber risk framework for the maritime industry. One key area is expanding the attack pattern database to include emerging threats, providing a more comprehensive perspective on potential threats and mitigation strategies. Additionally, developing dynamic risk models adjusted based on real-time data and threat intelligence, along with incorporating financial impact assessments, can significantly enhance the robustness and accuracy of risk calculations.

Another critical area for future research is the application and validation of the framework through extensive case studies and real-world implementations. Longitudinal case studies across multiple ships and ports can provide valuable data on the framework's effectiveness over time. Applying the framework to various maritime operations, such as commercial shipping, naval operations, and offshore platforms, can help evaluate its adaptability and effectiveness in different contexts.

Lastly, focusing on human factors and training, as well as policy and regulatory frameworks, can offer significant advancements. Analyzing the impact of human behavior on cybersecurity, developing simulation-based training programs, and examining the effectiveness of existing maritime cybersecurity policies can address critical gaps.

Encouraging interdisciplinary research and establishing public-private partnerships can foster innovation and improve the overall security posture of the maritime industry. By exploring these research directions, future studies can contribute to the advancement of maritime cybersecurity and ensure the industry is well-prepared to face evolving threats.

AUTHORS CONTRIBUTION

The Methodology and Results sections of this study were written by the first author, and the other sections were written by the first, second, and third authors.

STATEMENT OF CONFLICT OF INTEREST

There is no financial conflict of interest with any institution, organization, or person and there is no conflict of interest between the authors.

REFERENCES

Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). Analysis and characterization of cyber threats leveraging the mitre att&ck database. IEEE Access, 12, 1217-1234. https://doi.org/10.1109/access.2023.3344680

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of ais automated identification system. Proceedings of the 30th Annual Computer Security Applications Conference. https://doi.org/10.1145/2664243.2664257

Bakar, N. A. (2019). Monte carlo simulation for data volatility analysis of stock prices in islamic finance for malaysia composite index. International Journal of Advanced Engineering Research and Science, 6(3), 6-12. https://doi.org/10.22161/ijaers.6.3.2

BBC. (2016). North Korea 'jamming GPS signals' near South border. Erişim adresi: https://www.bbc.com/news/world-asia-35940542

Blonigen, B. A. and Wilson, W. W. (2007). Port efficiency and trade flows*. Review of International Economics, 16(1), 21-36. https://doi.org/10.1111/j.1467-9396.2007.00723.x

Cuong, T. N., Xu, X., Lee, S., & You, S. (2020). Dynamic analysis and management optimization for maritime supply chains using nonlinear control theory. Journal of International Maritime Safety, Environmental Affairs, and Shipping, 4(2), 48-55. https://doi.org/10.1080/25725084.2020.1784530

Data Breach Today. (2014). Navy Systems Admin. Faces Hacking Charge. Erişim adresi: https://www.databreachtoday.asia/navy-systems-admin-faces-hacking-charge-a-6816

Dimitrov, V. (2023). Capec ontology. Annual of Sofia University St. Kliment Ohridski. Faculty of Mathematics and Informatics, 110, 63-83. https://doi.org/10.60063/gsu.fmi.110.63-83

Drlling Contractor. (2015). Industry recognizing need for better cyber defenses as hackers become more sophisticated and drilling equipment becomes more interconnected. Erişim adresi: https://drillingcontractor.org/drilling-cybersecurity-36727

Grapa, A. and Lemoncito, E. (2021). Maritime security in coastwise domestic shipping as perceived by cadets. Pedagogika-Pedagogy, 93(7s), 197-207. https://doi.org/10.53656/ped21-7s.17mari

Karamperidis, S., Kapalidis, C., & Watson, T. (2021). Maritime cyber security: a global challenge tackled through distinct regional approaches. Journal of Marine Science and Engineering, 9(12), 1323. https://doi.org/10.3390/jmse9121323

Kim, H., Kwon, H. J., & Kim, K. K. (2018). Modified cyber kill chain model for multimedia service environments. Multimedia Tools and Applications, 78(3), 3153-3170. https://doi.org/10.1007/s11042-018-5897-5

Liu, R. (2024). Monte-carlo simulations and applications in machine learning, option pricing, and quantum processes. Highlights in Science, Engineering and Technology, 88, 1132-1137. https://doi.org/10.54097/5yrtzt20

Los Angeles Times. (2017). Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks. Erişim adresi: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

Maritime Executive. (2021). South Korean Shipbuilder DSME Confirms New Possible Cyber Attack. Erişim adresi: https://maritime-executive.com/article/south-korean-shipbuilder-dsme-confirms-new-possible-cyber-attack

NHL Stenden University of Applied Sciences (2023), MCAD Maritime Cyber Attack Database. https://maritimecybersecurity.nl

Papageorgiou, P., Dermatis, Z., Anastasiou, A., Liargovas, P., & Papadimitriou, S. (2023). Using a proposed risk computation procedure and bow-tie diagram as a method for maritime security assessment. Transportation Research Record: Journal of the Transportation Research Board, 2678(2), 318-339. https://doi.org/10.1177/03611981231173641

Pecina, K., Estremera, R., Bilbao, A., & Bilbao, E. (2011). Physical and logical security management organization model based on iso 31000 and iso 27001. 2011 Carnahan Conference on Security Technology. https://doi.org/10.1109/ccst.2011.6095894

Port Technology International. (2022). Dated security patches potential cause behind European port cyber attacks. Erişim adresi: https://www.porttechnology.org/news/dated-security-patches-potential-cause-behind-european-port-cyber-attacks/

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. Journal of Marine Science and Engineering, 9(12), 1384. https://doi.org/10.3390/jmse9121384

Radonja, R. and Glujić, D. (2020). Safety aspects of isps code onboard practice. Naše More, 67(2), 178-180. https://doi.org/10.17818/nm/2020/2.11

Safety4Sea. (2019). Cyber Security challenges for the maritime industry. Erişim adresi: https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/

Seatrade Maritime. (2013). Antwerp incident highlights maritime IT security risk. Erişim adresi: https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk

SeaTrade Maritime. (2020). MSC confirms malware attack caused website outage. Erişim adresi: https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

Security Week. (2023). Japan's Nagoya Port Suspends Cargo Operations Following Ransomware Attack. Erişim adresi: https://www.securityweek.com/japans-nagoya-port-suspends-cargo-operations-following-ransomware-attack/

Seid, E., Popov, O., & Blix, F. (2024). Security attack behavioural pattern analysis for critical service providers. Journal of Cybersecurity and Privacy, 4(1), 55-75. https://doi.org/10.3390/jcp4010004

Soner, O., Kayisioglu, G., Bolat P., Tam, Kimberly. (2024), University of Pplymouth, An investigation of ransomware incidents in the maritime industry: Exploring the key risk factorsindustry: Exploring the key risk factors. https://doi.org/10.1177/1748006X241283093

Tam, K. and Jones, K. (2019). Macra: a model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs, 18(1), 129-163. https://doi.org/10.1007/s13437-019-00162-2

The Jerusalem Post. (2012). Iran official: Cyber attackers target oil platforms. Erişim adresi: https://www.jpost.com/Iranian-Threat/News/Iran-official-Cyber-attackers-target-oil-platforms

Wu, M. and Pan, J. (2018). Research on monte carlo application based on hadoop. ITM Web of Conferences, 17, 03021. https://doi.org/10.1051/itmconf/20181703021

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber security threat modeling based on the mitre enterprise attack matrix. Software and Systems Modeling, 21(1), 157-177. https://doi.org/10.1007/s10270-021-00898-7